



Sistema Informativo-Informatico Regionale

Linee guida per la *Governance* del Sistema Informativo Regionale

(Aggiornamento 2016)

Principali novità della revisione 2016
Modello organizzativo della Governance ICT e il Piano ICT
Ampliamento dell'applicabilità ad Agenzie/Istituti e Assemblea Legislativa
Il Cloud Service Provider Regionale e la mappa dei servizi a seguito di consolidamento
Architettura cartografica e Applicazioni GIS
Ampliamento degli strumenti di business intelligence
Communication & Document Management Microsoft
Policy di patching dei server
I servizi Wi-Fi di Lepida
Accreditamento utenti, ciclo di vita e servizi di autenticazione Active Directory
Autenticazione federata
Servizio pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)
Log Applicativi
Elaborazione, esportazione e importazione di documenti in formato aperto
Il sistema di gestione documentale regionale (Doc/ER)
Workflow di approvazione basati su relazioni funzionali
Registro imprese locale - Parix
Abilitazioni e strumentazioni per i Dirigenti Volontari
Grafica condivisa dei siti web
Accessibilità (aggiornamento normativa e requisiti)
La gestione del servizio applicativo: aggiornamento
Procedure per l'aggiornamento della banca dati CMDBuild e il catalogo dei servizi informatici
Normativa e adempimenti sui Cookies

INDICE

Abstract.....	5
Contesto di riferimento.....	6
1. L'evoluzione del quadro normativo di riferimento per l'ICT regionale.....	6
2. Il Modello organizzativo per la Governance dell'ICT Regionale.....	7
3. Il Sistema di Governance dell'ICT regionale: gli attori, il Piano ICT e le linee guida.....	9
3.1 Gli attori dell'ICT Regionale.....	9
3.1.1 Il Servizio Sistema Informativo-Informatico Regionale.....	9
3.1.2 Le altre strutture regionale ed enti strumentali.....	10
3.1.3 L'Assemblea legislativa.....	10
3.1.4 Le Società Partecipate/In House.....	10
3.1.5 Lepida S.p.A.....	10
3.2 Il Piano ICT.....	10
3.3. Le linee guida: obiettivi e ambito di applicazione.....	11
Il SIIR: Cloud Service Provider Regionale.....	14
4. La trasformazione del datacenter regionale.....	14
5. Il consolidamento: una mappa semplificata.....	15
Standard metodologici e tecnologici di riferimento.....	17
6. Architetture applicative.....	17
6.1 Filiere applicative per le applicazioni custom.....	17
6.2 Architettura cartografica.....	17
6.3 Piattaforme di mercato.....	17
6.3.1 Erp Esteso.....	18
6.3.2 SAS.....	18
6.3.3 SAP NetWeaver Business Warehouse.....	19
6.3.4 SAP BusinessObjects (BO).....	20
6.3.5 SAP Business Planning & Consolidation (BPC).....	21
6.3.6 Oracle Business Intelligence.....	21
6.3.7 Spago BI.....	22
6.3.8 Communication & Document Management Microsoft.....	23
6.4 Tecnologie a supporto delle architetture e filiere applicative.....	24
6.5 Servizi centralizzati forniti a supporto dei sistemi e delle architetture applicative.....	25
6.5.1 Servizi di supporto in fase di progettazione, implementazione e gestione.....	25
6.5.2 Policy di patching dei sistemi server.....	27
6.6 Gestione operativa dei sistemi server e storage.....	28
6.6.1 Implementazione di un nuovo sistema server.....	28
6.6.2 Attività periodiche di gestione del sistema server.....	29
6.7 Networking.....	30
6.8 Wi-Fi.....	30
7. Applicazioni e servizi applicativi infrastrutturali.....	31
7.1 Documentazione.....	31
7.2 Sviluppo.....	32
7.3 Accessibilità.....	34
7.4 Sicurezza.....	35
7.4.1 Accreditamento utenti e servizi di autenticazione Active Directory.....	36
7.4.2 Autenticazione applicativa.....	39
7.4.3 Autenticazione federata.....	39
7.4.4 Servizio pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID).....	40
7.4.5 Cookies.....	41
7.4.6 Monitoraggio.....	41
7.4.7 Log Applicativi.....	41
7.5 Elaborazione, esportazione e importazione di documenti in formato aperto.....	42
7.6 Sistema di Gestione Documentale Regionale.....	42
7.7 Firma digitale.....	43
7.8 Organigramma.....	44
7.9 Workflow di approvazione basati su relazioni funzionali.....	44
7.10 Registro imprese locale - Parix.....	46
7.11 Cooperazione applicativa.....	46
7.12 Grafica condivisa dei siti web.....	49
8. Applicazioni GIS.....	50
8.1 L'Infrastruttura di Dati Territoriali.....	50
8.2 Moka CMS GIS.....	51
8.3 Il Gestore Catalogo Metadati.....	52
8.4 Sistemi di riferimento.....	52
8.5 Geoportale.....	53

8.6 Il Database Topografico Regionale (DBTR)	54
8.7 Pubblicazione dei dati	54
8.8 Servizi cartografici esposti	55
8.8.1 Il Catalog Service del GeoPortale (Internet).....	56
8.8.2 Servizi di Mappa – consultazione (WMS) e download (WFS) - (Internet)	56
8.8.3 Il Servizio di trasformazione coordinate del GeoPortale (Internet)	57
8.8.4 API del Geoportale (Internet)	57
8.8.5 Normalizzatore (Internet)	58
8.8.6 Localizzatore (Internet)	58
9. Siti web.....	58
9.1 Motori di ricerca	59
9.2 Statistiche di accesso a siti e applicazioni web	60
10. Servizi e strumenti web già disponibili	60
Procedure.....	61
11. Acquisizione di prodotti/servizi IT	61
11.1 Verifica preventiva progettuale	61
11.2 Verifica preliminare alla presa in carico.....	62
11.3 Verifica preliminare al rilascio in produzione	63
12. Gestione Servizio Applicativo	64
12.1 SIIR-SYS-App-01, presa in carico e avviamento di un servizio applicativo	65
12.2 SIIR-SYS-App-02, evoluzione di un servizio applicativo	68
12.3 SIIR-SYS-App-03, terminazione di un servizio applicativo	70
13. Aggiornamento della banca dati degli asset ICT e del catalogo dei servizi	72
Dotazioni	75
14. Strumenti di lavoro individuali	75
14.1 Assegnazione	75
14.2 Adempimenti in caso di cessazione del rapporto di lavoro	78
14.3 Modalità di utilizzo	78
14.4 Modalità di richiesta	79
14.5 Modalità di aggiornamento catasto attrezzature informatiche individuali	79
14.6 Modalità di presa in carico di attrezzature	79
14.7 Modalità di supporto ed assistenza.....	79
15. Servizi di rete.....	80
15.1 Accesso alla rete per i telelavoratori	81
15.2 Accesso alla rete via VPN client	81
15.3 Accesso alla rete per fornitori di servizi di teleassistenza	82
15.4 Accesso alle caselle di posta regionale tramite dispositivi mobili	83
Normativa di riferimento	84
Allegati tecnici	90
Allegato 1: Stack tecnologico delle filiere applicative supportate.....	90
Allegato 1a: Stack tecnologico delle architetture GIS supportate	90
Allegato 2: Tecnologie a supporto delle filiere applicative.....	90
Allegato 3: Linee guida per lo sviluppo .NET sui sistemi della Regione Emilia-Romagna	90
Allegato 4: Strumenti di supporto e linee guida per sviluppo applicazioni Java EE	90
Allegato 5: Clausola “accessibilità” per contratti e capitolati tecnici	90
Allegato 6: Lista dei requisiti di accessibilità.....	90
Allegato 7: Liste di controllo per le misure minime di sicurezza.....	90
Allegato 8: Clausola “Sicurezza, privacy e riservatezza” per contratti e capitolati tecnici	90
Allegato 9: Specifiche tecniche per l'utilizzo del sistema di autenticazione centralizzato	90
Allegato 9a: Specifiche tecniche per l'utilizzo del sistema di autenticazione federata (fedERa)	90
Allegato 10: Repository dei sorgenti e tracking	90
Allegato 11: Linee guida sulla grafica condivisa dei siti web.....	90
Allegato 12: Scheda tecnica per nuovo servizio da erogare o fruire tramite Porta di Dominio IcarER	90
Allegato 13: Specifiche tecniche per l'utilizzo dei web services di consultazione dei dati di personale e strutture	90
Allegato 14: Schede tecniche: applicativa e sistemi	90
Allegato 15: Livelli di servizio.....	90
Allegato 16: Cookie - normativa e istruzioni operative.....	90
Allegato 17: Regole per Sistemi di Riferimento dei dati geografici e nelle applicazioni GIS	90
Allegato 18: Linee guida per l'integrazione dei sistemi verticali con il sistema documentale regionale	90

Abstract

Il processo di riforma avviato dalla L. 124/2015 (**Legge Madia**) e dallo Schema di Decreto legislativo di riforma del Codice dell'Amministrazione Digitale approvato dal Consiglio dei Ministri il 20 gennaio 2016, pongono in capo ad ogni ente **la necessità di garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione, centralizzando in capo ad un ufficio unico a cui affidare il compito di accompagnare la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione, con l'obiettivo generale di realizzare un'amministrazione digitale e aperta, dotata di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità.**

Si tratta degli stessi **obiettivi che la Regione Emilia-Romagna ha implementato sia sul fronte legislativo che su quello organizzativo, tramite un modello di governance dei Sistemi Informativi e informatici improntati alla razionalizzazione della spesa, alla dematerializzazione e digitalizzazione nonché alla trasformazione dei servizi ai cittadini sempre più improntati alla trasparenza e all'accesso digitale.**

Infatti, **la Legge regionale 24 maggio 2004, n.11**, così come modificata con la L.r. 30 luglio 2015 n. 13, "**Sviluppo regionale della società dell'informazione**", prescrive che siano adottate modalità organizzative finalizzate a garantire la programmazione unitaria e integrata degli obiettivi e delle risorse finanziarie destinate allo sviluppo del Sistema informativo della Regione (SIR-ER) e **assegna alla Direzione Generale Centrale Organizzazione, Personale, Sistemi informativi e Telematica funzioni di programmazione, sviluppo, coordinamento generale e monitoraggio.**

Per raggiungere questi obiettivi, e già in linea con gli obiettivi della riforma Madia e del nuovo CAD, nel 2012 è stato delineato un "**Modello organizzativo per la governance dei sistemi informativi regionali**" (DGR n. 1783/2012) che **individua un percorso articolato in tre fasi successive verso la centralizzazione della gestione delle risorse ICT.**

Alla luce del completamento della Fase 2 del percorso di centralizzazione - Modello organizzativo in versione "Coordinata integrata" - e della necessità di predisporre il passaggio alla Fase 3 - Modello organizzativo in versione "Centralizzata" -, **le presenti linee guida alla Governance del sistema informatico regionale hanno come obiettivo** quello di fornire a tutti gli attori dell'ICT Regionale:

- L'evoluzione del quadro normativo di riferimento per l'ICT regionale
- La descrizione del sistema, degli attori e dei processi della governance dell'ICT Regionale;
- Gli obiettivi operativi delle presenti linee guida e il loro ambito di applicazione;
- La trasformazione del SIIR in Cloud Service Provider Regionale;
- La guida agli standard metodologici e tecnologici di riferimento in Regione;
- L'insieme dei servizi infrastrutturali da utilizzare e le metodologie da adottare per garantire lo sviluppo e/o l'adeguamento coordinato e integrato di nuovi sistemi;
- Le procedure da adottare per garantire la coerenza e la sicurezza del sistema informatico regionale;

Le presenti linee guida costituiscono pertanto un ulteriore passo nella direzione tracciata dall'art. 1 della riforma Madia in piena coerenza con quanto previsto dalla L.r. 11/2004 e dalla DGR 1783/2012.

Contesto di riferimento

1. L'evoluzione del quadro normativo di riferimento per l'ICT regionale

Termini quali **identità digitale, interoperabilità dei sistemi informatici, open data, cloud computing, decertificazione, pagamenti elettronici, comunicazioni telematiche, PEC, riuso del software, sicurezza informatica, accessibilità e usabilità dei servizi on-line, Carta della cittadinanza digitale, Freedom of Information Act, domicilio digitale**, ecc., sono sempre più ricorrenti nella produzione legislativa e sempre più spesso dettati dalle esigenze strettamente connesse al processo di digitalizzazione e semplificazione che è imprescindibile per una reale modernizzazione della PA.

In questo contesto, la riforma Madia (L. 124/2015) ha finalmente avviato un riordino complessivo del quadro di riferimento normativo e organizzativo dell'ICT. In particolare all'art. 1 "**Carta della cittadinanza digitale**", la legge ha delegato il Governo ad adottare uno o più decreti legislativi per "razionalizzare i meccanismi e le strutture deputati alla governance in materia di digitalizzazione, al fine di semplificare i processi decisionali";

Lo schema di decreto legislativo di riforma del **Codice dell'Amministrazione Digitale** (D.Lgs. n. 82/2005) approvato dal Governo il 20 gennaio 2016 costituisce dunque un punto di svolta nella turbolenza normativa avviata con la L. 150/2009 verso una PA moderna, digitale e sburocratizzata. Un punto di svolta che si basa su pochi elementi decisivi:

- Vengono **aggiornate le norme che guidano lo sviluppo ICT nazionale, regionale e locale** adeguandole contestualmente al Regolamento (UE) n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (**Regolamento eIDAS**);
- Vengono delegificate molte materie affidando all'**Agenzia per l'Italia Digitale** il compito di **attuare gli obiettivi di digitalizzazione e dematerializzazione dei servizi pubblici** tramite direttive e regolamenti tecnici da adeguare nel tempo;
- Viene fissato l'obbligo di **porre in capo ad un ufficio unico** il compito di accompagnare la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione, con l'obiettivo generale di realizzare un'amministrazione digitale e aperta, dotata di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;

La riforma avviata restituisce dunque **un quadro ordinato che indirizza le singole PA**, sia in forma autonoma che associata, **a ricercare maggiori livelli di integrazione e standardizzazione nelle proprie infrastrutture e servizi ICT per garantire la semplificazione e digitalizzazione dei propri processi** in un quadro di crescente trasparenza.

A livello regionale, precorrendo di gran lunga i tempi di produzione normativa nazionale, **la Legge regionale 24 maggio 2004, n.11 "Sviluppo regionale della società dell'informazione"**, ha inquadrato finalità e obiettivi della diffusione e dell'utilizzo delle tecnologie dell'informazione e della comunicazione (ICT) nella PA e nella società regionale, fissando il sistema di regole e lo sviluppo delle strutture tecnologiche per assicurare integrazione e interoperabilità dei sistemi informativi per lo sviluppo del "territorio digitale".

La Legge regionale al Capo IV definisce infatti il "**Sistema Informativo Regionale**" (SIR) come l'insieme costituito dal "**Sistema Informativo della Regione**" (SIR-ER) e dai "**Sistemi**

informativi integrati” che concorrono entrambi alla formazione del “Patrimonio informativo pubblico”.

Per quanto riguarda i Sistemi informativi Integrati, la Legge prevede all’art. 14 che la Regione provveda ad intese istituzionali con altri soggetti per l’integrazione nel SIR di flussi informativi a scala nazionale e regionale inclusi nei sistemi informativi da essi gestiti o posseduti, al fine di evitare duplicazioni e ridondanze. Nella realizzazione e nella gestione dei sistemi informativi integrati, la Regione può assumere il ruolo di nodo tecnico-informativo centrale, favorendo lo scambio dati fra PA e tra PA e privati: le attività del nodo tecnico-informativo centrale possono essere svolte dalla società Lepida spa.

E’ evidente quindi che **la legge regionale 11/2004**, pur prevedendo articolazioni settoriali di intervento e ambiti di azione che vanno oltre il confine strettamente inteso come “Amministrazione”, **richiama principi di unitarietà, omogeneità, interoperabilità e integrazione dei sistemi informativi.**

Con l’introduzione della **Legge regionale 7 dicembre 2011, n. 18** concernente “Misure per l’attuazione degli obiettivi di semplificazione del sistema amministrativo regionale e locale. Istituzione della sessione di semplificazione”, il Tavolo Permanente per la semplificazione ha inoltre elaborato un documento che individua alcune linee di azione tra cui **“Linea 1: Informatizzazione dei procedimenti amministrativi e interoperabilità delle Pubbliche Amministrazioni”**. Nell’ambito di tale linea d’azione Direzioni, Servizi e Agenzie regionali hanno collaborato attivamente ad elaborare il “Piano degli interventi di semplificazione”, avendo a riferimento l’attuazione del modello regionale **MAD** “Disegno della PA digitale: dematerializzata, interconnessa e cooperativa” (V. Allegato 2B al documento elaborato dal Tavolo Permanente per la semplificazione approvato con Delibera di Giunta n. 983 del 6 luglio 2012).

2. Il Modello organizzativo per la Governance dell’ICT Regionale

Per garantire la realizzazione degli obiettivi prefissati, la Legge Regionale 11/2004, all’art. 16, prescrive che siano adottate modalità organizzative finalizzate a garantire la programmazione unitaria e integrata degli obiettivi e delle risorse finanziarie destinate allo sviluppo del Sistema informativo della Regione (SIR-ER) e assegna alla Direzione Generale Centrale Organizzazione, Personale, Sistemi informativi e Telematica **funzioni di programmazione, sviluppo, coordinamento generale e monitoraggio** al fine di assicurare:

- il presidio della coerenza dell’architettura del SIR-ER, l’unitarietà di impostazione delle funzioni tecniche, sia trasversali che settoriali;
- la programmazione e il coordinamento dell’introduzione del software libero e open source e dell’uso di formati di dati e protocolli di comunicazione aperti o liberi, nonché degli standard indicati dagli enti internazionali preposti;
- lo sviluppo e la gestione delle infrastrutture e dei servizi di garanzia, la progettazione e realizzazione dei progetti trasversali, la definizione di standard generali di riferimento, il supporto e l’assistenza tecnica per lo sviluppo dei servizi e dei sistemi informativi settoriali.

Conseguentemente la Regione ha sviluppato un percorso di consolidamento per garantire uno sviluppo unitario e integrato del Sistema Informativo Regionale.

In particolare, con **la DGR n. 1783/2012**, al fine di superare la gestione delle funzioni ICT autonoma e indipendente da parte delle diverse strutture regionali, ha delineato un **“Modello**

organizzativo per la *governance* dei sistemi informativi regionali” avviando un percorso verso la **centralizzazione della gestione delle risorse ICT** articolato in tre fasi:

- **FASE 1 - Modello organizzativo in versione “Coordinata”**: prevedeva la centralizzazione della programmazione annuale di acquisizione di beni e servizi ICT, il monitoraggio della spesa ICT, la definizione di un quadro unitario del fabbisogno ICT, l'identificazione di soluzioni tecniche e servizi comuni, la pianificazione e l'identificazione delle priorità delle iniziative. La Direzione competente in materia di sistemi informativi **coordinava** la programmazione annuale di acquisizione di beni e servizi ICT. La gestione del Piano ICT era affidata ad una Cabina di regia interdirezionale coordinata dalla Direzione competente in materia di sistemi informativi. La responsabilità delle scelte e della loro realizzazione restava in capo alle strutture.
- **FASE 2 - Modello organizzativo in versione “Coordinata integrata”**: prosegue le attività previste per la Fase 1, rafforzando i processi di razionalizzazione della spesa ICT e attivando le misure correttive delle criticità riscontrate in Fase 1. Si ricomprende nel perimetro di osservazione della spesa ICT anche quella di ARPA e quella veicolata attraverso gli accordi di servizio/intese/convenzioni che le Direzioni stipulano con le società in house/partecipate. Si predispone il modello organizzativo e funzionale atto a supportare la piena realizzazione della Fase 3;
- **FASE 3 - Modello organizzativo in versione “Centralizzata”**: si assegnano piena autonomia e risorse ad un'**unica struttura organizzativa** che assume la responsabilità di gestire l'intero ciclo di vita dei servizi ICT dell'Ente, dalla loro progettazione e realizzazione, fino alla gestione. La strategia e la programmazione ICT vengono definite da tale struttura, a partire dagli obiettivi contenuti nei documenti programmatici e di pianificazione dell'Ente e dal fabbisogno espresso da Direzioni, Agenzie e Istituti regionali (i portatori della domanda di servizi ICT).

Le iniziative di riordino della Governance dell'ICT Regionale realizzate dal 2012 al 2015 (Fase 1 e Fase 2) restituiscono **un quadro notevolmente migliorato che costituisce una base di partenza per sviluppare le iniziative previste nella Fase 3**. In particolare:

- E' stato **consolidato il sistema di Governance dell'ICT regionale** chiarendo la divisione delle competenze assegnate ai **diversi attori** e fissando il processo di programmazione e controllo delle attività nel **Piano ICT annuale** e pluriennale;
- E' stato completato il **consolidamento dei servizi ICT nella nuova Server Farm** di Via Aldo Moro 52.
- Sono stati **standardizzati i sistemi e le piattaforme di riferimento per l'esercizio delle funzioni ICT** di tutta la Regione;
- Sono state **revisionate le linee guida per lo sviluppo e l'esercizio** delle iniziative ICT;
- E' stata **avviato il processo di certificazione ISO 27001:2013** per garantire, al crescere della percentuale di processi esercitati digitalmente e dematerializzati, tecniche, procedure e sistemi di gestione della sicurezza delle informazioni costantemente adeguati.

Le prime analisi sui risultati dell'attività di consolidamento evidenziano **un netto miglioramento dei costi di esercizio nella gestione dei servizi ICT a seguito delle azioni di consolidamento nella nuova server farm regionale. In particolare:**

- a. Il costo di esercizio delle infrastrutture si è ridotto nel 2015 rispetto al 2014 di oltre il 6,8%, pari ad una economia superiore a 1,5 milioni di euro € annui.
- b. A organici invariati, nel 2015 sono state attivate 75 nuove applicazioni presso la server farm regionale con una crescita del 20% rispetto al 2014;

3. Il Sistema di Governance dell'ICT regionale: gli attori, il Piano ICT e le linee guida

Il sistema di Governance dell'ICT Regionale, così come previsto dalle delibere della Giunta Regionale, si basa su una chiara divisione di ruolo e competenze tra i **diversi attori**, su un **sistema di programmazione** degli interventi ICT coordinato e integrato **basato sul Piano ICT** annuale e pluriennale, e su **uno strumento operativo di riferimento** per lo sviluppo, l'integrazione e l'esercizio dei sistemi Informatici e informativi costituito dalle **Linee Guida**.

Di seguito sono illustrate le funzioni assegnate alle tre componenti del sistema di Governance dell'ICT Regionale aggiornate al 2016 al temine della Fase 2.

3.1 Gli attori dell'ICT Regionale

3.1.1 Il Servizio Sistema Informativo-Informatico Regionale

Il Servizio Sistema Informativo-Informatico Regionale (SIIR), le cui competenze sono state aggiornate con DGR n. 519/2013, ha come *mission*:

- la gestione e lo sviluppo di tutte le infrastrutture informatiche (server, rete, data base, middleware, ecc.) presenti nel Data Center regionale ubicato presso la sede di Via Aldo Moro 52;
- la progettazione e la realizzazione di sistemi informativi regionali sia a supporto delle funzioni di governo, sia a supporto di alcuni ambiti settoriali di intervento della Regione;
- l'individuazione e la definizione di standard e piattaforme tecnologiche per lo sviluppo del sistema informativo della Regione;
- la progettazione e la realizzazione di sistemi informativi geografici e della relativa infrastruttura;
- la gestione della sicurezza informatica e l'individuazione di misure destinate a migliorare la sicurezza nei trattamenti dei dati personali nel rispetto delle disposizioni di legge;
- la gestione e lo sviluppo della Telefonia fissa e mobile in relazione anche all'integrazione con le infrastrutture di rete.

Al SIIR è dunque affidato **il coordinamento delle strutture regionali per la definizione della programmazione unitaria di risorse ICT tramite il Piano ICT** e l'individuazione di soluzioni tecniche e servizi comuni, **verificandone la coerenza con gli altri strumenti di programmazione regionale** (Piano della semplificazione, Agenda digitale regionale, Piano della trasparenza, Piano Anticorruzione, Piano della Comunicazione).

3.1.2 Le altre strutture regionale ed enti strumentali

Nell'ambito dello sviluppo del Sistema Informativo della Regione (SIR-ER), **le altre strutture regionali conservano come *mission specifica* la progettazione e la realizzazione di sistemi informativi integrati a supporto dei processi propri degli ambiti settoriali di intervento**, adeguando le proprie attività sotto il profilo programmatico al Piano ICT annuale e pluriennale sotto il profilo e tecnico alle Linee Guida ICT.

3.1.3 L'Assemblea legislativa

Da gennaio 2014 l'Assemblea legislativa rientra a pieno titolo nell'ambito degli attori della Governance ICT regionale a seguito dello sviluppo di un piano di ammodernamento che ha previsto il consolidamento delle infrastrutture nella Server Farm regionale, il riuso di tutte le piattaforme gestionali regionali per liberare risorse da dedicare alla realizzazione, nel pieno rispetto delle linee guida in materia di standard e integrazione, dei sistemi informativi dematerializzati relativi a funzioni proprie.

3.1.4 Le Società Partecipate/In House

Allo sviluppo del SIR-ER contribuiscono anche alcune Società partecipate/in house, che afferiscono alle diverse strutture regionali, a seconda della loro *mission*.

3.1.5 Lepida S.p.A.

Tra le Partecipate un ruolo particolare è svolto da Lepida Spa, la società a totale ed esclusivo capitale pubblico costituita dalla Regione Emilia Romagna ai sensi dell'art. 10, comma 3, della legge regionale n. 11/2004 per la realizzazione e la gestione della rete regionale a banda larga delle pubbliche amministrazioni e la fornitura dei relativi servizi di connettività.

Lepida Spa rappresenta lo strumento operativo per la pianificazione, l'ideazione, la progettazione, lo sviluppo, l'integrazione, il dispiegamento, la configurazione, l'esercizio, la realizzazione delle infrastrutture di telecomunicazione e dei servizi telematici che sfruttano le infrastrutture di rete, per Soci e per Enti collegati alla Rete Lepida. E' evidente quindi che nel panorama ICT regionale essa rappresenti un forte punto di riferimento non solo per le telecomunicazioni ma anche per l'erogazione di servizi IT di cui gli Enti soci, e quindi anche Regione Emilia-Romagna, possono usufruire: **Un ruolo di Hub tecnologico indispensabile per l'intero territorio regionale** per garantire ad Agid il dispiegamento locale della azioni previste dall'Agenda Digitale nazionale ma soprattutto **per garantire l'attuazione dell'Agenda Digitale dell'Emilia Romagna (ADER).**

3.2 Il Piano ICT

Il Piano ICT dell'Ente, previsto dalla Delibera di Giunta regionale n.1783 del 26 novembre 2012, è **uno strumento di pianificazione, coordinamento e programmazione** che descrive:

- gli obiettivi strategici e le linee di azione dell'ICT regionale;
- le iniziative ICT, con relative priorità, tempi di implementazione e stime economiche;
- le relazioni con altri Piani settoriali.

Il Piano dell'ICT contiene i fabbisogni di beni e servizi ICT delle Direzioni generali della Giunta e dell'Assemblea Legislativa, delle Agenzie e degli Istituti regionali, descritti in termini di obiettivi, priorità, tempi di implementazione e stime economiche.

Attraverso il Piano ICT le strutture regionali esprimono i propri fabbisogni ICT, sia quelli che realizzano con proprie risorse sia quelli di cui richiedono la realizzazione al Servizio SIIR. La periodicità con cui viene aggiornato il Piano ICT è almeno di 2 volte l'anno, a inizio anno e dopo l'assestamento di bilancio.

Il Servizio SIIR a seguito delle richieste produrrà le stime economiche per soddisfarle e in base alla priorità indicata e alle risorse disponibili verrà comunicato alla struttura richiedente le iniziative che verranno avviate in quanto compatibili con le risorse a disposizione.

Il Piano ICT è quindi uno strumento di programmazione in ambito ICT che, attraverso un processo unificato di raccolta del fabbisogno ICT, mira al raggiungimento di specifici benefici tra cui:

- l'introduzione di modalità condivise a livello di Ente per la definizione, progettazione, sviluppo e gestione economica delle iniziative ICT;
- l'introduzione di un modello organizzativo e di coordinamento, per la gestione e il monitoraggio del fabbisogno ICT;
- la razionalizzazione del panorama di tecnologie/soluzioni adottate;
- la riduzione dei costi di realizzazione e gestione dei servizi ICT;
- l'ottimizzazione delle risorse disponibili per l'ICT dell'Ente e il perseguimento di economie di scopo sulle iniziative ICT, anche tramite il riuso interno di soluzioni già disponibili;
- la migliore e più tempestiva definizione delle risorse economiche necessarie ogni anno alla gestione degli apparati ICT dell'Ente, in funzione delle soluzioni ICT sviluppate da Direzioni/Agenzie/Istituti;
- la migliore tracciatura e monitoraggio della spesa ICT dell'Ente.

Il Piano ICT si conclude con un monitoraggio annuale finalizzato a rendicontare a tutto l'ente e a tutti gli attori del Piano ICT i risultati ottenuti nell'esercizio precedente in termini finanziari, quantitativi e qualitativi.

3.3. Le linee guida: obiettivi e ambito di applicazione

Nel contesto descritto, data la pluralità degli attori che concorrono allo sviluppo ICT regionale e la loro autonomia, è evidente la necessità di sviluppare un sistema operativo di IT Governance con l'obiettivo di:

- allineare l'IT alla strategia dell'Ente in modo che possa portare i benefici attesi;
- migliorare l'erogazione dei servizi IT agli utenti, razionalizzando i criteri di scelta e la priorità delle richieste, gli impatti sulle risorse disponibili e sui sistemi/applicativi, sui processi e sull'organizzazione e garantendo un maggior e miglior controllo dello stato d'avanzamento delle richieste;
- responsabilizzare maggiormente gli utenti sulle richieste e sul loro impatto tecnico ed economico;
- valutare e bilanciare i rischi tecnici, organizzativi ed economici;
- monitorare periodicamente e sistematicamente le prestazioni e l'uso dell'IT;

- verificare la conformità delle richieste rispetto alla normativa vigente;
- assicurare l'integrità, la confidenzialità e la disponibilità dei sistemi, dei dati e delle risorse.

Per garantire gli obiettivi del Piano ICT è stato necessario:

- **individuare ruoli e processi adeguati, coerenti e integrati tra le diverse strutture:**

processi di lavoro snelli e trasparenti, supportati da strumenti condivisi che assicurino, da un lato, che i settori dell'Amministrazione, pur nella propria autonomia, costruiscano sistemi informativi interoperabili, non ridondanti, sicuri, accessibili; dall'altro, che consentano ai settori centrali competenti in materia di IT, di gestire in maniera più consapevole i sistemi informativi per fornire un servizio qualitativamente migliore. Ciò è possibile solo se l'intero processo che porta alla realizzazione di un qualsivoglia sistema informativo è condiviso e se le interazioni tra le strutture settoriali e quelle centrali non sono vissute come mere pratiche "dovute" bensì come scambio informativo e arricchimento reciproco, finalizzato all'erogazione di un Servizio pubblico più efficiente ed efficace;

- **definire standard metodologici e tecnologici:**

condividere metodologie di lavoro e standard tecnologici contribuisce a diffondere la conoscenza e prevenire l'insorgere di problemi che potrebbero compromettere la continuità dei servizi, la scalabilità e l'interoperabilità dei sistemi oltre che l'accessibilità e la sicurezza;

- **presidiare la conoscenza, ripensando l'organizzazione come rete di competenze:**

poiché il valore delle persone dipende dalla competenza professionale e dalla capacità di affrontare e risolvere problemi, bisogna generare e condividere la conoscenza;

- **porre attenzione al servizio e al cliente/utente, la cui soddisfazione è il metro e la condizione fondamentale per misurare l'efficacia del servizio stesso:**

In questa logica è importante comprendere il fabbisogno dell'utente/cliente e presidiare/gestire la domanda indirizzandola correttamente, individuandone tempi e costi, allocando le risorse, verificando la conformità a leggi e regolamenti, verificando l'adeguatezza delle infrastrutture esistenti, al fine di programmare investimenti per eventuali potenziamenti dell'infrastruttura.

Il raggiungimento di questi obiettivi è affidato alle Linee Guida per la governance del Sistema Informatico Regionale (in breve Linee Guida).

Le linee guida si applicano a tutti i sistemi informativi della Giunta, delle Agenzie, degli Istituti e dell'Assemblea legislativa della Regione Emilia-Romagna:

- strumento per condividere un modello organizzativo;
- strumento di riferimento per capitolati tecnici e/o allegati tecnici al conferimento di incarichi e/o documentazione di prodotto e/o servizi dichiarati da fornitori (in quanto contiene gli standard di riferimento dei sistemi informativi regionali);
- strumento per individuare l'offerta di soluzioni già realizzate e pronte per il riuso all'interno dell'Ente (in quanto contiene informazioni su servizi di interoperabilità già rea-

lizzati e disponibili a chi ne voglia far uso: es. firma digitale, SAP Self Service, organigramma, porta di dominio, integrazione con il sistema documentale, integrazioni tra sistemi di comunicazione e Document management, groupware, questionari online, iscrizione convegni, ecc);

- prontuario per effettuare verifiche di prodotti e servizi che si intendono acquisire o realizzare o prendere a riuso (in quanto contiene check list di riferimento: es. check list per l'accessibilità e la sicurezza delle applicazioni, per la verifica di documentazione obbligatoria per la gestione e manutenzione delle applicazioni, ecc.);
- strumento di riferimento per la richiesta e la distribuzione di dotazioni di strumenti informatici ad uso individuale (PC, portatili, stampanti, collegamenti remoti da casa, ecc.).

Lo scopo di queste linee guida è quindi quello di fornire uno strumento operativo di supporto ai soggetti incaricati di:

- riusare le soluzioni esistenti in un'ottica di miglioramento del ritorno degli investimenti ICT di tutta la regione;
- progettare, sviluppare o acquisire sistemi informativi;
- progettare e sviluppare applicazioni fruibili in mobilità;
- valutare/scegliere fornitori di servizi per la realizzazione di sistemi informativi;
- testare o adeguare sistemi informativi ai criteri di sicurezza previsti dalla normativa vigente;
- testare o adeguare sistemi informativi ai requisiti di accessibilità previsti dalla normativa vigente;
- installare, gestire o mantenere sistemi informativi;
- progettare e/o realizzare siti web;
- effettuare le verifiche preventive progettuali in merito al rispetto degli standard definiti in materia di tecnologie, metodologie di sviluppo e documentazione, livelli minimi di sicurezza e accessibilità;
- effettuare le verifiche preliminari alla presa in carico di prodotti e sottosistemi realizzati da terzi;
- effettuare le verifiche, preliminari al rilascio in produzione di prodotti e sottosistemi realizzati da terzi, anche se in hosting su sistemi esterni.;
- acquistare/distribuire attrezzature individuali all'interno delle strutture regionali;
- acquistare strumentazioni hardware.

Il SIIR: Cloud Service Provider Regionale

4. La trasformazione del datacenter regionale

Negli ultimi anni la crescente necessità di semplificazione, dematerializzazione e digitalizzazione, ha avviato un percorso di revisione dei processi interni e fra le Pubbliche Amministrazioni con la necessità di incrementare la loro interoperabilità.

Tale crescita, purtroppo non accompagnata da una visione strategica univocamente condivisa con tutte le strutture regionali, ha, in passato, comportato la proliferazione di soluzioni applicative eterogenee, governate più dall'offerta che non dalla domanda e installazioni di server dedicati "mono-progetto". Tutto ciò ha comportato nel tempo numerose difficoltà nella gestione dell'infrastruttura, con conseguente aggravio dei costi di gestione, di una qualità di erogazione del Servizio non ottimale e di una mancanza di possibili economie di scala.

Questa disomogeneità di soluzioni ha comportato anche una ricaduta e un appesantimento delle infrastrutture informatiche dei nostri enti locali, costretti a uniformarsi alle diverse richieste delle DG regionali: **il rischio era che un sistema informativo a sottosistemi stagni all'interno della Regione-Ente inducesse sistemi informativi a sottosistemi stagni negli Enti della regione-territorio, con la creazione di sistemi magari integrati verticalmente tra diversi livelli territoriali ma sempre più non comunicanti.**

In tale contesto, le necessità crescenti in termini di potenza elaborative, scalabilità, alta affidabilità e continuità di servizio dell'attuale infrastruttura IT regionale, hanno comportato l'urgenza di **evolvere l'infrastruttura tecnologica a supporto dei progetti informatici regionali nell'ottica di centralizzare la gestione delle piattaforme applicative**, la gestione della sicurezza informatica, la definizione e il controllo degli standard e piattaforme tecnologiche verso una maggiore omogeneità.

Ciò ha sostanzialmente modificato sia in termini qualitativi che quantitativi, il sistema informativo-informatico regionale: da un sistema informativo progettato e realizzato per le specifiche esigenze funzionali dell'Ente Regione, si è progressivamente implementato un sistema informativo che eroga servizi a tutte le strutture regionali, comprese le agenzie e le partecipate che cooperano con la Regione, fornendo anche servizi infrastrutturali in ottica Cloud.

Il modello di Private Cloud realizzato nel datacenter regionale di v.le Aldo Moro 52 **configura il Servizio Sistema Informativo-Informatico regionale come un vero e proprio Cloud service provider** a servizio delle strutture regionali. In [Allegato 2](#) sono descritte:

- le caratteristiche di tale servizio,
- in quali casi potervi accedere (prerequisiti per l'utilizzo e prerequisiti tecnologici),
- compiti del Service Provider,
- compiti della struttura regionale richiedente il servizio.

La gestione integrata e centralizzata dell'infrastruttura tecnologica e applicativa ha portato a notevoli benefici, quali in particolare:

- sinergie per l'Ente negli investimenti su hardware, licenze software e risorse umane, tramite condivisione degli ambienti dedicati alle filiere applicative;

- qualità e continuità di erogazione dei servizi garantita da una infrastruttura adeguata ad un Datacenter;
- controllo centralizzato della sicurezza di dati e applicazioni dell'Ente;
- backup e disaster recovery centralizzato per i dati dell'Ente;
- presidio specialistico delle varie piattaforme applicative;
- tempi di intervento praticamente immediati in caso di problemi alle piattaforme;
- politiche di gestione omogenee per tutti i sistemi dell'Ente.

5. Il consolidamento: una mappa semplificata

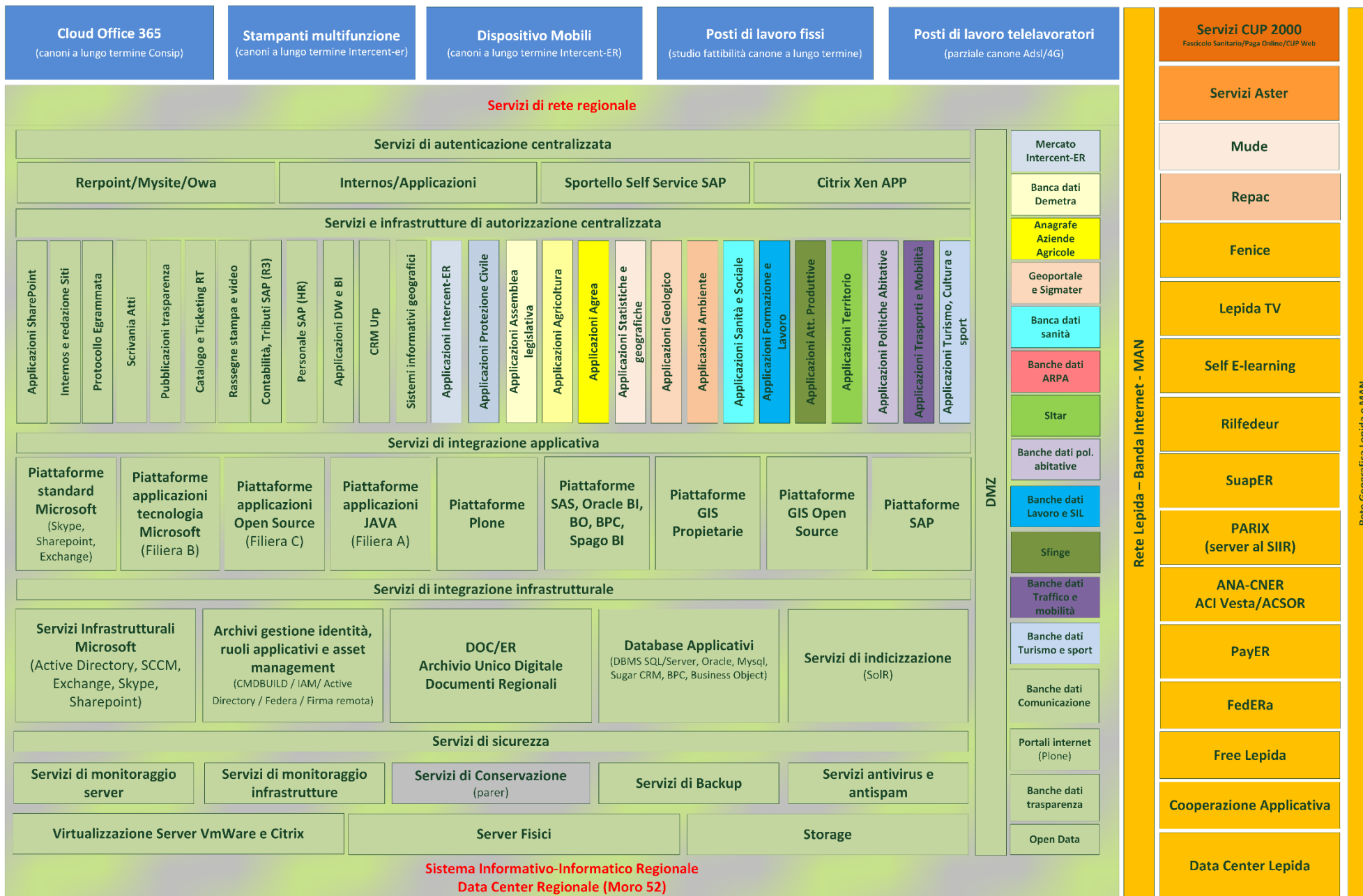
Il risultato delle attività di consolidamento infrastrutturale e applicativo realizzate negli ultimi anni, insieme alla razionalizzazione del sistema di competenze e funzioni realizzate con il piano ICT, sono rappresentate nella mappa funzionale riportata di seguito.

La mappa ha la duplice funzione di fornire, in forma stratificata e semplificata:

- una rappresentazione della divisione di competenze tra tutti gli attori del Piano ICT così come si presentano a inizio 2016.
- Una rappresentazione di tutte le componenti contenute nelle presenti linee guida che concorrono alla realizzazione di un sistema applicativo o servizio ICT regionale.

In particolare:

- In verde chiaro: sono evidenziate tutte le funzioni gestite direttamente dal SIIR attraverso la server farm sita in Viale Aldo Moro, 52
- In arancione: le funzioni esercitate da Lepida spa;
- In blu: le "commodity ICT" che progressivamente sono state (o stanno per essere) affidate al mercato tramite contratti con forme assimilabili al "noleggio a lungo termine";
- Altri colori: sono le funzioni di sviluppo software e banche dati che fanno capo ad altri attori del piano ICT.



Standard metodologici e tecnologici di riferimento

6. Architetture applicative

Di seguito vengono descritte le componenti applicative utilizzate per lo sviluppo dei sistemi informativi dell'Ente.

6.1 Filiere applicative per le applicazioni custom

Nell'ottica di ottimizzare la gestione dei sistemi e l'utilizzo delle risorse hardware e software, aumentare la sicurezza fisica dei dati, l'affidabilità e la disponibilità delle applicazioni, **sono state individuate e standardizzate tre filiere software di riferimento per le applicazioni custom** in uso presso l'Amministrazione e gestite centralmente dal Servizio Sistema Informativo-Informatico Regionale (d'ora in poi Servizio SIIR).

Le filiere supportate per applicazioni e siti web basate su architetture a tre livelli (web server, application server, database server) sono le seguenti:

- **filiere A:** applicazioni basate su tecnologia **JAVA**
- **filiere B:** applicazioni basate su tecnologia **Microsoft**
- **filiere C:** applicazioni basate su tecnologia **OpenSource**

Il dettaglio relativo allo stack tecnologico implementato sulle diverse piattaforme è descritto in Allegato 1.

L'architettura hardware e software attualmente implementata a supporto delle **Filiere applicative A e B** è in grado di garantire:

- scalabilità (crescita costante del numero di utenti target del Servizio),
- qualità e continuità nell'erogazione del Servizio (alta affidabilità dei sistemi),
- supporto sistemistico e specialistico immediato.

6.2 Architettura cartografica

Le applicazioni GIS del sistema informativo regionale che si intendono realizzare e installare sui server gestiti centralmente dal Servizio SIIR si dovranno basare su un'infrastruttura cartografica dispiegata secondo le seguenti due tipologie descritte in Allegato 1a:

- **architettura GIS proprietaria**
- **architettura GIS open source**

6.3 Piattaforme di mercato

Oltre alle filiere applicative standardizzate dedicate allo sviluppo e distribuzione di sistemi informativi custom dell'Ente, l'amministrazione regionale si è dotata di piattaforme di mercato raggruppabili in tre aree di business specifiche:

- **Il sistema ERP esteso** implementato attraverso il prodotto mySAP Business Suite;
- **Gli strumenti di Business Intelligence**, quali SAS, BW, Business Object, BPC, Oracle Business Intelligence e SpagoBI.

- **Il sistema di Communication & Document Management** implementato attraverso le piattaforme Microsoft SharePoint Server, OneDrive for Business, Skype for Business, Exchange Server sia in versione on premise che in versione Cloud Office 365.

Di seguito sono descritte le diverse piattaforme di mercato in uso.

6.3.1 Erp Esteso

Il trend di crescita delle soluzioni implementate negli ultimi anni presso l'Ente ne fanno a tutti gli effetti una filiera enterprise che si affianca alle precedenti ed assume un ruolo centrale nella gestione dei processi critici dell'Ente.

Il sistema ERP di SAP è modulare e composto da soluzioni specializzate e finalizzate alla gestione di determinati flussi organizzativi e procedurali.

Le componenti di SAP utilizzate nelle realizzazioni dei macro-processi implementati sono:

- R/3 Release ECC 6.07 FM, FI, AA, CO, MM, PM, SD, RE
- HCM Release ECC 6.07 (PA, OM, Payroll, TM, TV, ESS, TLM, E-recruiting, LSO, PE, PD)
- CRM Release 7.0 (ICWC, TREX)
- PO Release 7.0
- BPM (Process Orchestration)

Si sottolinea che le nuove release di SAP si basano tutte sulla piattaforma NetWeaver ovvero una piattaforma enterprise basata sulla *Service Oriented Architecture* (SOA).

Sap NetWeaver integra diverse componenti fra cui l'application server in grado di ospitare sia logica Java secondo lo standard J2EE che logica ABAP SAP proprietaria e il SAP Enterprise Portal tramite il quale è possibile fornire l'accesso al sistema agli utenti interni all'ente.

Oltre al portale è possibile accedere ai vari sottosistemi SAP tramite l'interfaccia applicativa client (SAPGUI 7.30). Tale componente è resa disponibile sui client degli utenti tramite Citrix XenApp. Questa modalità consente di avere una installazione centralizzata della SAPGUI che viene rilasciata in modalità virtuale agli utenti finali.

Qualora una struttura regionale intenda informatizzare un processo integrato, è necessario verificare a priori con il Servizio SIIR la fattibilità attraverso i moduli di SAP.

6.3.2 SAS

E' uno strumento software utilizzato in differenti settori della Regione Emilia-Romagna per l'inserimento, l'aggiornamento, la validazione e l'elaborazione dei dati che costituiscono il patrimonio informativo dell'Ente.

SAS viene utilizzato per realizzare report, tabelle e grafici che possono essere consultati sia via programmi SAS desktop accessibili tramite Citrix che tramite applicativi web; in quest'ultimo caso sono disponibili, sia internamente che aperte al cittadino, pagine statiche, pagine dinamiche navigabili (drill-down), reportistica su richiesta e aree download con archivi di dati e relativi tracciati record e descrizioni delle variabili, dal quale gli utenti possono estrarre direttamente file di dati da usare per ulteriori elaborazioni.

La versione di SAS attualmente installata è la 9.3 che consente una maggiore integrazione con i sistemi di autenticazione adottati dall'Ente e la realizzazione di pagine web con tecnologia Java.

Per la componente Java, SAS si integra con gli application server più diffusi: Tomcat, JBoss, Bea WebLogic.

L'applicazione è una web-application basata sui seguenti moduli:

- Data logic: SAS Scalable Performance Data Server o direttamente file SAS
- Business logic: Servlet Java, che interagiscono con lo SAS Scalable Performance Data Server via JDBC mediante le apposite SAS API for Java, oppure tramite SAS Integration Technologies mediante apposite SAS API
- Presentation logic: è realizzata mediante Java J2EE, pagine html e CSS.

L'applicazione web inoltre sfrutta le SAS Stored Process per la visualizzazione delle tabelle realizzate e per richiamare le stored process si sfrutta la SAS Stored Process Web Application installata su Jboss.

Le componenti SAS 9. 3 attualmente installate sono le seguenti:

Prodotti licenziati e installati su SERVER

- SAS BI Server
- Base SAS Software, incluso SAS Enterprise Guide
- SAS Integration Technologies Software
- SAS/ACCESS Interface to ORACLE Software
- SAS/ACCESS Interface to PC Files Software
- SAS/CONNECT Software
- SAS/GRAPH Software
- SAS/IntrNet Software
- SAS/SECURE for Windows Software
- SAS/STAT Software
- SAS Scalable Performance Data Server

Prodotti licenziati e installati su CLIENT

- SAS Analytics Pro
- Base SAS Software, inclusi i prodotti:
 - SAS/GRAPH Software
 - SAS/STAT Software
- SAS AppDev Studio
- SAS/ACCESS Interface to ODBC Software
- SAS/AF Software
- SAS/CONNECT Software
- SAS/SECURE for Windows Software

6.3.3 SAP NetWeaver Business Warehouse

E' un software di business intelligence per l'analisi, la reportistica e il data warehousing prodotto da SAP AG.

BW è una parte della tecnologia SAP NetWeaver, i componenti inclusi sono:

- Web Application Server (WAS)
- SAP Process Integration e Master Data Management (MDM).

Inoltre comprende strumenti di reportistica per l'utente finale come:

- Report Designer
- BEx Query Designer
- BEx Web Application Designer
- BEx Analyzer.

La versione attualmente utilizzata in Regione è la 7.40.

Il Data Warehouse realizzato in SAP BW è usato per estrarre, aggregare e modellare i dati dal sistema ERP di SAP sottostante e copre attualmente tre ambiti informativi: Bilancio/Contabilità finanziaria, Risorse Umane, Redditi; i vari dati aggregati rappresentano la sorgente delle analisi effettuate da strumenti di reportistica.

Inoltre BW viene utilizzato per il back end di BPC.

6.3.4 SAP BusinessObjects (BO)

E' uno strumento che consente a tutti gli utenti di interagire in tempo reale con le basi dati, analizzare informazioni aggiornate e verificate per tenere sotto controllo i principali indicatori dei processi.

Il sistema BO è utilizzato in differenti settori della Regione Emilia-Romagna come strumento di reportistica, analisi multidimensionale e cruscotti direzionali attraverso interfaccia sia Client che Web.

La versione di Business Objects attualmente installata è la XI r3.1 SP 7, installata in un singolo server dove sono memorizzati in cartelle fisiche l'insieme dei report pubblicati dagli utenti.

Per la loro gestione, ed in particolare per la gestione delle policy e delle impostazioni del sistema, il motore di Business Objects si avvale del repository installato su sqlserver.

La piattaforma di Business Objects XI r3.1 si compone dei seguenti prodotti software :

- Business View Manager
- Central Configuration Manager
- Data Source Migration Wizard
- Universe Designer
- Desktop Intelligence e Web Intelligence
- Diagnostic Tool
- Import Wizard
- Publishing Wizard
- Query As A Web Service
- Query Builder
- Report Conversion Tool
- Software Inventory Tool
- Translation Manager
- Universe Builder
- Web Intelligence Rich Client
- Xcelsius Enterprise per la creazione e fruizione di cruscotti direzionali

Sono presenti anche due applicativi accessibili via web attraverso l'Application Server Apache Tomcat 7.

- BusinessObjects Enterprise Central Management Console
- BusinessObjects Enterprise Java InfoView

I moduli di Business Object sono utilizzati sia direttamente sui sistemi gestionali regionali su cui sono stati sviluppati oltre duecento universi, sia come front end di Data Warehouse.

6.3.5 SAP Business Planning & Consolidation (BPC)

E' uno strumento che consente ad utenti di alto livello di effettuare analisi, simulazioni e permette la realizzazione di sistemi di budgeting e di pianificazione.

SAP BPC è utilizzato in differenti settori della Regione Emilia-Romagna come strumento di simulazione e analisi multidimensionale tramite la sua interfaccia Excel.

Attualmente sono installate due versioni di SAP BPC:

- versione Microsoft: è installata la versione 7.0 SP12, su due server
 - uno per quanto riguarda la parte applicativa
 - uno per quanto riguarda il back-end (DB Microsoft SQL Server)
- versione Netweaver: è installata la versione 7.50.05.

Entrambe le piattaforme si compongono di due parti:

- un'applicazione web, gestita mediante IIS 6.0, che fornisce l'accesso ai Business Process Flow e alle interfacce di amministrazione
- un'integrazione con la suite Office (2003 in su) che permette di interrogare i cubi multidimensionali e di inviare aggiornamenti ai dati stessi.

La parte Microsoft si basa su cubi Analysis Services, alimentati a partire da Data Warehouse già presenti in Regione, mentre la parte Netweaver è alimentata a partire dal SAP Business Warehouse realizzato per la gestione del Personale.

Al 31/12/2015 è stata completata la migrazione alla versione BPC MS 10 (SP 13). L'architettura è composta da due server:

- uno per quanto riguarda la parte applicativa
- uno per quanto riguarda il back-end (DB Microsoft SQL Server 2012)

6.3.6 Oracle Business Intelligence

La piattaforma **Oracle Business Intelligence** è utilizzata in differenti settori della Regione Emilia-Romagna come strumento a supporto delle decisioni che necessitano di analisi e simulazioni sul territorio per poter misurare e stimare tutte quelle attività legate ai servizi, alle infrastrutture e agli asset territoriali in generale. La piattaforma contiene perciò funzionalità evolute per trattare il dato spaziale proveniente dai Sistemi Informativi Territoriali e il dato alfanumerico tipico dei sistemi Business Intelligence classici. Le funzionalità sono relative sia all'integrazione, storicizzazione e analisi del dato all'interno del contenitore di Geo Data Warehouse, che alla fruizione di tali dati tramite cruscotti direzionali con componenti per analisi spaziali multi-dimensionali, simulazioni geo-spaziali.

Il dato viene acceduto tramite interfaccia web integrata con l'autenticazione regionale.

Lo stack tecnologico alla base della piattaforma di Location Intelligence della Regione-Emilia-Romagna è così composto:

- Oracle Business Intelligence Enterprise Edition (OBI EE) 11.1.1.7.0, contenente le seguenti componenti rese disponibili ai fruitori tramite accesso via web:
 - Portale Web Analytics per accesso ai cruscotti direzionali ai decisori
 - Administration Tool per la creazione dello strato dei metadati e del modello multidimensionale
 - Enterprise Manager per le attività sistemistiche di configurazione e manutenzione della piattaforma
- Oracle Database Enterprise 11.2.0.4, con le seguenti opzioni abilitate:
 - Spatial and Graph
 - Partitioning

6.3.7 Spago BI

SpagoBI è la suite di Business Intelligence open source, avente una architettura modulare basata su open standard, impiegata come strumento per la realizzazione di applicazioni di reportistica tradizionale, dashboard e cruscotti direzionali.

SpagoBI è una suite di business intelligence 100% open source sviluppata e gestita dal Competency Center SpagoBI del Gruppo Engineering con codice sorgente residente nel forge di OW2 (consorzio indipendente e organizzazione no-profit).

La suite si compone dei seguenti moduli:

- SpagoBI Server
- SpagoBI Studio
- SpagoBI Sdk
- SpagoBI Application

Il modulo server è una web application che si integra con il protocollo di autenticazione regionale e consente un accesso mediante SSO (single-sign-on) al repository dei documenti analitici realizzati con le seguenti funzionalità :

- Ad hoc query e reporting
- Real Time console
- Static reporting (Birt)
- Olap cubes
- Dashboard
- KPI
- Cruscotti interattivi
- Analisi Georeferenziate
- Data Mining
- ETL

6.3.8 Communication & Document Management Microsoft

Le funzioni di Communication & Document Management tra tutti gli utenti e le organizzazioni regionali sono implementati tramite le tre piattaforme integrate Microsoft SharePoint, Skype for Business ed Exchange.

Skype For Business è la piattaforma di Unified Messaging Microsoft che garantisce le funzioni di comunicazione istantanea, Chat, condivisione desktop, videoconferenza interna e funzioni VOIP integrate con i servizi di telefonia IP regionali. La piattaforma server è federata con nodi esterni accreditati per garantire l'estensione dei servizi Skype anche tra utenti regionali e nodi Skype esterni alla regione. Skype for Business è integrato con la rubrica utenti regionali di Active Directory e con i servizi di posta elettronica Exchange. I servizi di Skype for Business sono utilizzabili anche tramite App da dispositivi mobili.

Exchange è la piattaforma di gestione della posta elettronica regionale. Tramite i Client di Posta elettronica e le app per dispositivi mobili mette a disposizione degli utenti:

- la rubrica di tutti gli utenti regionali;
- le rubriche individuali e di gruppo
- i calendari degli appuntamenti sia individuali che di gruppo

Microsoft SharePoint è la piattaforma server dedicata alla condivisione delle informazioni e dei documenti tra gli utenti del sistema informativo regionale sia tramite cartelle di rete mappate sui singoli posti di lavoro che tramite le interfacce web disponibili sui siti Rerpoint, Alpoint, Mysite e OneDrive. Tramite SharePoint le strutture regionali possono:

- Gestire raccolte documentali personali tramite i siti Mysite e OneDrive;
- Creare e gestire raccolte documentali condivise tramite i siti Rerpoint, Alpoint, Qualità o la loro mappatura sui singoli pc;
- Creare e gestire liste di attività condivise;
- Creare e gestire calendari condivisi, anche sincronizzati con Outlook;

Oltre ai servizi standardizzati, **SharePoint permette lo sviluppo di processi documentali guidati da Workflow** integrabili tramite web services con i servizi resi disponibili dalle diverse piattaforme regionali.

Tramite la piattaforma SharePoint, oltre a gestire tutti i documenti di tutte i servizi regionali, sono stati sviluppati processi specializzati quali:

- Il processo di gestione dei documenti del sistema di qualità ISO 9000
- Il Social Desktop dell'Assemblea legislativa comprensivo del self-provisioning delle raccolte di documenti per ogni struttura;
- Il processo di gestione delle segnalazioni/richieste indirizzate alla redazione di Internos (in corso di rilascio);
- Il processo di gestione delle segnalazioni/richieste relative a quesiti sulla trasparenza (in corso di rilascio);
- Il processo di richiesta, protocollazione e consultazione dei DURC. Il processo è integrato con l'Anagrafe dei Fornitori SAP e con DOCER (in corso di rilascio);

- Il processo di richiesta, registrazione e consultazione dei CIG. Il processo è integrato con l'Anagrafe dei Fornitori SAP (in corso di rilascio);

Le piattaforme sono integralmente amministrate dal SIIR con funzioni di delega di amministrazione alle strutture regionale per la gestione delle profilazioni applicative degli utenti e per garantire la gestione ordinaria delle raccolte documentali.

Qualora una struttura regionale intenda informatizzare un processo sfruttando il process & document management della piattaforma SharePoint e/o integrare una applicazione con i servizi di posta Exchange è necessario verificare a priori con il Servizio SIIR la fattibilità.

L'autenticazione ai servizi SharePoint, Exchange e Skype for Business è trasparente in quanto completamente integrata sia con Active Directory che con i servizi di autenticazione centralizzata. Tutti i servizi sono raggiungibili anche fuori dalla rete regionale previa autenticazione integrata. I servizi sono disponibili sia tramite client tradizionali che tramite interfacce web e/o app per dispositivi mobili.

Al fine di razionalizzare le funzioni di gestione, ampliare gli spazi disponibili sia per la gestione documenti che per la posta elettronica, nonché contenere l'incremento dei costi di storage **è in corso uno studio di fattibilità per trasferire parte dei servizi sul Cloud Microsoft.**

6.4 Tecnologie a supporto delle architetture e filiere applicative

Il Servizio SIIR ha da tempo avviato la realizzazione di una infrastruttura tecnologica centralizzata al fine di conseguire i seguenti obiettivi principali:

- qualità e continuità di erogazione dei servizi da parte delle filiere applicative,
- gestione centralizzata della sicurezza di dati e applicazioni,
- backup e disaster recovery centralizzato per i database e le piattaforme operative,
- presidio specialistico delle filiere applicative,
- politiche di gestione omogenee per tutte le piattaforme hardware / software,
- ottimizzazione e sinergie nell'utilizzo delle piattaforme hardware / software.

Il dettaglio delle tecnologie utilizzate a supporto delle filiere applicative è riportato in [Allegato 2.](#)

6.5 Servizi centralizzati forniti a supporto dei sistemi e delle architetture applicative

Si evidenziano, di seguito, i vantaggi e le peculiarità che la centralizzazione dei sistemi e dei servizi comportano:

Assistenza sistemistica estesa	Il CED regionale garantisce assistenza 5 giorni su 7: dal lunedì al venerdì dalle 08.00 alle 19.
Riduzione dei costi per hardware e licenze	Centralizzando i sistemi diminuiscono i costi di gestione, in quanto si possono ottenere economie di scala sugli aggiornamenti dell'hardware, delle licenze software di base e sulla manutenzione delle apparecchiature
Architettura ridondante	Incremento della disponibilità e della affidabilità dei sistemi con ridondanza di server e storage, normalmente implementata attraverso le architetture tecnologiche del CED
Procedure centralizzate nella gestione dei sistemi	Controllo sulla sicurezza di dati e applicazioni, monitoraggio integrato dei sistemi e delle applicazioni, backup/restore centralizzato, patching periodico dei sistemi server e pianificato del middleware, business continuity, supporto sistemistico tempestivo e specializzato
Gestione centralizzata e governo della spesa su strumentazioni hardware e relativo software di base	E' possibile individuare sinergie e definire strategie di acquisto di beni e servizi condivise e aggregate

La centralizzazione presso la server farm regionale dei sistemi ed applicazioni installati presso altre Direzioni, l'Assemblea legislativa e le Agenzie regionali può avvenire solo se esse rientrano nell'ambito delle infrastrutture e architetture applicative supportate.

6.5.1 Servizi di supporto in fase di progettazione, implementazione e gestione

Il Servizio SIIR, nell'ambito delle architetture applicative prima descritte, fornisce servizi di supporto e system integration durante le fasi di progettazione, implementazione e gestione di sistemi informativi. I servizi forniti sono:

- Installazione, configurazione e gestione delle piattaforme hardware / software di sviluppo, test e produzione
- Monitoring tecnico e applicativo delle piattaforme hardware / software di sviluppo, test e produzione
- Gestione patching, security e business continuity delle piattaforme hardware / software
- Implementazione soluzioni inerenti software di integrazione
- Gestione evoluzione piattaforme hardware / software di sviluppo, test e produzione
- Gestione procedure di backup / restore

- Supporto sistemistico ai gruppi di sviluppo applicativo

Nella Tabella che segue sono elencate nel dettaglio le principali attività operative svolte dal Servizio SIIR a supporto delle filiere applicative.

Fase	Piattaforma	Attività svolte per le 3 filiere applicative supportate
<u>Progettazione</u>	Sistema Operativo	<ul style="list-style-type: none"> • Dimensionamento apparati hardware (storage / CPU / memory / network) • Network planning (assegnazione indirizzi IP privati e pubblici)
	Web Server	<ul style="list-style-type: none"> • Dimensionamento dei web server per gestione traffico utenza • Progettazione security policy
	Application Server	<ul style="list-style-type: none"> • Progettazione architettura clustering orizzontale o verticale • Dimensionamento degli application server
	Database Server	<ul style="list-style-type: none"> • Dimensionamento database server • Progettazione architettura fisica
<u>Implementazione</u>	Sistema Operativo	<ul style="list-style-type: none"> • Installazione e configurazione del sistema operativo • Configurazione servizi di clustering • Configurazione procedure di backup per il sistema operativo • Creazione utenze e configurazione permessi di accesso
	Web Server	<ul style="list-style-type: none"> • Installazione e configurazione dei web server nella rete DMZ • Configurazione procedure di backup e di monitoring dei web server
	Application Server	<ul style="list-style-type: none"> • Installazione e configurazione degli application server • Configurazione procedure di backup e di monitoring
	Database Server	<ul style="list-style-type: none"> • Installazione e configurazione dei database server • Configurazione procedure di backup e di monitoring • Creazione utenze e configurazione permessi di accesso
<u>Gestione</u>	Sistema Operativo	<ul style="list-style-type: none"> • Tuning, monitoring e patching sistema operativo • Verifica backup/restore sistema operativo
	Web Server	<ul style="list-style-type: none"> • Analisi log dei web server nella rete DMZ • Configurazione web server
	Application Server	<ul style="list-style-type: none"> • Deployment e maintenance applicazioni • Analisi log e patching application server • Tuning security, performance tuning e monitoring
	Database Server	<ul style="list-style-type: none"> • Supporto all'implementazione di modifiche evolutive/correttive • Tuning security, performance tuning e auditing dei database server • Verifica backup/restore • Monitoring e patching database server

Si evidenzia che il SIIR, a meno di particolari esigenze opportunamente motivate, non fornisce accesso ai sistemi server di test e produzione ai fornitori esterni.

6.5.2 Policy di patching dei sistemi server

Mantenere i sistemi operativi dei server costantemente aggiornati ha il duplice obiettivo di garantire l'evoluzione dei sistemi operativi nel tempo e di contrastare le vulnerabilità medie o gravi che con frequente periodicità vengono rilevate dai laboratori dei produttori del software.

La policy determina le modalità di attuazione del patching di tutti i sistemi Server regionali su qualsiasi piattaforma e sistema operativo. Questa verte in modo specifico sul patching a livello di "sistema operativo".

La policy si applica a tutti i Server fisici e virtuali localizzati presso il datacenter regionale o delocalizzati presso le varie sedi regionali.

Ogni singolo server è censito su CMDBuild ed ha associato il proprio "responsabile del patching" individuato in fase di attivazione del server stesso.

Per i server operativi in ambiente Private Cloud (descritto al paragrafo 4) è l'operatore IT del "tenant" (struttura regionale cliente del Cloud), a svolgere il ruolo di "responsabile del patching".

A tale responsabile è fatto obbligo di monitorare periodicamente il rilascio di "updates" da parte del produttore del sistema operativo e di applicarli nel rispetto della seguente policy:

1. l'aggiornamento dei server in DMZ deve avvenire con periodicità non superiore ai 30 giorni;
2. l'aggiornamento dei server in rete interna deve avvenire con periodicità non superiore ai 90 giorni;
3. se presenti, l'aggiornamento deve essere svolto prima sui server di test e collaudo;
4. dopo una o due settimane e nessun rilievo di problematiche derivanti dal patching sui sistemi di test, si procede sui sistemi di produzione.

Poiché l'applicazione degli "updates" comporta il riavvio del server, è necessario individuare i momenti della giornata più opportuni per procedere e previa comunicazione dell'impatto sui servizi erogati. La comunicazione può essere indirizzata all'utenza regionale (nel caso di disservizi di ampia portata) o ai referenti applicativi di settore (nel caso di disservizi confinati a specifici ambienti applicativi). In quest'ultimo caso, saranno tali referenti ad avvisare la propria utenza del disservizio.

Normalmente l'applicazione di "updates" sui server applicativi si conclude con la verifica e la conferma da parte dell'area applicativa del corretto funzionamento del servizio.

Si segnala che sono operativi strumenti centralizzati di monitoraggio sui quali sono registrati i server. Tali strumenti si occupano di scaricare gli aggiornamenti (facoltativi e critici) dai

repository esterni e di proporli come disponibili all'installazione.

Gli strumenti ad oggi attivati sono:

- WSUS per i sistemi operativi Microsoft Windows
- RedHat Satellite per le distribuzioni Linux Redhat, CentOS e Oracle Enterprise Linux

Per la distribuzione Linux Ubuntu non sono attualmente implementati repository centralizzati ed il controllo sullo stato del patching viene eseguito su ogni singolo server con la periodicità prima indicata.

Alla fine del processo di aggiornamento è prevista una fase di assessment e reportistica di corretta esecuzione del processo di “updates”.

Reports sullo stato degli aggiornamenti necessari sia per i sistemi server Windows che per le distribuzioni Linux vengono prodotti con periodicità mensile, inviati al responsabile dell'Area Sistemi del SIIR che li comunica ai vari “responsabili del patching” all'approssimarsi del termine ultimo di 90 giorni (per i server in rete interna).

In caso di “updates” di sicurezza ritenuti urgenti da parte del produttore del sistema operativo e tali da risolvere vulnerabilità gravi, l'Area Infrastruttura del SIIR valuta le effettive minacce ed impatti e se è il caso avvia una procedura di urgenza per l'applicazione del patching in tempi brevi e previa comunicazione ai settori informatici dell'Ente ed all'utenza regionale.

6.6 Gestione operativa dei sistemi server e storage

Il processo di consolidamento e razionalizzazione dell'infrastruttura server e storage presso la Server Farm Regionale di sistemi delocalizzati presso alcune Direzioni, l'Assemblea legislativa e le Agenzie regionali, si è concluso.

Tuttavia, ove permangano situazioni di server delocalizzati rispetto al CED per motivi specifici e particolari o perché non candidabili alla centralizzazione, tali sistemi dovranno essere presidiati dal personale tecnico della singola struttura regionale secondo le policy di seguito descritte:

6.6.1 Implementazione di un nuovo sistema server

Di norma non possono essere implementati nuovi server presso le strutture regionali, a meno di esigenze molto particolari e non risolvibili presso il CED.

Nel caso in cui il personale tecnico delle singole strutture regionali, in accordo con i tecnici del SIIR, verifichi la necessità di implementare un nuovo sistema fuori dal CED, tale sistema dovrà essere gestito ponendo attenzione alle seguenti attività (che costituiscono gli step necessari per attivare e gestire in modo puntuale una architettura hardware e software):

Attività di implementazione del sistema operativo:

- Dimensionamento apparati hardware (storage / CPU / memory / network)
- Network planning (assegnazione indirizzi IP privati e pubblici)
- Installazione e configurazione del sistema operativo
- Installazione e configurazione agenti di monitoring e integrazione con l'infrastruttura di monitoring e management regionale

- Configurazione eventuali servizi di clustering
- Configurazione procedure di backup per il sistema operativo
- Creazione utenze e configurazione permessi di accesso
- Integrazione con il sistema antivirus regionale
- Integrazione del sistema nel dominio regionale

Attività di implementazione dell'Application Server:

- Progettazione architettura clustering orizzontale o verticale
- Dimensionamento degli application server
- Installazione e configurazione degli application server
- Configurazione procedure di backup e di monitoring
- Creazione utenze e configurazione permessi di accesso
- Attivazione autenticazione integrata

Attività di implementazione del Database Server:

- Dimensionamento database server
- Progettazione architettura fisica
- Installazione e configurazione dei database server
- Configurazione procedure di backup e di monitoring
- Creazione utenze e configurazione permessi di accesso
- Attivazione autenticazione integrata

6.6.2 Attività periodiche di gestione del sistema server

Attività di gestione inerenti il Sistema Operativo:

- patching periodico (cadenza non superiore al trimestre) del sistema operativo (windows, linux, ecc..)
- Aggiornamento agenti di monitoring
- Verifiche periodiche Backup / Restore sistema operativo
- Monitoring piattaforma operativa (CPU, Memory, Storage, Network)
- Tuning periodico security piattaforma operativa

Attività di gestione inerenti l'Application Server:

- Verifiche periodiche della compatibilità e valutazione necessità di patching application server (es. WebSphere, Jboss, Tomcat,...)
- Verifiche periodiche Backup / Restore application server
- Performance tuning application server (CPU, memory, ecc..)
- Analisi periodica log application server (individuazione errori su servlet, EJB, ecc..)

Attività di gestione inerenti il Database Server:

- Verifiche periodiche compatibilità e valutazione necessità di patching database (Oracle, SQL Server, PostgreSQL, MySQL, ecc..)
- Verifiche periodiche Backup / Restore database
- Tuning security database e gestione grants di accesso ai dati
- Analisi periodica log database
- Performance tuning database server (Memory, CPU, ecc..)
- Delivery periodiche di modifiche evolutive/correttive al database

Il livello di aggiornamento dei sistemi delocalizzati sarà soggetto a verifiche periodiche nell'ambito dei controlli eseguiti da personale specializzato al fine di garantire la security dell'infrastruttura IT dell'Amministrazione e l'aderenza agli standard adottati.

Ove, visto il livello di complessità tecnica delle attività in oggetto, la struttura tecnica delle Direzioni/Agenzie non fosse in grado di operare in autonomia sui server, la struttura sistemistica del Servizio SIIR procederà con la massima tempestività alla dismissione dei sistemi delocalizzati ed alla migrazione delle funzionalità applicative presso i sistemi gestiti centralmente.

6.7 Networking

L'inserimento di nuovi sistemi informatici nella rete degli uffici regionali richiede di identificarne:

- la collocazione più opportuna tra le varie zone di rete gestite (Intranet con IP privati; Intranet con IP pubblici; DMZ; punto d'interconnessione della rete Lepida, Internet, ecc.);
- le esigenze di comunicazione, e con quali prestazioni di banda, con gli utenti interni all'ente Regione, con gli utenti di altri enti che fanno parte della rete regionale, con altri enti pubblici o con il mondo Internet;
- la necessità di realizzare ambiti di rete compartimentati, in cui non sia permesso l'accesso dall'infrastruttura di rete normalmente utilizzata dagli uffici;
- la necessità di usare protocolli di comunicazione particolari, che possono saturare la rete o danneggiare altre applicazioni preesistenti, o creare falle nei sistemi di sicurezza;
- la necessità di accedere a servizi di teleassistenza forniti da aziende che non fanno parte dell'ambito regionale.

Sostanzialmente è indispensabile realizzare uno studio approfondito, in collaborazione con i tecnici esperti in tecnologie di rete che gestiscono la rete regionale, di tutti gli aspetti del progetto che hanno impatto sulla rete locale e geografica.

Ciò va fatto fin dalle fasi iniziali della progettazione del sistema stesso, in quanto le scelte sugli strumenti ed i protocolli utilizzati possono permettere, o al contrario impedire, un corretto funzionamento dell'applicazione stessa o di altre applicazioni d'interesse dell'Amministrazione.

6.8 Wi-Fi

I servizi di accesso a Internet tramite Wi-Fi nelle sedi regionali sono gestiti da Lepida spa.

La rete di hot spot Wi-Fi di Lepida rende disponibili agli utenti tre tipologie di ambiti operativi:

- Free Lepida: rete aperta a chiunque;
- Wisper: rete con accesso libero tramite autenticazione Federa;
- Assemblea: rete privata ad alta velocità dedicata ai dispositivi mobili dell'Assemblea legislativa, previa loro registrazione e certificazione.

Tutte le reti Wi-Fi gestite da Lepida spa non fanno parte della rete intranet regionale.

Per accedere ai servizi della rete intranet regionale gli utenti devono accreditarsi e transitare dal firewall, come chiunque provenga da Internet.

7. Applicazioni e servizi applicativi infrastrutturali

Le applicazioni del sistema informativo regionale che si intendono installare sui server gestiti centralmente dal Servizio SIIR, dovranno rispettare gli standard tecnologici relativi alle filiere applicative supportate descritte al paragrafo precedente.

Tutte le applicazioni (comprese quelle per dispositivi mobili) facenti parte del sistema informativo regionale, anche se in hosting su server esterni, devono rispettare:

- i requisiti di accessibilità definiti dalla Legge Stanca n. 4 del 2004 e dalle relative indicazioni tecniche fornite in successivi decreti presidenziali e ministeriali; in particolare i requisiti tecnici da rispettare e la metodologia da seguire sono indicati nell'allegato A del DM 20/3/2013 (vedi paragrafo **7.3 Accessibilità**).
- le misure minime di sicurezza indicate nel D.Lgs. 196/2003 "Codice per la protezione dei dati personali" e devono essere considerati tutti gli aspetti di sicurezza in ogni fase del ciclo di vita delle applicazioni (vedi paragrafo **7.4 Sicurezza**).

Ogni applicazione deve essere corredata dalla documentazione necessaria all'installazione, alla gestione e manutenzione.

Per le applicazioni che lo necessitano, sono disponibili servizi per l'integrazione con:

- il sistema di gestione documentale,
- l'infrastruttura di firma digitale,
- lo sportello virtuale self-service per la gestione di cicli di approvazione,
- l'organigramma delle strutture e del personale,
- il registro delle imprese (Parix)

Inoltre la Regione Emilia-Romagna, nel contesto del Piano Telematico dell'Emilia-Romagna (PitER), ha promosso la realizzazione di una infrastruttura di cooperazione applicativa per il territorio regionale.

7.1 Documentazione

Di seguito si fornisce un riferimento di contenuti minimi per i principali documenti, di cui un'applicazione *custom* del sistema informativo regionale deve essere corredata. Il dettaglio di ogni singolo documento sarà commisurato alla complessità dell'applicazione. Per i prodotti che prevedono una propria metodologia, quali ad esempio SAP o SharePoint, la tipologia di documentazione va sottoposta per verifica al Servizio SIIR, a garanzia della copertura delle informazioni in essa contenute, necessarie all'attivazione e gestione dell'applicazione stessa.

Analisi dei requisiti: il documento deve contenere l'elenco formale e relativa descrizione di tutti i requisiti dell'applicazione, siano essi funzionali che qualitativi, emersi nella fase di definizione delle esigenze utente.

In particolare, deve contenere:

- definizione del contesto attuale
- descrizione delle esigenze
- vincoli
- requisiti di sicurezza

- numero e tipologia degli utenti coinvolti
- dati trattati, in forma di schema concettuale iniziale
- indicazioni generali della soluzione, sia in termini funzionali che architetturali
- matrice ruoli/funzionalità
- riferimenti a ulteriore documentazione di interesse prodotta o preesistente (esempio: definizione dei requisiti nella documentazione di gara, studi di fattibilità, documentazione a corredo del software originale da assoggettare a MEV, resoconti riunione, ecc.).

Analisi funzionale: il documento definisce totalmente l'applicazione in modo da ottenere una descrizione funzionale completa e non ambigua.

Contiene in modo completo ed esaustivo l'analisi dell'applicazione interessata sia relativamente ai processi ed alle modalità con cui tali processi risulteranno visibili agli utenti finali, sia al disegno logico dei dati secondo il modello relazionale, sia per quanto riguarda gli aspetti non funzionali (architettura, sicurezza, vincoli, prestazioni, ecc.), sia alla documentazione delle interfacce.

In particolare, deve contenere:

- descrizione dell'architettura tecnologica,
- descrizione del sistema di sicurezza da implementare a fronte di un'analisi dei rischi,
- disegno della base dati: schema concettuale definitivo e schema relazionale,
- descrizione della logica applicativa per ogni funzionalità individuata,
- dettaglio schema di navigazione/pagine e/o prototipo interfaccia/maschere,
- eventuali collegamenti con sistemi esterni,
- eventuale descrizione dei flussi di dati previsti dall'applicazione.

Manuale di installazione e gestione: è lo strumento necessario alle strutture preposte all'installazione ed esercizio dell'applicazione. È un manuale rivolto a personale tecnico e deve contenere tutte le informazioni necessarie per installare, configurare e gestire l'applicazione. Possono essere indicati eventuali requisiti particolari di gestione del backup/restore dei dati ed eventuale necessità di un piano di Disaster Recovery, se diversi dalle politiche definite sui server.

Manuale utente: il documento deve fornire una descrizione generale dell'applicazione e una guida operativa all'utilizzo delle singole funzionalità disponibili.

7.2 Sviluppo

Le applicazioni che l'Amministrazione regionale prende in carico sui propri sistemi dovranno essere progettate e sviluppate per:

- essere eseguite in concorrenza (condividendo la stessa infrastruttura tecnologica) con altre applicazioni e quindi non dovranno effettuare operazioni che potrebbero ridurre o bloccare il funzionamento di altre applicazioni e/o servizi;
- poter essere eseguite su application server configurati in cluster;
- poter accedere a database in remoto e configurati in cluster;
- essere esposte tramite un load balancer che funge da reverse proxy e bilanciamento dei nodi application server;

- essere compatibili con le patch e gli aggiornamenti dei sistemi operativi, dei rdbms e application server;
- in caso di utilizzo di componenti sw client, essere aggiornate/compatibili in funzione degli upgrade dei componenti sw presenti sulle postazioni client (ad esempio jvm, etc.);
- essere accessibili secondo i requisiti e la metodologia definiti nell'Allegato A del D.M. 20/03/2013 (vedi paragrafo **7.3 Accessibilità**) e usabili;
- essere sicure tenendo conto degli aspetti tecnici e procedurali definiti nel "Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna", approvato con Determinazione n. 4137 del 2014 (vedi paragrafo **7.4 Sicurezza**).

Nello sviluppo di un'applicazione si raccomanda di prestare particolare attenzione ai seguenti aspetti:

- convenzione per la scrittura del codice;
- documentazione del codice;
- meccanismi di autenticazione centralizzata;
- chiusura delle connessioni al database;
- validazione dell'input e dell'output (lato server);
- gestione e controllo degli errori;
- logging delle transazioni che effettuano chiamate al sistema documentale;
- riutilizzo del codice;
- scalabilità dell'applicazione.

Nel caso in cui si voglia fare uso in un'applicazione di componenti di terze parti occorre verificare con il Servizio SIIR la compatibilità con l'infrastruttura regionale.

In particolare il Servizio SIIR ha definito delle linee guida specifiche per lo sviluppo di applicazioni in tecnologia Microsoft .NET (filiera B) riportate in Allegato 3: è disponibile e documentata una libreria di utility per la gestione della sicurezza, utilizzo del DB server, gestione delle eccezioni, invio di mail, generazione documenti pdf, etc.

Le applicazioni sviluppate nell'ambito della filiera Java, per garantire l'indipendenza dall'application server devono attenersi alle specifiche dettagliate in Allegato 4.

Considerata l'eterogeneità del software di base ed applicativo implementato presso i sistemi informatici dell'Ente è opportuno adottare strumenti che facilitano ed automatizzano sia l'integrazione applicativa sia l'integrazione dei dati; ove si verificano tali esigenze occorre concordare preventivamente con il Servizio SIIR quali strumenti e metodologie adottare in fase di analisi dell'applicazione da sviluppare.

In Regione Emilia-Romagna i sorgenti vengono conservati su repository Subversion (SVN). SVN è utilizzato insieme a Redmine, un sistema di gestione progetti che unisce differenti applicazioni in un'unica interfaccia grafica permettendo una maggiore comunicazione e interoperabilità tra le varie aree di sviluppo di un progetto.

Redmine ha un sistema integrato di bug tracking/gestione dei ticket nonché la possibilità di essere integrato con diversi sistemi di versioning fra i quali SVN e GIT. SVN è il sistema attualmente adottato in Regione ma entro il 2015 verrà adottato anche GIT come sistema di versioning alternativo ad SVN. Maggiori dettagli si possono reperire nell'Allegato 10.

Infine un'applicazione prima di essere installata sui sistemi dell'Ente deve essere opportunamente testata dal fornitore in un ambiente analogo a quello regionale al fine di assicurare:

- il rispetto dei requisiti funzionali concordati con il committente,
- la conformità alla normativa vigente e ai regolamenti/disciplinari/linee guida dell'Ente (accessibilità, usabilità, sicurezza, etc..),
- il corretto funzionamento di eventuali integrazioni con altri sistemi,
- il rispetto dei requisiti prestazionali richiesti (nel caso in cui si prevede che l'applicativo debba essere utilizzato da un numero di utenti elevato prevedere un test di carico).

7.3 Accessibilità

Con il termine “accessibilità” si intende la caratteristica di un sito/applicazione di rendere possibile l'accesso ai suoi contenuti e funzionalità a tutti gli utenti, indipendentemente dalla presenza di disabilità (fisiche, sensoriali, cognitive) e dalle dotazioni hardware e software.

Una pubblica amministrazione deve realizzare siti/applicazioni accessibili: il punto di riferimento normativo è la legge n.4 del 9 Gennaio 2004 "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici" e le relative indicazioni tecniche fornite in successivi decreti presidenziali e ministeriali; in particolare i requisiti tecnici da rispettare e la metodologia da seguire sono indicati nell'allegato A del DM 20/3/2013..

La Legge 4/2004 (nota come “legge Stanca”) obbliga la PA ad inserire nei contratti che stipula con i fornitori di servizi web una clausola per il rispetto dei principi di accessibilità, in caso contrario è previsto l'annullamento del contratto e si incorre in responsabilità dirigenziali e disciplinari.

Inoltre, la Legge 4/2004 impone di considerare anche l'accessibilità nelle procedure per l'acquisto di beni e servizi informatici; chi non lo fa o chi acquista beni/servizi non accessibili deve motivare la scelta.

Quando si scrive un contratto o un capitolato tecnico per un prodotto o Servizio Web (sito, applicazione o CD-ROM/DVD) è quindi necessario inserire una clausola che preveda il rispetto dei requisiti di accessibilità (Allegato 5).

Il rispetto della normativa sull'accessibilità viene richiesto anche ai collaboratori regionali che a vario titolo progettano, realizzano, gestiscono siti e applicazioni web; il responsabile del sito/applicazione è infatti tenuto a rispondere anche del livello di accessibilità e qualità di tale prodotto per quanto di sua competenza.

In Allegato 6 viene riportata la lista dei requisiti che può essere utilizzata per effettuare la verifica di accessibilità su siti o applicazioni web.

Il Servizio SIIR è comunque a disposizione di tutte le strutture regionali (Giunta, Agenzie, Istituti e Assemblea legislativa) per fornire indicazioni tecniche, suggerimenti, supporto in merito.

La Legge 4/2004 non si limita ai siti ed applicazioni internet ma impone il rispetto dell'accessibilità anche per sistemi operativi, applicazioni o prodotti da scaffale, che non utilizzano tecnologie internet.

Anche quando si acquistano beni/servizi di questo tipo pertanto è necessario prevedere nelle procedure di acquisto una clausola sull'accessibilità del prodotto, e in caso contrario motivarne la scelta (Allegato 5).

7.4 Sicurezza

Qualora un sistema informativo tratti dati personali, esso deve essere realizzato assicurando il totale rispetto del D.Lgs. 196/2003 "Codice in materia di protezione di dati personali" (di seguito denominato Codice). Con ciò si intende che il sistema informativo non solo deve assicurare il rispetto di tutti gli obblighi di sicurezza *"in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta"* ma anche il rispetto delle regole ulteriori per i soggetti pubblici.

Il Codice dispone infatti delle regole particolari per il trattamento di dati personali da parte degli enti pubblici non economici, in particolare all'articolo 19.

L'art. 19, infatti, recita:

"Comma 1: Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o regolamento che lo preveda espressamente.

Comma 2: La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata.

Comma 3: la comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o regolamento".

In base a quanto disposto dall'articolo 19, comma 3, quindi, i soggetti pubblici possono effettuare operazioni di diffusione di dati personali diversi da quelli sensibili e giudiziari soltanto se questo è previsto da una norma di legge o di regolamento.

Si sottolinea anche che l'interconnessione tra sistemi telematici di enti diversi, equivale ad un trattamento di comunicazione ai sensi del Codice. E' opportuno quindi che qualora si intenda effettuare diffusione di dati personali di cui la Regione Emilia-Romagna è Titolare (ai sensi dell'art. 28 del Codice), anche attraverso portali gestiti da altri, o si intenda effettuare interconnessioni con sistemi di altri enti, si verifichi preventivamente, ciascuno per la parte di propria competenza e titolarità, la legittimità, la necessità, la pertinenza, la completezza e la non eccedenza rispetto alle finalità per le quali i dati stessi sono stati raccolti e trattati, nonché la legittimità dei trattamenti di diffusione e comunicazione.

La sicurezza dei dati e delle informazioni deve essere poi considerata in ogni fase del ciclo di vita di un'applicazione: dalla progettazione allo sviluppo, dal test alla gestione.

Gli aspetti tecnici e procedurali necessari per progettare, sviluppare, testare e gestire in modo sicuro un'applicazione regionale sono stati definiti nel "Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna", approvato con Determinazione del Direttore Generale all'Organizzazione, Personale, Sistemi informativi e Telematica n. 4137 del 2014.

Le indicazioni in esso contenute si basano sul fondamento che un'applicazione è sicura quando è in grado di preservare confidenzialità, integrità e disponibilità delle risorse, assicurando costantemente:

- l'identificazione dell'utente che accede alle risorse;
- la limitazione degli accessi alle risorse;
- la comunicazione sicura con l'esterno;
- la conservazione sicura dei dati.

Il Disciplinare definisce i principi chiave da rispettare durante la progettazione e lo sviluppo di un'applicazione e contiene inoltre utili liste di controllo che riassumono in modo schematico le indicazioni contenute nel documento.

In particolare ogni applicazione che tratta dati personali, deve rispettare le misure minime di sicurezza, di cui si fornisce in Allegato 7 la lista di controllo.

Quando si scrive un contratto o un capitolato tecnico per l'acquisizione di prodotti o servizi IT è necessario inserire una clausola che preveda la corretta applicazione di quanto previsto dal D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" (si veda l'Allegato 8).

In particolare nel caso in cui la ditta aggiudicataria/contraente:

1. debba trattare dati personali, occorre di norma designare l'aggiudicatario quale responsabile esterno (cfr. Appendice 5 della Deliberazione GR n. 2416/2008) prevedendo nel contratto o capitolato tecnico apposito articolo secondo lo schema scaricabile da Internos nella sezione Privacy/Fac-simili e modulistica,
2. debba adottare misure minime di sicurezza, occorre richiedere il rilascio dell'attestazione di cui al Punto 25 dell'Allegato B al sopra richiamato D. Lgs. 196/2003, secondo lo schema scaricabile da Internos nella sezione Privacy/Fac-simili e modulistica.

I due punti sopra esposti possono coesistere oppure essere alternativi.

7.4.1 Accredimento utenti e servizi di autenticazione Active Directory

La sicurezza dell'intero sistema informativo regionale è garantita dal rilascio di una identità unica digitale per ogni utente autorizzato ad usufruire di uno o più servizi ICT. L'identità unica costituisce il "passaporto" per l'accesso a qualsiasi servizio ICT regionale e garantisce la tracciabilità completa delle attività digitali svolte da ogni utente.

L'identità unica digitale è costituita dallo username unico concesso a seguito di un processo di accredimento tramite riconoscimento "de visu" di ogni utente da abilitare.

La gestione del ciclo di vita dell'identità digitale si basa su un processo costituito da tre componenti:

1. Il processo di riconoscimento, iscrizione e gestione del ciclo di vita anagrafico dell'utente è gestito tramite la piattaforma di gestione delle risorse umane SAP HR e Organigramma a cui è delegata la funzione amministrativa di accreditamento;
2. Il processo di gestione tecnica dell'archivio utenti unici del sistema informativo regionale è delegato al sistema Active Directory suddiviso logicamente in due sottoinsiemi integrati:
 - RERSDM: è l'archivio degli account utenti del sistema informativo regionale abilitabili a servizi sia interni che extranet. L'archivio prevede una particolare qualificazione per gli utenti con diritti di amministratore di sistema;
 - EXTRARER: è l'archivio degli account utenti esterni al sistema informativo regionale abilitati a funzioni di amministrazione di sistemi e/o con diritti di accesso a servizi applicativi;
3. Il processo di sincronizzazione tra la banca dati SAP degli accreditamenti amministrativi e l'archivio digitale degli utenti in Active Directory. Il processo di sincronizzazione permette di riflettere su Active Directory ogni movimento amministrativo riguardante il singolo utente. In particolare:
 - Ogni evento organizzativo che coinvolge una o più strutture (creazione/cessazione strutture/servizi, riorganizzazione) viene riprodotto automaticamente in Active Directory sia dal punto di vista gerarchico (OU) sia nella composizione di gruppi di utenti (Gruppi OG_* e ES_*) la cui composizione è automatica e sempre aderente alla situazione amministrativa;
 - Ogni modifica di relazione tra utenti e strutture si riflette su Active Directory;

Il sistema descritto garantisce pertanto:

- La separazione tra conservazione amministrativa e conservazione tecnica dei dati di accreditamento con la possibilità di ricostruire ogni movimento dei singoli utenti;
- Le identità e gli account costituiti da Username e password di accesso sono direttamente connessi ai dati contrattuali dell'utente, garantendo quindi che ogni variazione contrattuale (spostamento di struttura, cessazione del rapporto di lavoro, cessazione del rapporto di collaborazione, ecc.) venga immediatamente registrato sul rispettivo account di accesso e sulla composizione delle strutture gerarchiche e/o gruppi di Active Directory
- Che ogni servizio applicativo che necessita di integrarsi tramite l'interfaccia LDAP di Active Directory con la struttura organizzativa (organigramma), il ciclo di vita degli utenti o dei gruppi di Utenti risulti costantemente aggiornato, senza interventi manuali, alla realtà amministrativa in movimento.

Gli automatismi di accreditamento utenti sono già applicati per tutte le utenze registrate a qualsiasi titolo nella Banca dati dei rapporti contrattuali e delle relazioni organizzative SAP.

Nell'ambito del processo di certificazione ISO 27001 la procedura di accreditamento amministrativo su piattaforma SAP, già sperimentata in alcune direzioni, dovrà essere estesa anche:

- a tutti gli utenti che non sono registrati nel database del personale (collaboratori esterni, consulenti, ospiti accreditabili. ecc...).

- a tutti gli utenti per i quali vengono richieste credenziali di amministratore di sistema;

Nelle more della conclusione del processo di certificazione ISO 27001 e della standardizzazione e diffusione della procedura organizzativa di registrazione su SAP, le richieste di accreditamento di utenti non presenti sulla banca dati SAP sono regolamentate nel modo seguente:

1. la richiesta di creazione di una identità e del relativo account perviene agli amministratori del dominio (o al personale delegato) dal responsabile (o dal referente informatico) della struttura per la quale il nuovo utente collabora. La richiesta indica anche la data presunta di fine attività, che in ogni caso non può essere superiore a sei mesi;
2. sarà cura dell'utente stesso, avvisato dell'imminente scadenza del proprio account al momento del Log-in, richiedere al proprio referente una proroga per un periodo che non potrà in ogni caso essere superiore a sei mesi.

Le procedure transitorie non sono applicabili per tutte le strutture che hanno adottato il processo di accreditamento tramite SAP.

Al personale regionale in quiescenza che, nei casi previsti dalla normativa, riprenda l'attività lavorativa in qualsiasi forma (volontaria e non), dovranno essere rimodulate tutte le autorizzazioni in funzione delle nuove mansioni e su esplicita richiesta del responsabile della struttura a cui viene assegnato.

I servizi di gestione dell'archivio digitale degli utenti accreditati sono garantiti dalla piattaforma Active Directory.

Active Directory è un ambiente di directory protetto che consente l'autenticazione e l'autorizzazione degli utenti per l'accesso alla rete e alle relative risorse.

Active Directory supporta vari protocolli Internet e meccanismi di autenticazione sicuri utilizzati per la verifica dell'identità al momento dell'accesso, inclusi Kerberos V5, i certificati X.509 v3, le smart card, l'infrastruttura a chiave pubblica (PKI) e il protocollo LDAP (Lightweight Directory Access Protocol) mediante SSL (Secure Sockets Layer).

Oltre a garantire la protezione dell'accesso alla rete mediante l'autenticazione, Active Directory consente di proteggere le risorse condivise semplificando l'autorizzazione degli utenti. Dopo l'autenticazione di un accesso utente in Active Directory, i diritti assegnati all'utente mediante i gruppi di protezione e le autorizzazioni assegnate per la risorsa condivisa determinano se l'utente potrà accedere alla risorsa, e con quali autorizzazioni. Questo processo di autenticazione protegge le risorse condivise da accessi non autorizzati e consente l'accesso solo ad utenti e gruppi autorizzati.

Durante il processo di assegnazione delle autorizzazioni di accesso per le risorse, ad esempio condivisioni file, stampanti, applicazioni e così via, si assegnano le autorizzazioni a un gruppo di protezione anziché a singoli utenti. Questo approccio consente di concedere le autorizzazioni un'unica volta al gruppo, anziché più volte ai singoli utenti. Ogni account aggiunto a un gruppo riceve i diritti assegnati al gruppo in Active Directory e le autorizzazioni sulla risorsa definite per tale gruppo.

Active directory è fonte autoritativa per il sistema di Identity Management: le modifiche fatte sul dominio interno vengono replicate sul sistema di Identity e sui sistemi target ad esso collegati. La gestione degli utenti del dominio Active Directory esterno è spostata sul sistema di Identity che permette un sistema distribuito di delega ai referenti più capillare. Le policy

di gestione dell'utente sono le stesse che erano state impostate per l'Active Directory esterno.

7.4.2 Autenticazione applicativa

Nel caso in cui un'applicazione preveda un meccanismo di autenticazione, è opportuno utilizzare, ove possibile, meccanismi centralizzati, in modo che l'autenticazione non sia parte del codice applicativo ma sia basata su meccanismi dedicati.

Utilizzando sistemi di autenticazione centralizzati si ottiene un doppio vantaggio: l'utente non è costretto a ricordare una nuova userid/password e le policy impostate sui domini comportano l'adempimento di alcune delle misure minime di sicurezza previste dal "Codice in materia di protezione dei dati personali" (D. Lgs. 196/03). In particolare, considerato che tutti i client delle sedi principali della Regione fanno riferimento a un dominio nativo Microsoft Windows 2008 (e sue successive evoluzioni) che certifica tutti gli utenti regionali e che tutti gli utenti sono censiti nel sistema di Identity Management, è possibile utilizzare il sistema di Access Management, il quale permette agli utenti già autenticati sul dominio di accedere senza digitare nuovamente le credenziali (Single Sign On).

Il sistema di Identity & Access Management consente un controllo centralizzato sia nella gestione delle identità che nel controllo degli accessi ai sistemi ed alle applicazioni, migliorando, inoltre, l'usabilità degli stessi da parte degli utenti, in conformità con i requisiti di legge.

Il meccanismo utilizzato dal sistema di Access Management si appoggia su un Directory LDAP che contiene le credenziali degli utenti, che sono le stesse dei domini Active Directory, e su un Policy Server che gestisce il profilo di base dell'utente per l'accesso alle applicazioni. In questo modo ogni utente che si collega all'Access Manager vede solo le applicazioni per le quali è autorizzato ad accedere.

Il Directory è popolato tramite il sistema di Identity Management che, attraverso i suoi meccanismi di delega, permette ai referenti delle applicazioni di gestire in autonomia l'accesso degli utenti alle stesse.

Il sistema di Identity & Access Management si occupa solo dell'autenticazione dell'utente e dell'autorizzazione all'accesso all'applicazione. Le altre autorizzazioni (ad esempio profilature degli utenti, etc...) rimangono a carico dell'applicazione.

La documentazione tecnica di dettaglio con le specifiche per utilizzare il sistema di Identity Management per la gestione centralizzata degli utenti e per utilizzare l'autenticazione dell'Access Management è fornita in Allegato 9.

7.4.3 Autenticazione federata

Nel caso in cui un'applicazione, che preveda un meccanismo di autenticazione, debba essere resa disponibile ad utenti di altri Enti del territorio o a cittadini, è possibile utilizzare il sistema di autenticazione federata (FedERa).

All'interno di fedERa l'identificazione, ovvero il procedimento con cui una identità fisica viene associata ad una utenza, può essere svolto secondo tre modalità:

- **Nessuna identificazione.** Non c'è nessun controllo sulla veridicità dei dati associati all'utenza. Non esiste alcun dato per risalire all'identità dell'utente. Tipicamente l'utente si registra compilando un form web.
- **Identificazione debole.** L'utente dimostra che ha accesso ad una SIM/USIM. Non

c'è nessun controllo diretto sulla veridicità dei dati associati all'utenza, mentre questo è demandato al soggetto terzo che ha rilasciato la SIM/USIM. Viene conservato il numero di SIM/USIM che è stata usata nella procedura di identificazione.

- **Identificazione forte.** I dati degli utenti sono verificati da un operatore che ne controlla la corrispondenza con quelli contenuti in un documento di identità valido presentato dall'utente. I documenti possono essere consegnati di persona, spediti via fax o spediti per posta. I documenti accettati sono Carta di Identità, Passaporto e Patente di Guida. Gli estremi del documento sono annotati ed una fotocopia dello stesso viene conservata. Equivalentemente l'utente si registra al servizio usando una smartcard tipo carta nazionale dei servizi (CNS) o carta di identità elettronica (CIE).

L'autenticazione può avvenire attraverso smartcard CIE/CNS oppure mediante username e password. In quest'ultimo caso, per gli utenti con livello di identificazione forte, sono previsti tre livelli di sicurezza delle password:

- **password minima:** la password deve essere lunga almeno sei caratteri;
- **password per dati personali:** vengono implementate regole di sicurezza delle password che consentono di operare su dati personali ai sensi del D.Lgs 196/2003. In particolare la password deve essere lunga almeno otto caratteri e deve essere cambiata ogni sei mesi;
- **password per dati sensibili:** vengono implementate regole di sicurezza delle password che consentono di operare su dati sensibili ai sensi del D.Lgs 196/2003. In particolare la password deve essere lunga almeno otto caratteri e deve essere cambiata ogni tre mesi.

L'integrazione delle applicazioni con fedERa avviene attraverso il sistema di Access Management, che rende disponibili alle applicazioni federate gli utenti del dominio RERSDM registrati nel database del personale e permette di interfacciarsi con fedERa al fine dell'autenticazione degli utenti esterni.

In fase di integrazione di un'applicazione con fedERa è possibile stabilire il livello minimo di identificazione e di sicurezza degli utenti accettati dall'applicazione.

Il sistema di autenticazione federata si occupa solo dell'autenticazione dell'utente e del rispetto del livello minimo di identificazione e di password policy richiesti dall'applicazione. Le autorizzazioni (ad esempio profilature degli utenti, etc...) rimangono a carico dell'applicazione.

La documentazione tecnica di dettaglio con le specifiche per utilizzare il sistema di autenticazione federata è fornita in Allegato 9a.

Nell'Allegato 15 (capitolo 3) sono dettagliati i livelli di servizio per la fruizione del servizio di autenticazione federata.

7.4.4 Servizio pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)

Lo SPID è istituito a cura dell'Agenzia per l'Italia digitale (AgID) per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità.

I soggetti pubblici o privati che partecipano allo SPID sono:

- a) i gestori dell'identità digitale;
- b) i gestori degli attributi qualificati;
- c) i fornitori di servizi;
- d) l'AgID;
- e) gli utenti.

I gestori dell'identità, degli attributi e i fornitori di servizi dovranno essere qualificati da AgID.

Lo SPID e' basato su tre livelli di sicurezza di autenticazione informatica:

- a. sistema di autenticazione informatica ad un fattore, quale la password;
- b. sistema di autenticazione informatica a due fattori, non necessariamente basati su certificati digitali, quali password e OTP;
- c. sistema di autenticazione informatica a due fattori basati su certificati digitali, quali smartcard.

7.4.5 Cookies

La normativa in materia di protezione dei dati personali e in particolare il Provvedimento del Garante Privacy del 2014 (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884>) prevedono specifici adempimenti per chi utilizza cookies nei siti o applicazioni web. Per i dettagli si rimanda all'Allegato 16.

7.4.6 Monitoraggio

Tra i compiti della gestione operativa del SIIR vi è il monitoraggio dei sistemi e delle applicazioni. Tale monitoraggio di primo livello avviene oggi con lo strumento Open Source ZABBIX.

Al fine di rendere tale monitoraggio più efficace nel controllo della disponibilità delle applicazioni verso l'utenza finale, è richiesto che nelle varie applicazioni avviate in produzione e prese in carico dal CED Regionale sia reso disponibile un link HTTP e/o HTTPS invocabile dal software di monitoraggio al fine di controllare la disponibilità del motore application server e del motore database relativamente all'applicazione installata.

In sostanza il software di monitoraggio deve invocare una funzionalità applicativa neutra ma che accerti il corretto funzionamento del middleware e del database (quindi una funzione che preveda l'autenticazione o applicativa o via sistema IAM unitamente all'esecuzione di una o più query sul database).

Viene lasciato al Team di Sviluppo ideare il tipo di procedura da invocare che può essere più o meno complessa a seconda della profondità dei controlli che si intendono attivare.

7.4.7 Log Applicativi

Al fine di uniformare il formato dei log prodotti dalle applicazioni in filiera A, nell'ottica di migliorare le azioni di troubleshooting e di una futura centralizzazione e aggregazione dei log ad uso anche dei team di sviluppo, è necessario che le applicazioni rispettino i seguenti criteri:

- Le applicazioni devono utilizzare per i propri log il sistema nativo di logging del container poiché questo consente la gestione a caldo della configurazione;

- Ogni applicazione deve produrre un file di log dedicato all'interno del percorso di logging predefinito del container.

Per soddisfare questi requisiti è sufficiente comunicare la categoria e il livello di log nella scheda tecnica di richiesta deploy nuova applicazione riportata nell'allegato 4.

7.5 Elaborazione, esportazione e importazione di documenti in formato aperto

Le applicazioni possono prevedere funzionalità per elaborare, esportare o importare documenti.

Gli utenti delle applicazioni possono essere interni o esterni all'amministrazione (cittadini, imprese, collaboratori, ecc.) e devono poter operare su propri dispositivi senza l'obbligo di sostenere dei costi dovuti al particolare formato in cui i documenti sono forniti o richiesti.

Quando è possibile occorre quindi utilizzare formati standard aperti, scegliendo quelli più diffusi per la tipologia di documenti trattati.

In particolare nei casi di documenti contenenti testi formattati, fogli di calcolo, presentazioni occorre utilizzare:

- HTML (4.0.1 o successivi) per le elaborazioni di documenti web-based;
- PDF per l'esportazione di documenti che richiedono solo lettura o stampa;
- PDF/A¹ per l'archiviazione per l'archiviazione nel lungo periodo di documenti elettronici
- ODF² (1.1 o successive) per l'importazione e per l'esportazione nei casi in cui sia possibile o richiesta un'elaborazione dei documenti. I formati TXT (plain text) e CSV (comma separated value) possono essere utilizzati ma, dal momento che non sono uno standard formalizzato, si consiglia di utilizzarli in aggiunta e non in alternativa ai formati ODF.

Il supporto dei formati elencati deve pertanto essere garantito e verificato:

- Nello sviluppo di applicazioni e nella scelta di applicazioni di terze parti;
- In tutte le suite di produttività d'ufficio e nei servizi in Cloud per garantire l'interoperabilità nell'editing dei documenti;
- In tutte le app che verranno distribuite sui dispositivi mobili;

7.6 Sistema di Gestione Documentale Regionale

Il Sistema di Gestione Documentale Regionale (da ora GDR) è la componente trasversale di base del sistema informativo regionale che, oltre ai servizi di front end, offre una gamma completa di servizi di gestione documentale (ERDMS) ai sistemi applicativi interni.

Il paradigma è stato realizzato nell'ottica della massima astrazione possibile, ovvero prevedendo di mantenersi il più possibile indipendente non solo dai software di base ma anche dai Sistemi verticali di protocollo/registo, costruendo delle interfacce standard sia da che verso il sistema GDR.

¹ Per una più precisa definizione del Formato PDF/A è possibile consultare la voce Wikipedia <https://it.wikipedia.org/wiki/PDF/A>

² ODF prevede le estensioni di file .odt per i testi, .ods per i fogli di calcolo, .odp per le presentazioni. Per una più precisa definizione del formato ODF è possibile fare riferimento alla voce Wikipedia <https://it.wikipedia.org/wiki/OpenDocument>

La concretizzazione di questi principi ispiratori ha portato alla costruzione del sistema **Doc/ER** che eroga uno strato intermedio di servizi documentali per l'archiviazione/indicizzazione dei documenti, per la protocollazione e fascicolazione di documenti, per la gestione dei fascicoli, per la timbratura. Tali servizi sono indipendenti sia dal software di base sottostante sia dai sistemi che erogano ciascuna di queste funzioni ma integrati con questi sistemi in modo trasparente per i sistemi consumer; Doc/er inoltre è integrato in modo trasparente anche con il sistema regionale di conservazione.

Allo stato attuale i servizi Doc/er erogano le seguenti macro funzionalità:

- servizi di gestione dell'intero ciclo di vita dei documenti indipendentemente dal sistema di EDMS sottostante;
- servizio di invio in conservazione automatica dei documenti archiviati all'interno del sistema documentale (al ParER);
- servizi di protocollazione, di repertorizzazione, di fascicolazione dei documenti (richiamando omologhi servizi del protocollo con interfacce standard comuni a tutti i sistemi qualificati Doc/er).

Per la descrizione dei servizi e il loro utilizzo nel contesto della Regione Emilia –Romagna si rimanda all'allegato 18 "*Linee guida per l'integrazione dei sistemi verticali con il sistema documentale regionale*" e alla sezione su Internos "*Il protocollo informatico: il sistema di gestione documentale*" (<https://internos.regione.emilia-romagna.it/sapere-e-fare/funzionacosi/gestione-documentale/il-protocollo-informatico>).

7.7 Firma digitale

In attesa che venga attivata la soluzione di firma digitale remota nel corso del 2016, l'attuale infrastruttura di servizi di firma digitale è basata su un server per la centralizzazione delle funzioni di firma, verifica, cifratura, decifratura e timestamp. Questa infrastruttura è realizzata in ambiente di sviluppo Oracle e Java ed è interfacciabile dalle applicazioni attraverso web services.

La Regione si avvale di un Certificatore accreditato per i servizi di certificazione.

Si elencano in maniera sintetica i servizi disponibili:

- **Firma:** consente la firma digitale di un file o più file, restituendo il file firmato secondo lo standard PKCS#7 (richiede thin client e smart card).
- **Verifica** di un file firmato: consente la verifica della firma apposta ad un file restituendo l'esito della verifica, i certificati dei firmatari e i dati originari recuperati dalla verifica.
- **Cifra:** consente di cifrare un file restituendo un file cifrato secondo lo standard PKCS#7 (richiede thin client).
- **Decifra:** consente di decifrare un file cifrato secondo lo standard PKCS#7 (richiede thin client e smart card).
- **Verifica di una marca temporale:** consente di verificare l'integrità di una marca temporale e di controllare la credibilità e la validità del certificato del firmatario.

- **Firma e verifica di un documento XML:** consente di firmare un file XML nel formato XMLSignature, secondo lo standard: XML-Signature Syntax and Processing. Consente inoltre di verificare l'integrità di un file XML firmato.

I web service sono disponibili ai seguenti indirizzi:

- ambiente di test: <https://firmadigitaletest.ente.regione.emr.it/axis/>
- ambiente di produzione: <https://firmadigitale.ente.regione.emr.it/axis/>

La documentazione completa della libreria è consultabile all'indirizzo <https://firmadigitale.ente.regione.emr.it/doc/> (raggiungibile solo dall'interno della rete dell'ente) oppure può essere fornita su richiesta.

7.8 Organigramma

La banca dati relativa a strutture e personale risiede su SAP HR. Sono state implementate classi .net e servizi web per la consultazione di alcuni di questi dati.

Si elencano in maniera sintetica i servizi disponibili:

- Dettaglio persona: consente di effettuare una ricerca per matricola per reperire i della persona, compresi i dati di assegnazione e responsabilità.
- Dettaglio unità funzionale: consente di effettuare una ricerca per codice unità per reperire i dati dell'unità funzionale.
- Elenca unità funzionale: consente di elencare le unità funzionali secondo diversi criteri.
- Elenca persone assegnate all'unità funzionale: consente di elencare le persone assegnate ad una unità funzionale.

Per la descrizione dei servizi e il loro utilizzo si rimanda all'Allegato 13.

7.9 Workflow di approvazione basati su relazioni funzionali

Al fine di razionalizzare i processi di approvazione di attività e/o sottoporre a firma fasi di processi e/o documenti, le applicazioni regionali dovranno essere integrate con la piattaforma SAP Self Service tramite i servizi offerti dal modulo Universal Work List (UWL).

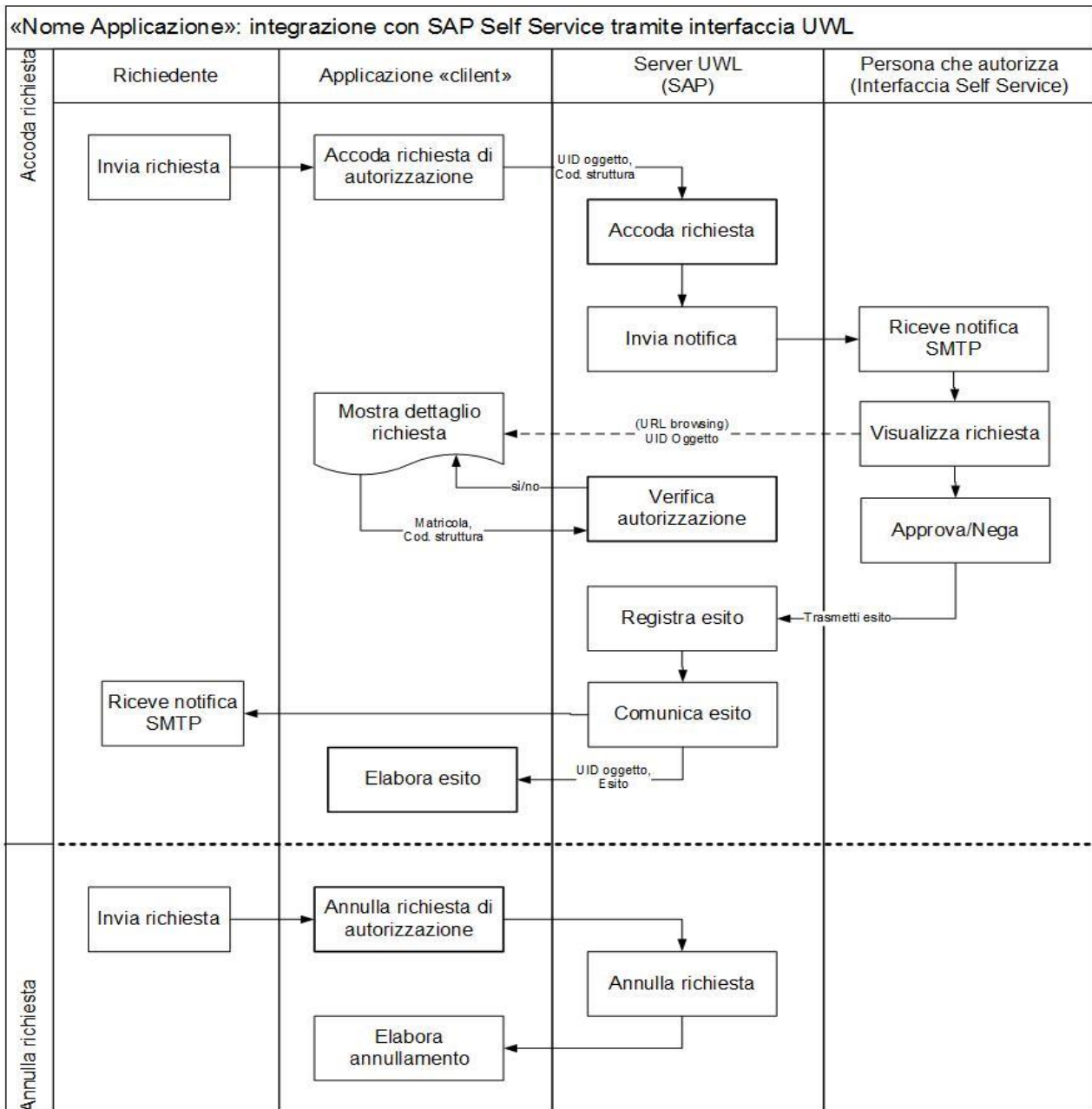
Il modulo SAP UWL garantisce infatti un insieme di funzioni (tasks, alerts, notifications) per interagire con SAP Self Service.

Gli obiettivi di questa linea guida sono finalizzati al riuso di soluzioni già in uso con l'obiettivo di semplificare sia le fasi di sviluppo applicativo che la user experience di chi deve firmare e/o validare documenti, dati o fasi di processo. In particolare la soluzione permette di:

- Evitare di riprodurre all'interno di applicazioni e/o database le relazioni funzionali tra utenti già rappresentate in Organigramma;
- Evitare di riprodurre la movimentazione del sistema gerarchico di rapporti funzionali (in gergo tecnico relazioni Segretaria-Direttore) molto complesso e soggetto a costanti variazioni nel tempo (es. sostituzione di un firmatario durante le ferie, sostituzione di un firmatario con un interim, modifiche organizzative con riallocazione di operatori e/o funzioni in altri servizi);
- Evitare di scrivere nuova interfacce per i cicli di approvazione;

- Concentrare su SAP Self Service tutte la fasi di approvazione di qualsiasi dato, documento e/o fase di processo evitando di disperdere l'attenzione del firmatario già abituato a vistare ferie, permessi, pubblicazioni trasparenza, ecc...;
- Concentrare su un'unica piattaforma l'utilizzo della "Firma Debole" per semplificare l'eventuale passaggio alla "firma digitale remota" quando necessaria e disponibile;

Per la realizzazione di cicli di approvazione che sfruttano l'integrazione tra Sap Self Service (SAP NetWeaver Portal) tramite il modulo Universal Work List (UWL) è necessario contattare il SIIR previa compilazione di uno schema di processo DFD simile a quello riprodotto di seguito.



7.10 Registro imprese locale - Parix

PARIX è la piattaforma di accesso ai dati del Registro delle Imprese, tenuto dalle Camere di Commercio italiane, che mette a disposizione dei servizi applicativi delle Pubbliche Amministrazioni le informazioni aggiornate sulle imprese. I dati, distribuiti in formato XML, sono integrabili con qualsiasi sistema informativo esistente presso la Regione. Inoltre i dati possono essere messi a disposizione delle altre Pubbliche Amministrazioni attraverso l'impiego di una porta di cooperazione applicativa dell'ente stesso.

PARIX - Registro Imprese Locale: l'accesso alle informazioni tramite il "Registro Imprese Locale" consente alla PA di ottenere presso il proprio CED informazioni estratte dalla banca dati del Registro Imprese secondo le sue specifiche esigenze e si configura come un sistema informativo composto da 4 moduli.

PARIX DATA BASE: è il data base che contiene i dati del "Registro Imprese Locale" basato su Oracle e viene alimentato da Xml acquisiti da Infocamere tramite il modulo PARIX DATI. PARIX DATI e DATA BASE assumono il ruolo di archivio di riferimento per tutte le applicazioni e i sistemi informativi specifici della Regione.

PARIX GATE è la componente che realizza la funzionalità di cooperazione applicativa tra le Pubbliche Amministrazioni e consente ad altri enti locali di interrogare, tramite le proprie applicazioni, l'archivio di sintesi integrato con gli altri data base.

PARIX WEB è l'applicazione che consente all'ente di consultare via web l'archivio Registro Imprese Locale.

Per la descrizione dei servizi e il loro utilizzo si rimanda a Lepida, in particolare per richiedere la documentazione tecnica e le credenziali per l'accesso inviare una mail a parixinfo@regione.emilia-romagna.it.

7.11 Cooperazione applicativa

L'utilizzo della cooperazione applicativa nello sviluppo dei sistemi informativi è prescritto dal Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82 e successivi aggiornamenti) e deve avvenire secondo le specifiche del Sistema Pubblico di Connettività e Cooperazione (SPC- SPCoop), esplicitate in particolare nelle regole tecniche e di sicurezza SPC emanate con il DPCM del 1 aprile 2008.

Le specifiche **Sistema Pubblico di Cooperazione (SPCoop)** di AGID definiscono le linee guida per le amministrazioni che vogliono interagire con i sistemi informativi di altre amministrazioni attraverso cooperazione applicativa.

In tali specifiche un **dominio** è definito come il confine di responsabilità di un ente o soggetto amministrativo e racchiude al suo interno tutte le applicazioni da esso gestite. Il confine applicativo del Dominio è rappresentato dalla **Porta di Dominio (PdD)**, attraverso la quale devono transitare tutte le comunicazioni applicative "formali" da e verso il dominio. A livello concettuale la PdD funge da proxy per l'accesso alle risorse applicative che si trovano all'interno dello stesso dominio.

La PdD ha lo scopo di assicurare che lo scambio elettronico di informazioni tra le Pubbliche Amministrazioni abbia le stesse caratteristiche di formalizzazione di quello tradizionale (carta, firma, protocollo, fax...). In questo modo l'amministrazione che invia le informazioni in modo elettronico ad un'altra, sarà garantita del fatto che la destinataria (e non altri) le abbia ricevute, così come la ricevente potrà trattare le informazioni elettroniche ricevute con

pari dignità di quelle che oggi riceve con i metodi tradizionali, considerati fino ad ora gli unici probanti ai fini del procedimento amministrativo. Questo deve essere possibile indipendentemente da come viene realizzata la porta di dominio (fornitore, linguaggi, tecnologia...) in quanto la sua interfaccia è stata definita formalmente.

L'interoperabilità fra amministrazioni deve svilupparsi attraverso le PdD, sulla base di standard definiti a livello nazionale da Agid, in modo tale che:

- siano identificati i servizi ed i dati che ogni amministrazione decide di rendere disponibili sulla rete;
- siano rispettate, per ogni Servizio applicativo esposto, le politiche di sicurezza, di accesso e di controllo di qualità e correttezza dei servizi erogati, stabilite dall'amministrazione erogante.

A livello concettuale **esiste una sola porta per ogni dominio per Ente**. Sono però in via di definizione nuove regole organizzative (da parte di AGID) che prevedono anche aspetti di sussidiarietà in questo ambito.

Per scambiare messaggi applicativi fra PdD viene utilizzata la **busta di eGovernment** che è la definizione del formato di codifica e del contenuto dei messaggi SOAP scambiati tra le porte di dominio. Anche il formato della busta di eGovernment è stato definito da Agid. Attualmente la busta di eGov implementata è la versione 1.1.

Il formato della busta di eGovernment non è "parlato" nativamente dalle applicazioni degli Enti, pertanto la PdD deve anche occuparsi di convertire le richieste applicative nel formato busta eGov. Facendo riferimento a questa problematica, i compiti della PdD vengono solitamente classificati in due componenti: il componente di cooperazione, che riguarda la comunicazione tra le PdD e quello di integrazione, che riguarda la comunicazione tra i Servizi Applicativi dell'Ente e la PdD. Il componente di integrazione si differenzia a sua volta in due diversi moduli: **la porta delegata e la porta applicativa**. In particolare la porta delegata è utilizzata come proxy per l'accesso al Servizio destinazione, mentre la porta applicativa deve essere in grado di gestire la consegna dei contenuti delle buste di eGovernment ricevute al corrispondente Servizio applicativo interno al dominio destinazione.

Lo strumento utilizzato per definire un formato dei dati condiviso tra tutte le amministrazioni, a prescindere dai sistemi "legacy" e dalle basi dati, è XML. SOAP è invece utilizzato come standard per veicolare le informazioni codificate con XML sulla rete Internet, mediante il protocollo HTTP.

Altra "componente" della cooperazione applicativa secondo le specifiche Agid, è l'**Accordo di Servizio**, ossia un documento standard totalmente formalizzato in XML che regola il rapporto erogatore/fruttore di un Servizio applicativo in tutte le parti che lo caratterizzano: l'interfaccia, le modalità di interazione, i punti di accesso, i livelli di Servizio e le caratteristiche di sicurezza previste.

L'Accordo di Servizio ha l'obiettivo di consentire lo sviluppo armonico di un insieme trasparente di relazioni di Servizio. L'inserimento di un catalogo degli Schemi/Ontologie negli Accordi di Servizio consentirà di descrivere la semantica delle informazioni veicolate e dei servizi stessi (ma ad oggi non è ancora disponibile)

AGID, in accordo con le Regioni nell'ambito della Commissione di coordinamento SPC, ha prodotto un set di documenti di specifiche tecniche e organizzative della cooperazione applicativa SPCoop. Questi documenti delineano compiutamente il quadro tecnico-

organizzativo del SPCoop.

Tali specifiche rappresentano il riferimento per i piani di convergenza dei progetti infrastrutturali di cooperazione già realizzati o in corso di realizzazione.

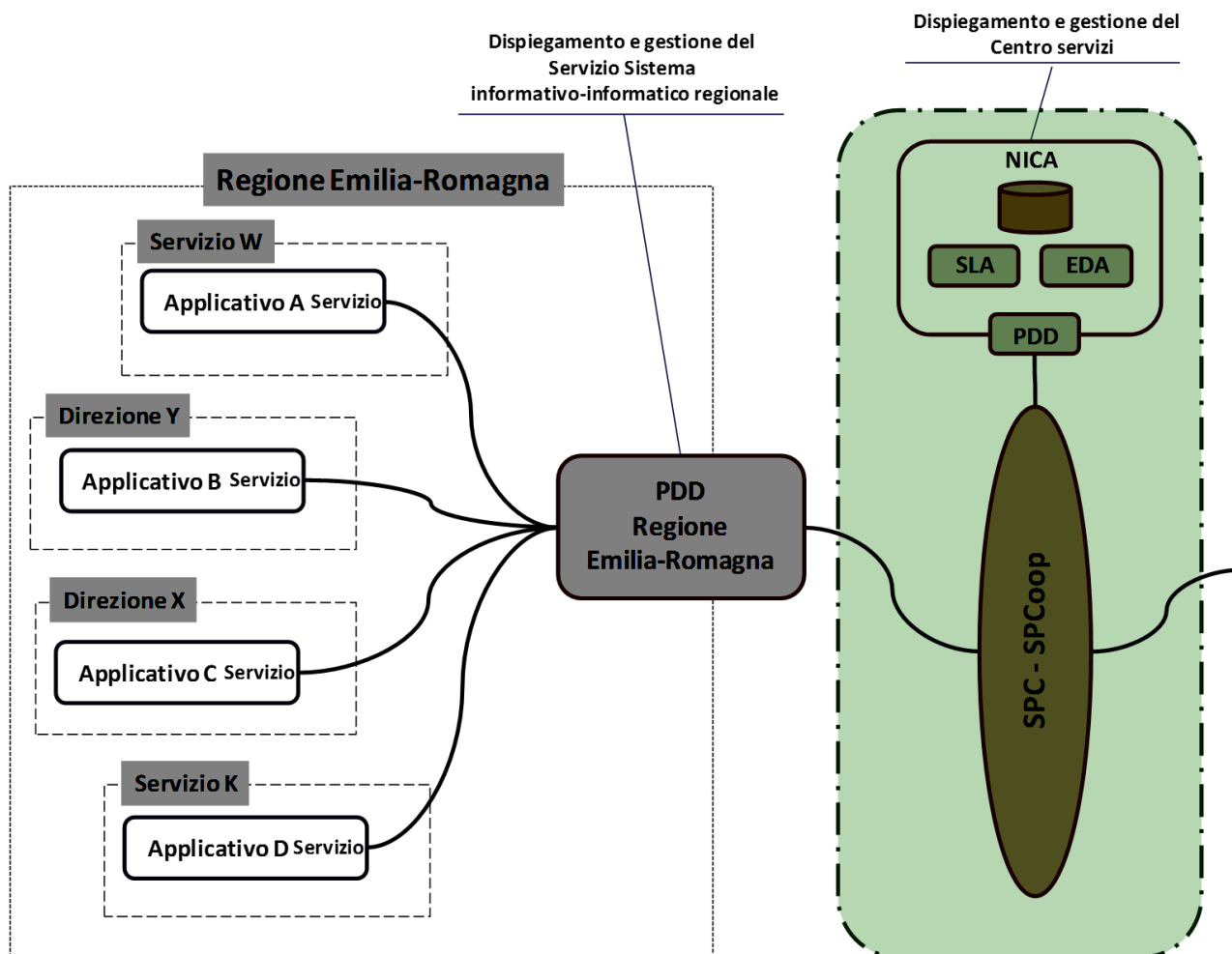
Tra questi progetti il progetto **ICAR** rappresenta il motore della convergenza dei progetti regionali di cooperazione applicativa nel SPCoop.

La Regione Emilia-Romagna, nel contesto del Piano Telematico dell'Emilia-Romagna (PitER), ha promosso la realizzazione di una infrastruttura di cooperazione applicativa per il territorio regionale. Tale infrastruttura è stata denominata ICAR-ER, anche per evidenziare la sua "continuità" con le attività e i risultati ottenuti nel progetto interregionale ICAR.

Le principali componenti della infrastruttura ICAR-ER possono essere così sintetizzate:

1. un insieme di componenti detto Nodo di Interconnessione per la Cooperazione Applicativa (NICA), unico a livello regionale. I principali componenti del NICA sono:
 - una PDD conforme alle specifiche SPCoop per l'accesso ai servizi erogati;
 - un registro dei servizi erogati dagli enti regionali (che può eventualmente fungere da registro SICA di secondo livello), per la pubblicazione degli Accordi di Servizio SPCoop;
 - un Gestore Eventi in grado di supportare comunicazioni di tipo EDA (Event Driven Architecture – Cooperazione ad eventi) a livello regionale ed interregionale;
 - una componente che implementa gli strumenti necessari per il monitoraggio dei livelli di servizio (SLA) dei servizi erogati (modulo infrastrutturale sviluppato nel task INF2 del progetto ICAR).
2. la PDD conforme alle specifiche SPCoop e nativamente integrata con le componenti del NICA suddetto.

Il modello di gestione e manutenzione dell'infrastruttura ICAR-ER di cooperazione applicativa ha visto l'implementazione presso i sistemi del CED regionale della propria PDD su piattaforma Open Source Linux / Jboss / Mysql configurata per colloquiare con il modulo NICA installato presso il Data Center di Lepida SpA ("centro servizi").



In coerenza con il modello SPCoop e con l'infrastruttura ICAR-ER (qualificata da DigitPA a giugno 2011) le applicazioni della Regione Emilia-Romagna che prevedono cooperazione applicativa formalizzata tra Enti dovranno utilizzare detta Porta di Dominio. Il Servizio SIIR e Lepida SpA, a tale scopo, mettono a disposizione il supporto e la documentazione necessaria per la realizzazione di tali integrazioni.

Nell'Allegato 12 sono presenti i moduli che vanno compilati per la richiesta di attivazione di un nuovo servizio tramite PDD (modulo di fruizione e modulo di erogazione) che dovrà essere inviata al SIIR.

Nell'Allegato 15 (capitolo 2) sono dettagliati i livelli di servizio per la fruizione del servizio di cooperazione applicativa.

7.12 Grafica condivisa dei siti web

Per agevolare la navigazione degli utenti all'interno dei siti web regionali e relative applicazioni, è opportuno che le applicazioni destinate alla consultazione web abbiano un aspetto graficamente coerente con quello dei siti da cui vengono consultate. A tale scopo, per ogni sito Plone realizzato dal Servizio SIIR viene predisposto un insieme di files che ne rappresentano la cosiddetta "grafica condivisa", e che possono essere utilizzati secondo le indicazioni tecniche riportate in Allegato 11.

Se si includono dinamicamente i template forniti dal SIIR, le applicazioni saranno sempre aggiornate anche a fronte di modifiche nella linea grafica dei portali web.

Se l'applicazione tratta dati personali o cookies in maniera differente da quanto dichiarato nell'informativa privacy linkata nel footer condiviso, o se i cambiano i Contatti o altre informazioni contenute nel footer del portale tematico di riferimento, sarà necessario definire un footer (e relative pagine) ad hoc per l'applicazione.

8. Applicazioni GIS

Le applicazioni GIS custom del sistema informativo regionale che si intendono installare sui server gestiti centralmente dal Servizio SIIR, dovranno rispettare gli standard tecnologici relativi alle filiere applicative supportate e si dovranno basare su un'infrastruttura cartografica tra quelle dispiegate (vedi paragrafo **6. Architetture applicative**).

Tutte le applicazioni GIS facenti parte del sistema informativo regionale, anche se in hosting su server esterni, devono rispettare i requisiti di accessibilità definiti dalla Legge Stanca n. 4 del 2004 e dalle relative indicazioni tecniche fornite in successivi decreti presidenziali e ministeriali; in particolare i requisiti tecnici da rispettare e la metodologia da seguire sono indicati nell'allegato A del DM 20/3/2013 (vedi paragrafo **7.3 Accessibilità**). Devono inoltre rispettare le misure minime di sicurezza indicate nel D.Lgs. 196/2003 "Codice per la protezione dei dati personali" e devono essere considerati tutti gli aspetti di sicurezza in ogni fase del ciclo di vita delle applicazioni (vedi paragrafo **7.4 Sicurezza**).

E' importante che ogni applicazione GIS sia corredata dalla documentazione necessaria all'installazione, alla gestione e manutenzione (vedi paragrafo **7.1 Documentazione**).

Per garantire la compatibilità e il rispetto della Infrastruttura regionale (e l'omogeneità di crescita di quest'ultima) nella progettazione e nello sviluppo di applicazioni GIS ci si dovrà avvalere della consulenza dei tecnici del Servizio SIIR, scrivendo a GisGovernance@regione.emilia-romagna.it

8.1 L'Infrastruttura di Dati Territoriali

L'Infrastruttura di Dati Territoriali (SDI-Spatial Data Infrastructure) della Regione Emilia-Romagna è costituita dai:

- dati cartografici
- servizi OGC (WMS, WFS, CSW)
- metadati che rispettano lo standard ISO 19115.

La SDI è gestita tramite un catalogo in ambiente "Moka CMS" che organizza i dati secondo la classificazione ISO con una struttura condivisa a livello regionale (vedi Allegato Linee-GuidaCatalogazione_Moka.pdf scaricabile da <http://www.mokagis.it/>) ed alla quale ci si dovrà attenere all'atto della catalogazione; quest'ultima è fondamentale per rendere disponibili a tutti i client della SDI i dati cartografici con i propri attributi descrittivi e con eventuali tabelle associate.

I metadati sono gestiti tramite il "Gestore Catalogo Metadati" che recepisce sia la normativa italiana RNDT sia quella europea INSPIRE.

I due ambienti (catalogo dei dati e catalogo dei metadati) sono facilmente interfacciabili dai client; il primo tramite web service documentati e il secondo attraverso servizi standard CSW 2.0.2.

I dati e metadati sono accessibili tramite il Geoportale che rispetta i requisiti di interoperabilità e la direttiva INSPIRE sulla diffusione dei dati cartografici.

Mediante il Geoportale infatti, i dati sono visualizzabili con mappe interattive, sono scaricabili, in vari formati e sistemi di riferimento, comprensivi dei propri metadati e delle licenze associate (secondo lo standard Creative Commons).

Inoltre possono essere utilizzati con dei servizi web secondo gli standard OGC WMS (Web Map Service) e WFS (Web Feature Service).

8.2 Moka CMS GIS

MOKA è un Content Management System, di seguito definito CMS, di tipo GIS che permette tramite il modulo MokaKit, la gestione della SDI Regionale.

L'attività di catalogazione degli oggetti del CMS (non solo cartografie ma anche funzioni, servizi, template, ecc.) è normalmente svolta dall'amministratore o dai personalizzatori, che utilizzano una componente di Moka denominata MokaKit e/o una estensione appositamente sviluppata per il software ArcGis (ArcMap).

Il modulo MokaKit è stato realizzato con tecnologia web ed è pertanto fruibile (disponendo ovviamente delle necessarie autorizzazioni) in intranet dagli utenti delle strutture regionali ed in extranet dagli enti locali del territorio regionale.

Essendo un CMS, Moka consente ad utenti, che non possiedono conoscenze specifiche di programmazione o di ambienti di sviluppo, di creare interattivamente applicazioni GIS, sia in ambiente web che desktop, utilizzando oggetti organizzati nel catalogo condiviso. Le applicazioni generate con MOKA possono essere rese fruibili da una o più categorie di utenti, interne e/o esterne all'ente.

Tramite il MokaKit è possibile comporre applicazioni da parte di utenti non esperti, utilizzando gli oggetti già catalogati nel CMS. È possibile sviluppare applicazioni per diversi ambienti:

- Web GIS basati sul motore ESRI ArcGIS Server in modalità Web ADF (Application Developer Framework), Flex e Javascript;
- Web GIS con tecnologia Open Layers;
- Mobile per dispositivi con s.o. Android (2.3.3 o sup.) ed IOS (6 o sup.)
- Desktop basati sulla suite ESRI ArcGIS (ArcView, ArcEditor, ArcInfo).

E' inoltre possibile utilizzare il catalogo per accedere alle cartografie della SDI tramite un'estensione Moka per il client gratuito ArcGisExplorer.

Analogamente sul client cartografico Open Source Quantum GIS, è stata sviluppata un'analoga estensione, a partire dalla versione 2.2, che consente l'accesso alle cartografie della SDI che normalmente sono filtrate dal protocollo SDE (proprietario di ESRI)

Il sistema Moka si configura pertanto come strumento per condividere e standardizzare dati ed applicazioni GIS non soltanto per le strutture regionali ma anche per le amministrazioni locali, con particolare riferimento alla Community Network della Regione Emilia Romagna.

Il sistema Moka utilizza gli application server cartografici ArcGIS Server ed Image Server ed è integrato con:

- SigmaTer disponendo di funzionalità che consentono l'accesso diretto (ad utenti abilitati), alle informazioni del censuario consultabili attraverso l'integrazione con le Applicazioni General Purpose (AGP) partendo dalle geometrie delle particelle selezionate. Attualmente l'interrogazione è possibile negli ambienti ADF, Flex ed ArcGisExplorer

- il Sistema di Normalizzazione degli Indirizzi;
- la piattaforma Parix che è la Piattaforma di Accesso al Registro Imprese in formato XML e che consente di realizzare un sistema informativo che integra i dati di impresa presenti nel Registro Imprese Nazionale con i dati di impresa registrati in altri sistemi locali;
- le applicazioni GIS regionali (e di altri Enti) realizzate in ambiente ESRI (desktop o web GIS) o che supportano lo standard WMS.

In ogni nuova applicazione Moka si dovrà sempre fare riferimento, tramite il logo, al sito MokaGIS.

Per l'utilizzo del CMS Moka ci si dovrà rivolgere al "Servizio statistica e informazione geografica" che si farà carico di coinvolgere il SSIIR per verificare l'impatto sui sistemi.

8.3 Il Gestore Catalogo Metadati

Un metadato (dal greco meta "oltre, dopo" e dal latino datum "informazione"), letteralmente "dato su un (altro) dato", è l'informazione che descrive, spiega e colloca una risorsa informativa.

La funzione principale dei metadati è quella di fornire agli utenti le informazioni utili per:

- individuare la presenza di un dato nella SDI;
- conoscere le modalità di accesso e di utilizzo dei dati geografici;
- valutare l'utilizzabilità dei dati in specifici contesti applicativi;
- conoscere i sistemi e le procedure utilizzate per la produzione dei dati;
- conoscere le modalità e la frequenza di aggiornamento dei dati.

Il sistema per la gestione dei Metadati ISO rispetta lo standard ISO19115 per quanto riguarda il modello dei dati e mantiene la compatibilità con le "Linee Guida per l'Applicazione dello standard ISO19115" previste da AGID per il Repertorio Nazionale di Dati Territoriali (RNDT).

Il sistema consente di gestire i metadati di dati geografici e non, rispettando quanto previsto dalla Direttiva INSPIRE (2007/2/EC)

Gli standard e le linee guida implementati sono:

- Lo standard "ISO 19115" per i metadati di dati geografici, in conformità alle Linee Guida "RNDT" (AGID) e le INSPIRE Metadata Implementing Rules
- Lo standard "Dublin Core" (recepito anche come standard ISO 15836:2003) per i metadati di altre tipologie di dati (es. testi, pubblicazioni, ...)
- Lo standard "ISO 19119" che descrive i servizi esposti dall'infrastruttura (web service)

Il Gestore Catalogo Metadati, di cui la regione Emilia-Romagna è dotata consente la gestione e l'aggiornamento di tali informazioni.

8.4 Sistemi di riferimento

Per ciò che riguarda i dati geografici, le applicazioni di tipo GIS e i servizi cartografici esposti, è opportuno definire le regole e le metodologie con le quali devono essere trattati i Sistemi di riferimento.

In particolare:

- viene adottato come Sistema di riferimento geodetico della Regione Emilia-Romagna il Sistema ETRS89 nella realizzazione ETRF2000 all'epoca 2008.0
- nell'ambito dei prodotti cartografici e delle applicazioni GIS, sono adottati: il relativo sistemi di coordinate geografico ETRS89 (codice EPSG:4258) e i relativi Sistemi di coordinate proiettate ETRS89 / UTM Zone 32N e ETRS89 / UTM Zone 33N (rispettivamente EPSG:25832; EPSG:25833);
- per dare pieno supporto al continuo territoriale anche nelle applicazione cartografiche il Sistema ETRS89 UTM Zona 32N (codice EPSG: 25832) è considerato esteso a tutto il territorio regionale, quindi anche all'area territoriale convenzionalmente assegnata al fuso 33;
- i dati geografici pubblicati o resi fruibili tramite servizi, devono quindi essere resi disponibili in ETRS89 o in uno dei relativi sistemi proiettati indicati sopra;
- viene definita una lista dei Sistemi di riferimento e delle loro definizioni che possono essere trattate dalle diverse applicazioni e dai servizi di pubblicazione e per i quali è definita la modalità di conversione da e verso il Sistema di riferimento di cui sopra;
- vengono definite le modalità, i dati e le procedure per la conversione tra i diversi Sistemi di riferimento, che devono essere adottate sia dalle applicazioni GIS lato client/desktop, sia dalle applicazioni lato Server.

Il Sistema di riferimento UTM-ED'50* (o UTMA), per come è originato, non è adeguato a supportare correttamente le conversioni verso ETRS89 e risulta pertanto deprecato. Il sistema di riferimento regionale UTMREER (EPSG:5659), definito a partire dal Sistema di inquadramento originario della CTR 1:5000 regionale, sostituisce il sistema UTMA come sistema di riferimento dei dati pregressi con falsa origine nord di -4.000.000.

Per motivi di compatibilità verso dati e applicazioni esistenti, il Sistema di riferimento regionale UTMREER (ESP: 5659) continua ad essere supportato, pur essendo obsoleto rispetto al Sistema di riferimento geodetico nazionale.

Allo scopo di garantirne la massima fruibilità, i dati pubblicati potranno essere resi fruibili, oltre che in ETRS89, anche in altri sistemi di riferimento tramite opportune conversioni gestite dalla Regione (es: lato server come nei servizi WMS e nei servizi di download del geoportale).

Nell'Allegato 17 e negli ulteriori i documenti di riferimento indicati, vengono illustrate in modo esaustivo le modalità con cui devono essere trattati i Sistemi di riferimento dei dati geografici allo scopo di garantire la necessaria omogeneità e confrontabilità geografica tra i numerosi dati di tipo territoriale trattati in Regione Emilia-Romagna.

8.5 Geoportale

La Regione Emilia-Romagna ha predisposto un canale di diffusione delle informazioni territoriali prodotte: il GeoPortale (<http://geoportale.regione.emilia-romagna.it>).

Il GeoPortale rappresenta il punto di riferimento e snodo della conoscenza "geo-localizzata" regionale sia a supporto delle attività istituzionali delle Amministrazioni Locali che operano a livello regionale che dei singoli cittadini.

La Regione Emilia-Romagna ha realizzato il Geoportale rendendo disponibile il suo utilizzo a tutte le strutture regionali.

Il Geoportale rende possibile la diffusione dei dati cartografici della Regione Emilia-Romagna seguendo gli standard e le direttive europee di INSPIRE adottate anche dal governo nazionale con l'istituzione del Geoportale Nazionale presso il Ministero dell'Ambiente. La direttiva a tale scopo stabilisce "misure in materia di scambio, condivisione, accesso e utilizzo dei dati territoriali e dei servizi relativi ai dati territoriali interoperabili tra i vari livelli dell'amministrazione pubblica e tra i vari settori."

Il Geoportale rispetta anche gli standard standard Open Geospatial Consortium (OGC) e International Standardization Organization (ISO).

8.6 Il Database Topografico Regionale (DBTR)

Il Database Topografico regionale è l'evoluzione della Cartografia Tecnica alle grandi scale che permette di rappresentare gli oggetti rilevanti del territorio tramite una base dati di tipo geografico definita secondo modelli e regole standard condivise a livello nazionale.

Dal 2011, grazie alle attività del progetto PiTER, il Database Topografico Regionale (DBTR) è completamente informatizzato e gestito in modalità cooperativa, con atti di aggiornamento diversificati e continuativi nel tempo.

Il sistema informatico del DBTR è evoluto verso un sistema di fruizione dei dati pienamente integrato nell'infrastruttura geografica regionale, che permette di rendere disponibile agli utenti prodotti e servizi derivate dal DBTR secondo diverse modalità e tecnologie in riferimento gli standard attuali.

Tramite il Geoportale e il portale Open Data i prodotti del DBTR sono distribuiti anche al pubblico con licenze di tipo aperto.

Tra i prodotti/servizi di fruizione disponibili citiamo, oltre ai cataloghi e metadati:

- strati vettoriali del DBTR (layers DBTR)
- strati raster di rappresentazione CTR 5K (DBTR_CTR)
- rappresentazioni WMS/WFS
- servizi di Download dal Geoportale regionale (Shape file e dxf, raster)
- servizi off-line di download tramite archivio (grandi aree e formati diversi) - ESRI Shape, DWG/DXF, Esri Filegeodb, PostGIS
- servizi di immagini Tiled per la rappresentazione su web (mappa cache) stile Google Maps

8.7 Pubblicazione dei dati

La Regione Emilia-Romagna distribuisce i propri dati cartografici, corredati da licenze di tipo aperto, tramite il Geoportale (con i servizi di download sia applicativi sia tramite browser) ed il portale Open Data regionale (dati preconfezionati).

La pubblicazione dei dati cartografici della Regione Emilia-Romagna deve sottostare ai vincoli imposti dalle normative nazionali ed internazionali (direttiva INSPIRE) che impongono la documentazione dei dati medesimi (Metadati). Lo standard da adottare è l'ISO19115 per quanto riguarda il modello dei dati mantenendo la compatibilità con le "Linee Guida per l'Applicazione dello standard ISO19115" previste dall'Agenzia per l'Italia Digitale (AgID, ex

CNIPA) per il Repertorio Nazionale di Dati Territoriali e con quanto previsto anche dall'Implementing Rules di INSPIRE.

Non è quindi possibile pubblicare dati cartografici nel Geoportale mancanti dei relativi metadati.

La Regione Emilia-Romagna mette a disposizione lo strumento Gestore Catalogo Metadati per la creazione e manutenzione dei metadati ed il Geoportale per la loro pubblicazione secondo lo standard OGC Catalog service for the web (CSW 2.0.2).

Tutte le applicazioni che pubblicano dati cartografici devono consentire la consultazione dei relativi metadati. In mancanza di tool specifici è consigliato l'utilizzo dei predetti servizi di catalogo CSW 2.0.2.

Inoltre la distribuzione dei dati cartografici (che ne consentono il download) non è possibile senza l'associazione di almeno una licenza d'uso (Creative Common o Open Data Commons – CC o ODC) specifica per i dati medesimi. Attualmente la versione scelta dalla Regione Emilia-Romagna per gran parte dei dati archiviati nel proprio repertorio è la CC-by 2.5. Si consiglia l'uso di tale tipologia o successive versioni.

Per tutti i dati che rientrano nelle categorie "Reticoli", "Civici" e "Punti fiduciali" la Regione Emilia-Romagna ha associato la licenza non commerciale CC-by NC 2.5. finchè l'uso di tali dati non sarà liberalizzato.

La Regione Emilia-Romagna mette a disposizione uno strumento integrato con il Geoportale per la creazione e gestione delle licenze.

La pubblicazione in qualunque forma e con qualunque applicazione, anche specifica e/o "verticale" (es SentieriWeb) dei dati cartografici presuppone che i medesimi siano anche inseriti e resi disponibili (con i loro metadati ed eventuali licenze per la distribuzione) anche nel Geoportale.

Fanno eccezione quei dati georeferenziati in base all'indirizzo ed utilizzati in applicazioni specifiche (es. Impianti sportivi, Forni a Qualita' controllata, ecc) che possono non essere inseriti nel Geoportale.

Tutte le cartografie dovranno essere inserite in una delle 19 categorie ISO che sono il riferimento del catalogo utilizzato nel Geoportale (vedi Allegato LineeGuidaCatalogazione_Moka.pdf scaricabile da <http://www.mokagis.it/>).

8.8 Servizi cartografici esposti

Nell'ottica INSPIRE il portale, agevola la ricerca dei dati spaziali della Regione Emilia-Romagna attraverso il web, grazie alla presenza di servizi di rete che ne consentono l'utilizzo in molteplici modi, dalla visualizzazione, al download, alle varie trasformazioni. I dati sono facilmente individuabili e adatti ad un uso specifico, facili da capire ed interpretare.

All'interno del GeoPortale sono presenti:

- servizi di ricerca, che consentono di cercare i set di dati territoriali e i servizi ad essi relativi in base al contenuto dei metadati corrispondenti e di visualizzare il contenuto dei metadati;
- servizi di consultazione, che consentono di eseguire almeno le seguenti operazioni: visualizzazione, navigazione, variazione della scala di visualizzazione (zoom in e zoom out), variazione della porzione di territorio inquadrata (pan), sovrapposizione dei set di dati territoriali consultabili e visualizzazione delle informazioni contenute nelle legende e qualsivoglia contenuto pertinente dei metadati;

- servizi per il download dei dati, che permettono di scaricare copie di set di dati o una parte di essi e di accedervi direttamente;
- servizi di conversione, che consentono di trasformare i set di dati territoriali, onde conseguire l'interoperabilità;
- servizi di normalizzazione di indirizzi e di localizzazione.

8.8.1 Il Catalog Service del GeoPortale (Internet)

Il GeoPortale gestisce Servizi di Catalogo dati CSW (Catalogue Service for the Web) consultabili da client esterni in modo automatico.

Il CSW è uno standard OGC che definisce una serie di operazioni che è possibile effettuare sul Catalogo Dati.

Nel caso del GeoPortale Emilia-Romagna sono consentite esternamente solo le seguenti chiamate:

- **GetCapabilities:** consente ai client di recuperare i metadati del servizio da un server. La risposta a una richiesta GetCapabilities è un documento XML contenente i metadati del servizio sul server.
- **DescribeRecord:** permette ad un client di scoprire gli elementi del modello di dati supportati dal servizio di catalogo di destinazione. L'operazione consente di ottenere una risposta che descriva alcune o tutte le informazioni del modello
- **GetRecords:** consente di ricercare i metadati sul server. Tramite opportuni filtri è possibile raffinare la ricerca facendo restituire una risposta con un determinato numero di metadati a partire da una specifica posizione
- **GetRecordById:** consente di recuperare le informazioni di un metadato con un dato identificativo.

Il servizio può essere richiamato con http://geoportale.regione.emilia-romagna.it/rer_csw.

La documentazione tecnica di dettaglio è disponibile sul geoportale (<http://geoportale.regione.emilia-romagna.it/it/services/servizi%20tecnici/servizio-di-ricerca/catalogue-service-for-the-web-csw>)

8.8.2 Servizi di Mappa – consultazione (WMS) e download (WFS) - (Internet)

Sono disponibili i servizi cartografici sul continuo territoriale della Regione Emilia-Romagna in standard ESRI ed OGC in formato WMS (Web Map Service) e WFS (Web Feature Service).

Per quanto riguarda i WMS, gli strati cartografici esposti sono sia dati raster che vettoriali.

Tra i raster troviamo sia la CTR (Carta Tecnica Regionale) 1:5.000 – 1:25.000 – 1:250.000 tradizionale sia quella 1:5.000 derivata dal DBTR2008, le ortofoto AGEA 2008 e 2011, i DTM a 5 e 40 metri ecc.

Tra i vettoriali troviamo il DataBase Topografico(DBTR), i dati degli Usi del suolo ecc.

Nel futuro seguiranno tutti i dati raster e vettoriali prodotti dalla Regione.

Per quanto riguarda i servizi WFS lo standard OGC permette la richiesta e l'importazione da parte di un client di oggetti geografici attraverso il Web, usando chiamate indipendenti dalla piattaforma..

L'elenco dei Servizi esposti è reperibile direttamente nelle pagine del GeoPortale (sezione Servizi – Servizi Tecnici).

Sono state predisposte delle interfacce per il download che, previa autenticazione, consentono sia lo scaricamento dei dati relativi al database topografico sia dei dati più tradizionali. Questi, una volta prodotti off-line, sono inviati direttamente nella casella e-mail dell'utente.

E' presente anche un servizio di estrazione e download dei prodotti cartografici in formato raster.

Il servizio permette, agli utenti registrati, di prenotare un'estrazione dei prodotti raster nei tagli cartografici, selezionando gli Elementi, Sezioni, Tavole e Fogli di interesse, nei formati TIFF nel sistema di riferimento scelto o PDF completi di cartelletta.

8.8.3 Il Servizio di trasformazione coordinate del GeoPortale (Internet)

Il GeoPortale espone il servizio WCTS (Web Coordinate Transformation Service) con un interfaccia basata sullo standard dei Web Processing Service (WPS), che consente un'armonizzazione dei dati attraverso il protocollo standard dettato dall'OGC.

Le interfacce messe a disposizione del servizio sono:

- **GetCapabilities:** fornisce al client le informazioni sui servizi che espone il WPS.
- **DescribeProcess:** istruisce il client su come dover fornire le informazioni per la riproiezione, come fornire il sistema di riferimento dei dati di input, quello dei dati di output, le coordinate da convertire attraverso il protocollo GML (Geography Markup Language), etc.
- **Execute:** avvia lo scambio dei dati tra il server ed il client. Il client invia le coordinate delle geometrie da convertire secondo il protocollo standard, ed il server risponde al client inviando i dati riproiettati.

Il servizio può essere richiamato con http://geoportale.regione.emilia-romagna.it/rer_wcts

La documentazione tecnica di dettaglio è disponibile sul geoportale (<http://geoportale.regione.emilia-romagna.it/it/services/servizi%20tecnici/servizio-di-conversione/web-coordinate-transformation-service>).

8.8.4 API del Geoportale (Internet)

Nel Geoportale all'indirizzo <http://geoportale.regione.emilia-romagna.it/GeoER-API/> sono presenti le GeoER-API a loro volta basate sulle API open source OpenLayers, per la realizzazione di pagine contenenti mappe e servizi della Regione; contiene la documentazione, i test, gli esempi ed un wizard per la creazione di pagine html con mappa e servizi che su di essa insistono.

Le API consentono di creare mappe interattive che insistono sul territorio della regione Emilia Romagna e che interagiscono con i servizi che la stessa Regione mette a disposizione attraverso il Portale.

Sono state estese le applicazioni che è possibile creare tramite il CMS Moka; Moka Kit è ora in grado di generare applicazioni web gis in tecnologia Javascript basate sulle GeoER-API.

Le applicazioni web potranno utilizzare servizi cartografici nei formati OGC WMS, WFS e WCS (ed eventualmente altri formati supportati da OpenLayers come il KML) ed utilizzare funzioni personalizzate costruite sempre sulla base delle API del Portale Geografico, di OpenLayers e di altri strumenti messi a disposizione dalla Regione Emilia-Romagna o da comunità open source.

8.8.5 Normalizzatore (Internet)

Web Service che si propone di fornire una serie di funzioni di normalizzazione di dati relativi ad indirizzi, Comuni e Province.

E' costituito da una serie di procedure in ambiente Oracle PL/SQL che consentono la ricerca e la normalizzazione di toponomastica, località, indirizzi, incroci e luoghi notevoli anche in presenza errori sintattici, e di effettuarne quindi la geocodifica restituendo le coordinate geografiche e cartografiche relative.

La soluzione utilizza una base dati di riferimento che viene aggiornata direttamente dall'infrastruttura geografica (DBTR) tramite opportune procedure di ETL.

Sono disponibili anche delle procedure batch che possono normalizzare in maniera massiva, banche dati che contengono elementi che hanno come riferimento degli indirizzi.

La documentazione tecnica di dettaglio è disponibile su richiesta alla casella GISAdmins@regione.emilia-romagna.it, a cui va inviata anche la richiesta di attivazione di apposite credenziali per l'utilizzo.

8.8.6 Localizzatore (Internet)

Il Localizzatore è servizio web costituito da due componenti ben distinte:

1. un web service REST sviluppato in Java che espone una serie di metodi che permettono una serie di operazioni tra le quali:
 - collegamento a un map server cartografico, ed in particolare navigazione cartografica di base (zoom, pan, scala, accensione e spegnimento layer);
 - collegamento ad un servizio LRS (Linear Referencing System) per la gestione del sistema di interrogazione tramite progressive chilometriche su percorsi dotati di misura, ed in particolare:
 - posizionamento ad una certa coordinata data strada e progressiva;
 - ricavare strada e progressiva data una certa coordinata.
 - collegamento al normalizzatore per la ricerca e localizzazione di indirizzi, incroci, civici;
2. un framework javascript (Localizzatore-API) che estende le GeoER-API e che permette agli utenti di creare mappe interattive dotate di tutte le funzionalità delle GeoER-API, con l'aggiunta di operazioni specifiche per il processo di localizzazione e normalizzazione.

La documentazione tecnica di dettaglio è disponibile su richiesta alla casella GISAdmins@regione.emilia-romagna.it.

9. Siti web

La Regione Emilia-Romagna ha avviato nel 2010 un percorso di riorganizzazione della comunicazione web regionale, descritto nella Delibera di Giunta 1394/2010, con l'obiettivo di razionalizzare e rendere più coerente e funzionale la presenza regionale sul web.

Nell'ambito di questo percorso sono state realizzate le "Linee guida per la comunicazione web regionale", approvate con Delibera 1567/2011, dove vengono illustrate le procedure, gli standard metodologici e comunicativi, i modelli organizzativi, che devono essere applicate a tutti i progetti web dell'Ente, in ciascuna fase del ciclo di vita del progetto (proposta, fattibilità, progettazione esecutiva, realizzazione, gestione e monitoraggio).

In particolare, prima di avviare qualunque progetto di comunicazione web (o prima di realizzare modifiche ai progetti web esistenti) è necessario farne richiesta alla Cabina di regia web allegando uno studio di fattibilità redatto secondo apposito modello, tramite il referente per la comunicazione web della propria struttura.

Nell'ambito della governance del Sistema Informatico Regionale, tutti i siti web devono essere realizzati tramite il sistema di web content management regionale "Plone", gestito direttamente dal Servizio SIIR; eventuali altre modalità di realizzazione vanno motivate e concordate con la Cabina di regia web nella fase di proposta e studio di fattibilità propedeutiche alla progettazione.

Inoltre, per tutti i siti web pubblicati, anche se in hosting su server esterni, valgono le indicazioni fornite al paragrafo **7.3 Accessibilità**, **7.4 Sicurezza**.

Infine, siccome l'Amministrazione mette a disposizione di tutti i settori l'infrastruttura tecnologica necessaria alla gestione di siti web, è opportuno motivare adeguatamente il ricorso a hosting presso aziende esterne.

9.1 Motori di ricerca

Il motore di ricerca è uno strumento che consente di rintracciare le informazioni presenti in un sito web grazie ad una preventiva ed opportuna indicizzazione dei contenuti del sito stesso.

Esistono motori di ricerca pubblici su web, che indicizzano tutti i siti web esistenti e consentono di cercare informazioni tra tutte le risorse web disponibili (Google, Yahoo, Bing,...); inoltre, ogni gestore di siti web può dotarsi di un "motore di ricerca interno" per indicizzare i propri siti e favorire le ricerche all'interno del proprio dominio di riferimento.

Per i siti web della Regione Emilia-Romagna sono disponibili due tipologie di motori di ricerca interni:

- il **motore di ricerca dei siti Plone**, disponibile di norma per tutti i siti web che utilizzano il cms Plone, per effettuare ricerche circoscritte all'interno del singolo sito/portale; il motore di Plone indicizza i contenuti che ha nel suo database, quindi non indicizza applicazioni e banche dati esterne; inoltre, non tiene conto delle indicazioni fornite per i motori di ricerca esterni quali il file robots.txt e i meta tag (index/noindex, follow/nofollow)
- il **motore di ricerca interno della Regione (SOLR)**, tramite il quale vengono indicizzati tutti i siti web regionali (su richiesta), sia interni che presso fornitori esterni, ed eventualmente anche le applicazioni e banche dati (sempre su richiesta, e previa valutazione di fattibilità), e viene usato per effettuare ricerche trasversali nei vari siti della Regione o all'interno di particolari sistemi web

Maggiori informazioni sul funzionamento dei motori di ricerca e come migliorare il proprio "posizionamento" nei risultati delle ricerche sono reperibili nelle "Linee guida per la comunicazione web regionale" (Delibera 1567/2011)

Per attivare l'indicizzazione del proprio sito e per consentire la ricerca all'interno del sito e/o in una sua porzione è indispensabile rivolgersi al Servizio SIIR (a tale scopo consultare il Catalogo dei servizi informatici, <https://rt.regione.emilia-romagna.it/rt/>, alla voce "Utilità web - Motore di ricerca interno su siti o applicazioni web").

9.2 Statistiche di accesso a siti e applicazioni web

Le analisi statistiche dei dati di traffico relativi ai siti internet consentono di determinare il grado di fruizione del sito stesso e forniscono indicazioni preziose per i gestori sulle sezioni da implementare, da potenziare, da rimuovere, sull'efficacia di determinate iniziative di comunicazione, sui visitatori del proprio sito e le loro modalità di navigazione; a tale scopo è necessario realizzare il monitoraggio dei propri progetti web con cadenza almeno semestrale, da condividere con la Cabina di regia web.

Dalle analisi statistiche degli accessi web è possibile monitorare il comportamento del visitatore: quante volte ha visitato il sito, quali sono le pagine che ha visto, il tempo di permanenza in quelle pagine, come è arrivato sul sito, quali sono le keywords (parole chiave) che ha utilizzato per cercarlo con i motori di ricerca, quali sono i percorsi maggiormente utilizzati e quali meno. Queste informazioni risultano estremamente utili al fine di valutare se la struttura delle pagine e la sequenza di navigazione facilitano o scoraggiano il visitatore alla permanenza sul sito e a comprendere quali sono i contenuti ritenuti più interessanti e quindi da valorizzare e quali invece da eliminare o modificare.

In Regione Emilia-Romagna i dati di traffico sui server web regionali vengono elaborati da un programma di analisi statistica degli accessi web (Piwik) che produce appositi report per ogni sito o applicazione web.

L'attivazione dell'analisi statistica degli accessi ad un sito o applicazione va richiesta al Servizio SIIR da parte del responsabile del sito (a tale scopo consultare il Catalogo dei servizi informatici, <https://rt.regione.emilia-romagna.it/rt/>, alla voce "Utilità web - Statistiche web per siti e applicazioni").

Maggiori informazioni sulle attività di monitoraggio dei siti web e sulle analisi statistiche più opportune per ogni tipologia di progetto web sono reperibili nelle appendici delle "Linee guida per la comunicazione web regionale" (Delibera 1567/2011)

10. Servizi e strumenti web già disponibili

Internet ed il web, oltre a contenere pagine informative e documenti da scaricare, possono diventare luoghi di scambio e di lavoro.

A questo scopo, il Servizio SIIR mette a disposizione una serie di strumenti (conformi alla normativa sulla privacy e sull'accessibilità) personalizzabili per le più diverse esigenze, che si consiglia di usare invece di ricorrere a servizi esterni:

1. Iscrizione online a convegni
2. Sondaggi e questionari
3. Groupware (ambienti di lavoro collaborativo)

Per maggiori informazioni su questi strumenti e per richiederne l'attivazione, consultare il Catalogo dei servizi informatici, <https://rt.regione.emilia-romagna.it/rt/>, alla voce "Utilità web".

Inoltre nelle appendici alle "Linee guida per la comunicazione web regionale" (Delibera 1567/2011) sono descritti tutti i possibili strumenti e tipologie di contenuti che si possono attivare di norma in un sito web (es. newsletter, e molti altri).

Procedure

11. Acquisizione di prodotti/servizi IT

Le strutture regionali (della Giunta, delle Agenzie, degli Istituti e dell'Assemblea legislativa) nell'ambito della loro autonomia finanziaria, anche mediante il concorso di fondi non provenienti dal Bilancio regionale, realizzano segmenti del sistema informativo regionale, acquistando prodotti e/o servizi IT.

La Direzione generale competente in materia di sistemi informativi e telematica (nel seguito *Direzione generale SIT*), attraverso queste Linee guida, individua gli standard metodologici e tecnologici di riferimento, a cui le strutture regionali (della Giunta, delle Agenzie, degli Istituti e dell'Assemblea legislativa) dovranno attenersi. Tali Linee guida dovranno quindi essere richiamati nei capitolati tecnici o nei contratti con fornitori terzi o con società in house. Inoltre La Direzione generale SIT ha il compito di effettuare le necessarie verifiche, attraverso le sue strutture.

Le verifiche sono di tre tipologie:

1. **preventive progettuali**: da effettuare sulla documentazione di gara o sul contratto a monte dell'attivazione della procedura di acquisto o dell'affidamento diretto o sulla documentazione tecnica relativa alla convenzione quadro a cui si intende aderire o sul protocollo/convenzione per il riuso;
2. **preliminari alla presa in carico**: da effettuare sulla documentazione tecnica (a valle dell'analisi tecnica se si tratta di sistema informativo), in particolare sui requisiti/fabbisogni hardware e software;
3. **preliminari al rilascio in produzione**: da effettuare a valle dell'acquisizione e dell'implementazione e sono propedeutiche al passaggio in produzione.

L'esito delle verifiche viene espresso attraverso un visto preliminare di riscontro di congruenza tecnica.

E' stata istituita una casella di posta elettronica dedicata, ITgovernance@regione.emilia-romagna.it, a cui inviare comunicazioni relative alle verifiche e/o per chiedere chiarimenti e supporto sia sugli standard sia sulle procedure trattate sul presente documento.

11.1 Verifica preventiva progettuale

Le strutture regionali (della Giunta, delle Agenzie, degli Istituti e dell'Assemblea legislativa) che acquisiscono prodotti e servizi IT, preliminarmente all'adozione degli atti di acquisizione e, in caso di gara, all'invio della documentazione a Intercent-ER, trasmettono al Servizio SIIR per via telematica la documentazione tecnica necessaria alla valutazione. Tale documentazione include, ma non si limita a, i seguenti elementi:

- capitolati tecnici,
- documentazione di prodotto dichiarata dal fornitore,
- documentazione tecnica relativa alla convenzione quadro a cui si intende aderire,
- protocollo d'intesa/convenzione/accordo per il riuso di soluzione software e/o documentazione di prodotto fornita dall'Ente che concede in riuso,
- contratti per il conferimento di incarichi e/o servizi professionali ICT.

11.1.a Espressione visto di riscontro di congruenza tecnica

Il Servizio SIIR è responsabile dello svolgimento delle verifiche preventive progettuali in merito al rispetto degli standard definiti in materia di tecnologie, metodologie di sviluppo e documentazione, livelli minimi di sicurezza e accessibilità, attraverso l'espressione di un visto preliminare di riscontro di congruenza tecnica.

L'espressione del visto avviene:

- a. sui capitolati tecnici per procedure di acquisizione di prodotti software (progetti a corpo), ivi inclusi i siti web e i prodotti multimediali distribuiti su supporto fisico;
- b. sui capitolati tecnici per procedure di acquisizione di servizi di sviluppo e manutenzione;
- c. sulle specifiche tecniche di prodotti software che si intende acquisire nella forma proposta dal venditore, sia in proprietà che in licenza d'uso, onerosa o gratuita;
- d. sui protocolli/convenzioni per il riuso di soluzione software e/o sulle specifiche tecniche di prodotti software proposti e concessi in riuso da altri Enti;
- e. sui contratti per acquisire, tramite affidamento diretto e/o convenzione e/o contratto di servizio, prodotti software o servizi di sviluppo e manutenzione da fornitori specifici o società in house;
- f. sulle specifiche tecniche di apparecchiature hardware che le strutture regionali (della Giunta, delle Agenzie, degli Istituti e dell'Assemblea legislativa) intendono acquisire al di fuori delle procedure generali dell'Ente.

entro un arco temporale che di norma può variare da un minimo di 10 giorni a un massimo di 30 giorni (in funzione della documentazione da visionare) dalla ricezione dei capitolati o delle specifiche oggetto di esame, fatto salvo i periodi di festività natalizie e di ferie estive in cui i tempi di espressione del visto potrebbero subire variazioni che saranno tempestivamente comunicati. L'espressione del visto verrà comunicato per via telematica.

Il visto è necessario per tutte le tipologie di prodotti software e hardware, ad eccezione delle “**piccole periferiche**” quali ad esempio mouse, monitor, pen drive USB, tastiere USB, Hub USB, moduli di memoria RAM aggiuntivi, dischi esterni USB, scanner dotati di programmi di scansione a corredo.

Qualora il visto di riscontro di congruenza tecnica evidenzia carenze o requisiti non rispondenti agli standard definiti, la struttura regionale (della Giunta, delle Agenzie, degli Istituti e dell'Assemblea legislativa) acquirente è tenuta ad adeguare le specifiche secondo quanto indicato dal Servizio SIIR e a richiedere nuovamente la valutazione della documentazione fino a quando non venga formulato un visto di riscontro positivo di congruenza tecnica.

11.2 Verifica preliminare alla presa in carico

Le strutture regionali (della Giunta, delle Agenzie, degli Istituti e dell'Assemblea legislativa) che acquisiscono prodotti e servizi IT o che li realizzano con proprio personale, inviano al Servizio SIIR la documentazione tecnica necessaria alla verifica preliminare alla presa in carico sull'infrastruttura regionale sui requisiti/fabbisogni hardware e software secondo lo schema in Allegato 14. Tale verifica risulta essere propedeutica alla predisposizione degli ambienti, su cui il prodotto hardware e/o software verrà installato, all'interno dell'infrastruttura regionale.

La richiesta di presa in carico dovrà essere registrata sul sistema di protocollo.

11.2.a Espressione visto di riscontro di congruenza tecnica

Il Servizio SIIR è responsabile dello svolgimento delle verifiche preliminari alla presa in carico sui requisiti/fabbisogni hardware e software, attraverso l'espressione di un visto preliminare di riscontro di congruenza tecnica.

L'espressione del visto avviene:

- a. sulle specifiche di realizzazione di sottosistemi informativi realizzati dalle strutture regionali mediante ricorso a specifica gara o ad affidamento diretto;
- b. sulle specifiche di realizzazione di sottosistemi informativi realizzati dalle strutture regionali mediante ricorso a servizi di sviluppo software precedentemente acquisiti;
- c. sulle specifiche di realizzazione di sottosistemi informativi realizzati da personale regionale delle strutture regionali;
- d. sulla documentazione tecnica del prodotto software fornita dal Venditore che lo commercializza o dall'Ente che lo propone in riuso;
- e. sulla documentazione tecnica delle apparecchiature hardware esibita dal fornitore.

entro un arco temporale che di norma può variare da un minimo di 10 giorni a un massimo di 30 giorni dalla ricezione della richiesta corredata della documentazione tecnica (Allegato 14) necessaria alla verifica, fatto salvo i periodi di festività natalizie e di ferie estive in cui i tempi di espressione del visto potrebbero subire variazioni che saranno tempestivamente comunicati. L'espressione del visto verrà registrato sul sistema di protocollo.

Qualora il visto di riscontro di congruenza tecnica evidenzia carenze o requisiti non rispondenti agli standard definiti, la Direzione generale acquirente è tenuta ad adeguare le specifiche secondo quanto indicato dal Servizio SIIR e a richiedere nuovamente la valutazione della documentazione fino a quando non venga formulato un visto di riscontro positivo di congruenza tecnica.

Solo in seguito ad una valutazione positiva la Direzione generale acquirente potrà procedere nell'implementazione del sistema secondo le specifiche approvate e il Servizio SIIR potrà procedere nella predisposizione degli ambienti, su cui il prodotto hardware e/o software verrà installato, all'interno dell'infrastruttura regionale al fine di effettuare i necessari collaudi.

11.3 Verifica preliminare al rilascio in produzione

Le strutture regionali (della Giunta, delle Agenzie, degli Istituti e dell'Assemblea legislativa) che acquisiscono prodotti e servizi IT o che li realizzano con proprio personale, effettuato il collaudo funzionale del sistema, inviano per via telematica (attraverso la casella di posta ITgovernance@regione.emilia-romagna.it) al Servizio SIIR la richiesta di rilascio in produzione abilitando all'accesso il/i referente/i incaricato/i di effettuare le verifiche e fornendo le indicazioni e i chiarimenti che dovessero essere necessari, nonché tutta la documentazione relativa al sistema da attivare in produzione (in caso di software basarsi sullo schema dell'Allegato 14).

11.3.a Espressione visto di riscontro di congruenza tecnica

Il Servizio SIIR è responsabile dello svolgimento delle verifiche preliminari al rilascio in produzione di prodotti e sottosistemi realizzati da terzi, sul rispetto degli standard definiti in

materia di tecnologie, metodologie di sviluppo e documentazione, livelli minimi di sicurezza e accessibilità, attraverso l'espressione di un visto preliminare di riscontro di congruenza tecnica.

L'espressione del visto avviene:

- a. sul rispetto degli standard definiti (filieri applicative, documentazione, sviluppo), per i prodotti ospitati sui sistemi regionali;
- b. sugli aspetti inerenti la sicurezza (analisi dei rischi, meccanismi di sicurezza implementati, misure minime di sicurezza qualora il sistema tratti dati personali);
- c. sugli aspetti inerenti l'accessibilità (rispetto dei criteri di accessibilità secondo i requisiti e la metodologia definiti dalla Legge n. 4 del 9 Gennaio 2004 e nell'Allegato A del D.M. 20/03/2013 (vedi paragrafo 7.3 Accessibilità))
- d. se pertinente, sugli aspetti inerenti l'integrazione con il sistema di gestione documentale doc/er (rispetto delle "Linee guida per l'integrazione dei sistemi verticali con il sistema documentale regionale")
- e. sugli aspetti di performance valutando caso per caso, ed in funzione delle caratteristiche dell'applicazione stessa, l'opportunità dell'esecuzione dei test di carico prestazionali;
- f. sulla congruenza delle apparecchiature hardware con l'infrastruttura regionale preesistente.

entro un arco temporale che di norma può variare da un minimo di 10 giorni a un massimo di 30 giorni dalla ricezione della richiesta di rilascio in produzione corredata della documentazione tecnica e delle abilitazioni necessarie alla verifica, fatto salvo i periodi di festività natalizie e ferie estive in cui i tempi di espressione del visto potrebbero subire variazioni che saranno tempestivamente comunicati. L'espressione del visto verrà inviata per via telematica attraverso la casella di posta ITgovernance@regione.emilia-romagna.it..

Qualora il visto di riscontro di congruenza tecnica evidenzia carenze o requisiti non rispondenti agli standard definiti, la struttura regionale acquirente è tenuta ad adeguare il sistema secondo quanto indicato dal Servizio SIIR e a richiedere nuovamente la valutazione fino a quando non venga formulato un visto di riscontro positivo di congruenza tecnica.

12. Gestione Servizio Applicativo

Con il termine Gestione Servizio Applicativo si intendono tutte le attività di avvio di un servizio applicativo, di evoluzione e terminazione dello stesso. Esse riguardano in parte tutti quegli aspetti di "confine" tra le attività di sviluppo e le attività di esercizio a regime, ma soprattutto le attività di presa in carico, valutazione di impatto, predisposizione ed evoluzione delle tecnologie a supporto, aggiornamento operativo dell'applicazione, verifica del corretto funzionamento, performance tuning ed asset management (manutenzione dell'anagrafica degli Asset sul CMDB adottato dal SIIR: CMDBuild).

Gli obiettivi di questa attività sono:

- garantire la presa in carico di un servizio applicativo (già sviluppato) integrando e coordinando le attività dei team di sviluppo e dei team di esercizio;
- garantire le normali evoluzioni del servizio applicativo (nonché la terminazione) legati ad eventi tipicamente di MEV e/o MAC;

- predisporre i sistemi e formare l'organizzazione per l'erogazione delle attività

I processi individuati per l'attività "Gestione Servizio Applicativo" sono riepilogati nella tabella seguente:

Processo	Denominazione	Obiettivo
SIIR-SYS-App-01	Presa in carico, verifica ed avviamento di un servizio applicativo	Predisposizione e validazione dell'infrastruttura per l'erogazione del servizio applicativo
SIIR-SYS-App-02	Evoluzione di un servizio applicativo	Mantenimento dell'efficienza del servizio a fronte di evoluzione del servizio stesso
SIIR-SYS-App-03	Terminazione del servizio applicativo	Sospendere, archiviare le componenti del servizio in uno stato coerente e rilasciare le componenti tecnologiche per il riutilizzo in altri servizi

Per ognuno dei processi sotto descritti è elaborata la matrice RACI per definire ruoli e responsabilità nell'esecuzione delle attività. Si ricorda che l'acronimo RACI corrisponde a:

- **R – Responsible**, chi deve svolgere il lavoro e portarlo a termine.
- **A – Accountable**, chi è in ultima analisi effettivamente responsabile del raggiungimento dell'obiettivo di quella attività. Chi deve validare in ultima istanza, il lavoro svolto dal responsabile sopra descritto.
- **C – Consulted**, persona che deve essere consultata e con la quale ci deve essere uno scambio di opinioni rispetto a quel task, in quanto particolarmente interessata o qualificata in quell'area.
- **I – Informed**, coloro i quali devono essere informati sull'esecuzione delle attività correlate.

12.1 SIIR-SYS-App-01, presa in carico e avviamento di un servizio applicativo

Il processo è costituito dall'insieme delle attività di predisposizione dell'ambiente di esercizio, dell'infrastruttura di gestione e di avviamento iniziale del servizio in produzione.

La componente applicativa del servizio può essere implementata dalle strutture di sviluppo interne alla Regione o essere una componente acquisita dall'Ente presso un fornitore esterno o nell'ambito delle politiche di riuso. Al termine delle attività il servizio applicativo è in esercizio, CMDBuild risulta aggiornato con le informazioni necessarie alla gestione del nuovo servizio e le strutture preposte all'erogazione sono state adeguatamente istruite per essere in grado di governarlo tramite il rilascio di una documentazione operativa. Mentre ai team di sviluppo viene consegnato un rapporto di presa in carico.

L'area applicativa, per avviare l'implementazione di un nuovo servizio applicativo, deve avere ottenuto riscontro positivo alla presa in carico (vedasi paragrafo 11) da parte dell'Area IT Governance del SIIR, deve fornire alle aree tecniche del SIIR, *in primis* all'Area Sistemi e Sicurezza, la documentazione tecnica necessaria per la configurazione, il dimensionamento e la predisposizione degli ambienti di test, collaudo (se previsto) ed esercizio.

Per prendere in carico un nuovo servizio è necessario che sia predisposta l'infrastruttura di esercizio in tutte le sue componenti: hardware e software di sistema, software applicativo, sistema di gestione e sistema di monitoraggio. È quindi necessario che l'intera configurazione sia collaudata e che venga effettuato il passaggio di consegna al team di gestione per l'esercizio.

Per fare ciò è necessario prevedere una serie di attività relative alla verifica dell'impatto che tale cambiamento apporta al sistema complessivo. Queste attività normalmente fanno parte della progettazione del servizio e comportano l'identificazione delle specifiche architetture, di monitoraggio e di test. Se le specifiche del nuovo servizio non risultano aderenti agli standard ed alle filiere definite, ritornano alle strutture di sviluppo o ai fornitori terzi per le necessarie integrazioni.

Le attività effettuate nell'ambito della **gestione del rilascio** assicurano non solo che tutte le componenti del sistema siano predisposte secondo quanto definito nella fase di progettazione, ma soprattutto che l'infrastruttura di erogazione sia configurata per poter esercire il servizio secondo le caratteristiche attese. Per punti le attività riguardano:

- l'allestimento dell'ambiente di test, collaudo (quando richiesto) e di esercizio: Server, storage, software di base, software applicativo, base dati e popolamento iniziale;
- l'allestimento dell'ambiente di monitoraggio mediante la predisposizione e la configurazione delle regole di monitoraggio specifiche;
- l'allestimento dell'ambiente di gestione con: la parametrizzazione del monitoring, la registrazione dei CI (Configuration item) su Cmdbuild, l'acquisizione delle informazioni di ulteriori informazioni necessarie per la gestione del servizio ed il passaggio di consegne alle strutture operative;
- il collaudo di tutta l'infrastruttura predisposta prima di avviare il servizio in esercizio.

Di seguito si descrive graficamente il processo di **avvio di un nuovo servizio applicativo** sui sistemi del Datacenter regionale:

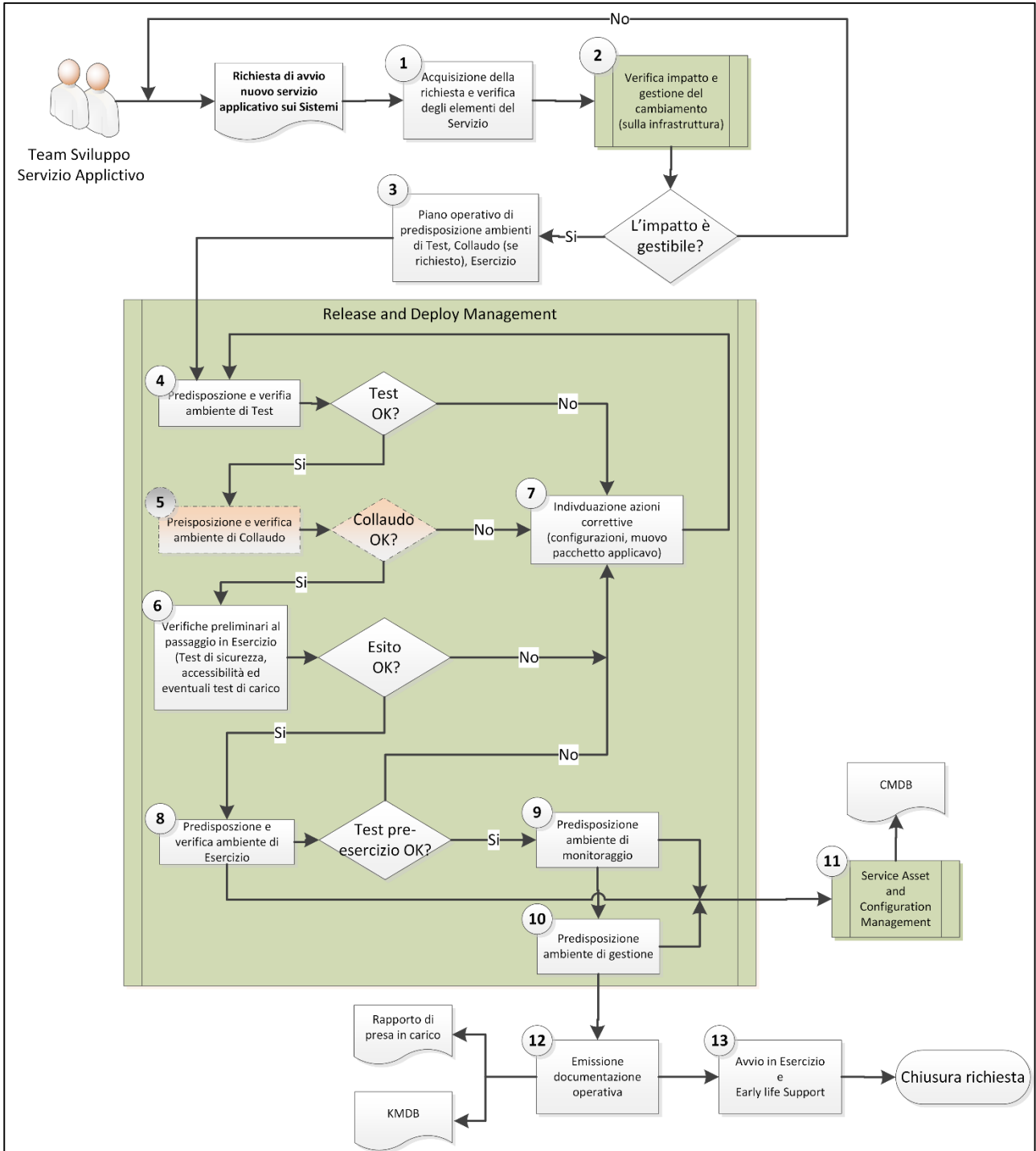


Tabella RACI:

	Service Desk	Area Client	Area Sistemi	Area Dominio e IAM	Area Sicurezza	Area Reti	Area Governance	Area Applicativa
Attività 1			AR	C	C	C	I	
Attività 2		C	AR	C	C	C		C
Attività 3		I	AR	I	I	I		I
Attività 4			R	R	R	R		A
Attività 5			R	R	R	R		A
Attività 6			C	C	R		A	C
Attività 7			R	R	R		I	AR
Attività 8			R	R	R	R	I	A
Attività 9		C	AR	C	C	C		C
Attività 10		C	AR	C	C	C		C
Attività 11		R	R	R	R	R	C	A
Attività 12		R	R	R	R	R	I	AR
Attività 13	I	R	R	R	R	R	I	AR

12.2 SIIR-SYS-App-02, evoluzione di un servizio applicativo

L'evoluzione del servizio applicativo è il processo relativo alla gestione dei cambiamenti indotti al servizio che comportano l'aggiunta di nuove funzionalità (nuove release), a fronte di nuove esigenze applicative, o la correzione/revisione di alcune logiche di funzionamento, o addirittura il cambiamento della configurazione di esercizio (di sistema), a fronte ad esempio di un aumento del numero di utenti del servizio.

L'obiettivo del processo è il mantenimento dell'efficienza nell'erogazione del servizio applicativo.

L'area applicativa, a fronte di una richiesta di evoluzione del servizio deve prevedere una serie di attività relative alla identificazione delle modifiche da approntare e dell'impatto che tale cambiamento determinerà nella sua erogazione. Il risultato del processo può comportare la messa in esercizio delle modifiche evolutive e correttive, o riguardare la revisione della configurazione dell'ambiente di esercizio (es. potenziando le risorse elaborative della catena tecnologica per aumentarne le capacità di erogazione), o determinare l'aggiornamento del middleware su cui è in esecuzione l'applicazione.

L'area applicativa, realizzata la nuova release del software o individuata l'esigenza di una revisione infrastrutturale, avvia il processo di aggiornamento del servizio applicativo indirizzando la richiesta a due interlocutori differenti secondo la seguente casistica:

1. Area Sistemi del SIIR (nelle modalità di dettaglio descritte in allegato 4a) nei casi in cui si tratti di modifiche di basso o medio impatto sulla struttura, sulle logiche e sulle funzionalità applicative (già analizzate in fase di verifica preliminare al passaggio in produzione).
2. Area IT Governance (nelle modalità descritte nel paragrafo 11) nel caso di evoluzione importante (aggiunta di moduli funzionali, revisione sostanziali delle logiche applicative) del servizio applicativo. In tali casi risulta evidente che prima deve essere eseguito un Regression Test da parte dell'area applicativa.

Comunque è lasciata all'area applicativa la responsabilità di valutare se le modifiche evolutive apportate necessitano di un nuovo test di sicurezza, accessibilità o di carico.

Di seguito si descrive graficamente il processo di **gestione dell'aggiornamento di un servizio applicativo** sui sistemi del Datacenter regionale:

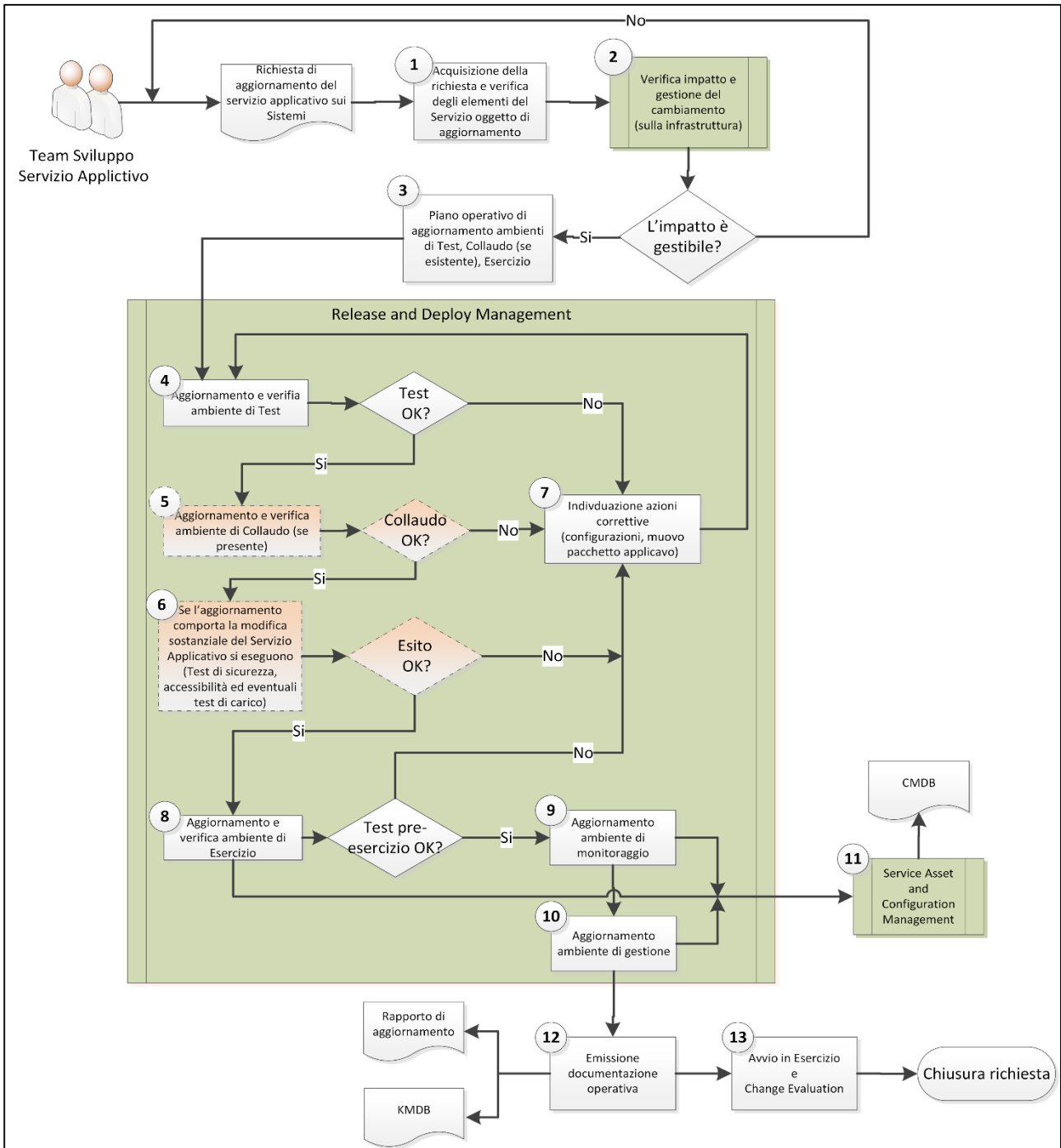


Tabella RACI:

- per l'area Governance ruoli e responsabilità nell'esecuzione delle attività sono indicati con riferimento alla casistica 2 su menzionata (evoluzione importante del servizio applicativo);
- l'area Client è coinvolta nelle attività nei casi in cui, per il tipo di applicazione, occorre intervenire sui desktop, ad esempio, potenziandone le risorse, installando SW a supporto.
- in tutte le situazioni di aggiornamenti che possono determinare un impatto nella fruizione da parte dell'utenza regionale deve essere coinvolto il Service Desk.

	Service Desk	Area Client	Area Sistemi	Area Dominio e IAM	Area Sicurezza	Area Reti	Area Governance	Area Applicativa
Attività 1			AR	C	C	C	I	
Attività 2		C	AR	C	C	C		C
Attività 3		I	AR	I	I	I		I
Attività 4			R	R	R	R		A
Attività 5			R	R	R	R		A
Attività 6			C	C	R		A	C
Attività 7			R	R	R		I	AR
Attività 8			R	R	R	R	I	A
Attività 9		C	AR	C	C	C		C
Attività 10		C	AR	C	C	C		C
Attività 11		R	R	R	R	R	C	A
Attività 12		R	R	R	R	R	I	AR
Attività 13	I	R	R	R	R	R	I	AR

12.3 SIIR-SYS-App-03, terminazione di un servizio applicativo

Il processo è avviato a fronte di una richiesta, inoltrata all'area Sistemi del SIIR, di terminazione del servizio informativo applicativo. Dapprima si interrompe l'erogazione del servizio, quindi sono effettuate le attività di salvataggio degli archivi del servizio e di disinstallazione della componente applicativa dagli ambienti di esercizio. La nuova configurazione viene riportata nella gestione degli asset del sistema CMDDB - CmdBuild.

Obiettivo del Processo è archiviare l'applicazione in una sua versione coerente (consistente nella versione finale di software), la documentazione e gli archivi, nonché dismettere le risorse hardware per il riutilizzo in altri servizi applicativi.

A fronte di una richiesta di terminazione del servizio, è necessario definire l'impatto provocato dalla sua terminazione e le azioni che devono essere effettuate per giungervi. Questa attività si rende necessaria perché **il servizio che deve essere terminato potrebbe condividere elementi con altri servizi** e la sua terminazione comportare delle inefficienze negli altri servizi. È quindi necessario identificare nel dettaglio i passi operativi da eseguire per non avere conseguenze sull'erogazione degli altri servizi.

La prima conseguenza della terminazione di un servizio è che le risorse che fino a quel momento venivano utilizzate dal servizio possono essere allocate su altri servizi. Queste risorse riguardano sia lo storage dei dati, sia la potenza di calcolo. Al fine di **programmare la disponibilità di risorse per l'erogazione dei servizi** risulta di primaria importanza disporre delle informazioni di capacità sempre aggiornate e quindi è necessario che a fronte della terminazione del servizio si provveda all'aggiornamento del piano della capacità (Capacity Plan).

Di seguito si descrive graficamente il processo di **gestione della dismissione di un servizio applicativo** dai sistemi del Datacenter regionale:

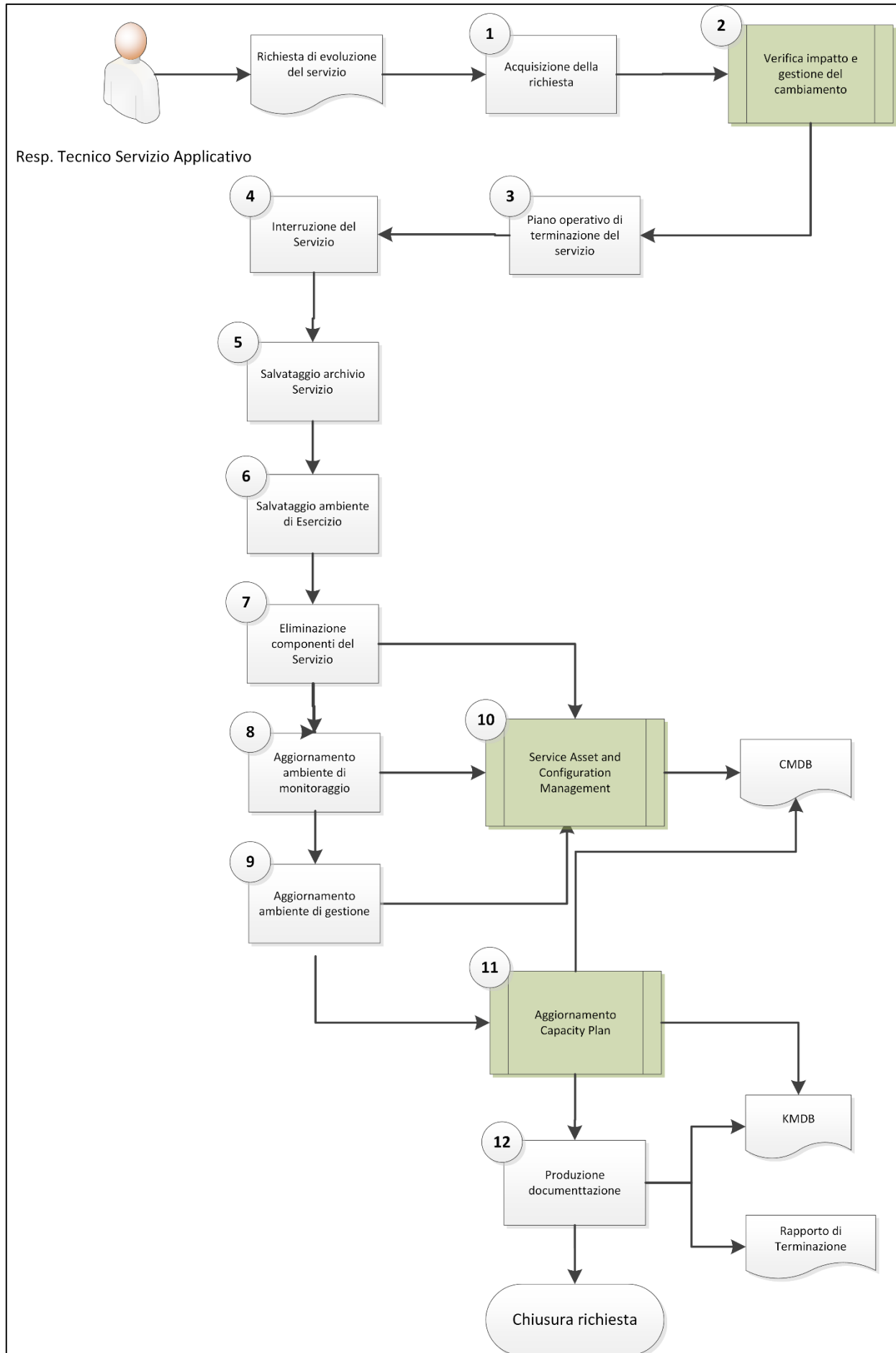


Tabella RACI:

	Service Desk	Area Client	Area Sistemi	Area Dominio / IAM	Area Sicurezza	Area Reti	Area Applicativa	Area Governance
Attività 1			AR	C	C	C		I
Attività 2		C	AR	C	C	C		I
Attività 3		I	AR	I	I	I	I	
Attività 4	I	R	R	R	R	R	A	
Attività 5			AR				I	
Attività 6			AR				I	
Attività 7		R	AR	R	R	R		
Attività 8			AR				C	
Attività 9			AR	C	C	C	C	
Attività 10		R	R	R	R	R	A	R
Attività 11			AR	C	C	C		
Attività 12		R	R	R	R	R	AR	I

13. Aggiornamento della banca dati degli asset ICT e del catalogo dei servizi

Negli ultimi anni il Servizio SIIR ha avviato un progetto per il miglioramento dell'erogazione dei servizi IT prendendo a riferimento le Good Practices di ITIL v3, con l'obiettivo di trasformarsi **da soggetto “realizzatore di infrastrutture e prodotti software” a “IT Service Provider”**, ovvero soggetto capace di costruire un'offerta di servizi e presidiarne l'erogazione. Sono stati individuati e analizzati i principali processi di erogazione dei servizi IT e si è dato avvio alla loro modellazione all'interno di un catalogo di servizi fruibile dall'utente finale.

Completata la mappatura dei servizi IT tramite il catalogo e la costruzione delle linee guida per la Governance del Sistema Informatico regionale, **dal 2015 il servizio SIIR ha avviato il percorso di certificazione ISO 27001 secondo lo Standard ISO/IEC 27001:2013** (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti).

Il processo di certificazione ha come **obiettivo** quello di **individuare i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni**.

Poiché l'informazione è un bene che aggiunge valore all'impresa, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, la Regione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento. L'obiettivo dello standard ISO 27001 è proprio quello di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (SGSI) finalizzato ad una corretta gestione dei dati e dei documenti.

Pur non essendo obbligatorio nel processo di certificazione, l'analisi dei rischi informatici chiama in causa anche aspetti relativi alla sicurezza logica, fisica ed organizzativa della gestione del sistema informativo.

La mappatura dei rischi informatici ha richiesto al SIIR l'adozione di una metodologia di

lavoro propedeutica al processo di certificazione ISO 27001 basata sui seguenti strumenti:

- **La costruzione della banca dati CMDBuild (Configuration and Management DataBase) degli asset ICT in uso.** CMDBuild è utilizzato per modellare ed amministrare il database degli asset informatici (hardware, piattaforma software, pacchetti e soluzioni applicative) e supportarne i workflow di gestione secondo le Best Practice ITIL. Il suo obiettivo è quello di agevolare gli operatori nel mantenere sotto completo controllo la situazione degli asset informatici sia materiali che immateriali, conoscendone in ogni momento la composizione, la dislocazione, le relazioni funzionali e le modalità di aggiornamento, gestendone il ciclo di vita in modo completo.
- **La mappatura, in CMDBUILD, delle dotazioni hardware e software concesse agli utenti del sistema informativo.** La mappatura, a breve visibile anche al singolo utente tramite un report su Sportello Self Service, permette di garantire un costante monitoraggio di tutti gli accreditamenti applicativi concessi ad ogni singolo utente.
- **La mappatura, in CMDBUILD, degli amministratori di sistema** non solo al fine di adempiere all'obbligo della tenuta del registro ai fini delle misure minime in materia di privacy, ma anche e soprattutto per garantire la rimozione di diritti di amministrazione non più legittimi in caso di cambi di ruolo;
- **L'identificazione e standardizzazione dei processi critici di aggiornamento della banca dati CMDBuild** per garantire la coerenza di tutto il sistema. I processi di aggiornamento della banca dati riguardano:
 - L'inserimento, la cessazione e l'aggiornamento degli utenti. Questo processo è automatizzato tramite integrazione con la banca dati SAP;
 - L'inserimento, la revoca e l'aggiornamento degli amministratori di sistema;
 - L'inserimento, la revoca e l'aggiornamento degli asset hardware assegnati agli utenti;
 - L'inserimento, la revoca e l'aggiornamento di tutte le relazioni funzionali tra servizi applicativi e/o infrastrutture;
 - L'inserimento, la revoca e l'aggiornamento delle profilazioni applicative concesse agli utenti. Questo processo è parzialmente automatizzato tramite integrazioni con Active Directory (Diritti di accesso ai servizi di rete, email, Skype, Sharepoint), e IAM (diritti di accesso alle applicazioni). E' in fase avanzata lo studio per l'introduzione di un processo di richiesta di servizi (provisioning applicativo) basato sul Self Service Sap e il relativo sistema autorizzatorio;
- **La standardizzazione dei servizi di assistenza tramite la piattaforma di Ticketing RT** per garantire un flusso ordinato e tracciabile di tutti gli interventi richiesti sia dagli utenti finali (Service desk - 1° livello) che tra gli utenti tecnici (2° livello). L'obiettivo del sistema è quello di garantire non solo l'ordine di evasione di ogni richiesta ma anche di tracciare l'evoluzione dei fabbisogni al fine di rendicontare l'efficienza dei servizi erogati e/o ottenere indicazioni per introdurre azioni correttive e/o formative sulle singole piattaforma;

- **La standardizzazione del processo di applicazione di modifiche ai sistemi tramite un sistema di richieste di intervento tecnico (change RT)** che permette di tracciare l'intero ciclo di evasione;
- **La costruzione del catalogo dei servizi Informatici regionali.** Il catalogo (<https://rt.regione.emilia-romagna.it/rt/>), realizzato su CMDBuild e già in uso dal 2013, ha l'obiettivo di:
 - dare evidenza e trasparenza dei servizi erogati dal SSIIR;
 - fornire informazioni su tali servizi e sui riferimenti per inviare le richieste;
 - consentire agli utenti di richiedere supporto o segnalare un malfunzionamento compilando un semplice ticket, di cui è possibile controllare lo stato di lavorazione in qualsiasi momento.

Un canale privilegiato e più efficiente per consultare i servizi informatici, fare segnalazioni e ottenere assistenza online.

Entrando nel nuovo strumento di Assistenza e servizi informatici i colleghi possono scegliere il servizio informatico di proprio interesse e avere a portata di mano una serie di informazioni per sapere come funziona, chi se ne occupa, gli orari (fasce critiche e fermi programmati, compresi) e quali tipi di richieste si possono fare.

Chi non trova quello che stava cercando, può chiedere assistenza o fare una segnalazione semplicemente aprendo un ticket online: una volta compilato, si possono seguire direttamente tutte le fasi di lavorazione di ogni singola richiesta.

Il Catalogo dei servizi informatici restituisce così una vera e propria mappatura di tutto quanto è a disposizione degli utenti, garantendo una maggiore uniformità e trasparenza sui livelli di servizio erogati: il catalogo sarà aggiornato nel tempo sia per contenere i nuovi servizi sia per mantenere aggiornate le informazioni.

Nel corso del 2015 il catalogo è stato esteso per garantire un suo utilizzo multi-ente. L'obiettivo di questa modifica è quello di permettere una rappresentazione dei servizi agli utenti finali in una logica federata che permetta, a fronte della centralizzazione dei servizi al SIIR, di presentare agli utenti finali solo i servizi fruibili nella propria struttura oltre a quelli di utilità generale.

Dotazioni

14. Strumenti di lavoro individuali

Poiché le informazioni e le attrezzature informatiche sono fattori critici per il successo dell'Ente e per la qualità dei processi amministrativi, devono essere protette contro perdite, alterazioni o distruzioni. È necessario inoltre che la disponibilità degli strumenti sia improntata a principi di equità, di razionalizzazione e contenimento dei costi, adottando criteri che verranno di seguito specificati e rispetto ai quali verranno promosse graduali azioni di armonizzazione.

Nel governo di tali strumenti, sotto il profilo hardware e software, ai referenti informatici di Direzione è assegnato un ruolo di coordinamento organizzativo, di presidio di eventuali competenze specifiche o settoriali e di raccordo con la struttura centrale; i referenti costituiscono dunque un interlocutore privilegiato ed hanno come impegno prioritario da un lato quello di segnalare in modo tempestivo ed il più possibile pianificato le esigenze evolutive in campo tecnologico della propria Direzione, dall'altro quello di presidiare la corretta assegnazione delle risorse nel tempo, alla luce delle priorità della Direzione stessa, in particolare, e dell'Amministrazione in generale.

14.1 Assegnazione

Dotazione standard

A ciascun collaboratore dell'Ente in servizio, viene assegnato di norma uno strumento di informatica individuale (personal computer desktop) collegato alla rete informatica aziendale, qualora la tipologia delle mansioni assegnate o gli aspetti logistici non ostino.

Tale strumento sarà unico: chi quindi, per comprovate esigenze di lavoro, necessita di uno strumento mobile (pc portatile notebook o ultraleggero) dovrà rinunciare alla postazione desktop. Eventuali deroghe potranno essere autorizzate dal Servizio SIIR previa richiesta del Direttore competente.

Dotazione per contratti di telelavoro

Ai collaboratori regionali inseriti nel progetto "Telelavoro" l'Amministrazione fornisce:

- uno strumento "network computer" per l'accesso alla postazione di lavoro in ufficio ovvero un personal computer portatile per lavorare sia da casa che dall'ufficio;
- un collegamento telematico che consenta l'accesso sicuro ai servizi della rete regionale Intranet dal domicilio scelto per il telelavoro. Sono possibili più modalità tecniche per realizzare il collegamento, a seconda dell'offerta di servizi disponibile presso il domicilio stesso. Le varie soluzioni tecniche possono prevedere l'installazione di un telefono e/o di altre apparecchiature di rete presso il domicilio, oppure solo configurazioni SW su strumentazioni private esistenti.

Lo strumento in dotazione a casa potrà essere corredato da monitor esterno e tastiera che sarà possibile conservare a casa per tutta la durata del contratto. Analogamente a quanto avviene per le dotazioni standard, non è prevista la dotazione di stampanti individuali per l'attività di telelavoro. Tutta la strumentazione assegnata dovrà essere riconsegnata al termine del telelavoro, per essere eventualmente sostituita con la strumentazione standard.

Dotazione per volontari, stagisti e collaboratori con presenza inferiore a sei mesi

Per tale tipologia di utenti è prevista l'assegnazione di postazioni di lavoro virtuali su server, accedute tramite strumenti "network computer"; tali postazioni sono approntabili e successivamente eliminabili con grande flessibilità e costi contenuti e sono dotate dei prodotti standard di Office automation.

Dotazione per volontari con funzioni dirigenziali

Per tale tipologia di utenti è autorizzata l'assegnazione della dotazione previste per i dirigenti. La richiesta della dotazione deve essere avanzata dal Responsabile della struttura a cui riporta il volontario.

Dotazione di strumenti portatili aggiuntivi

A ciascun Servizio sarà possibile assegnare un personal computer portatile, notebook o ultraleggero che potrà essere utilizzato da collaboratori della struttura stessa secondo necessità per convegni/riunioni/missioni e che verrà formalmente assegnato al Responsabile di struttura o di segreteria. Servizi regionali dislocati su più sedi provinciali potranno essere dotati di un portatile di presidio per ciascuna sede.

A ciascuna Direzione o Agenzia o Segreteria di Assessore sarà possibile assegnare fino ad un massimo di due personal computer portatili.

Dotazione di strumenti aggiuntivi per progetti o funzioni speciali

Per garantire all'amministrazione l'uso razionale delle risorse ed il contenimento di costi per licenze di prodotti specialistici o per l'uso di attrezzature hardware non standard o per la gestione di sale operative, si possono assegnare postazioni desktop o portatili aggiuntive.

Dotazione di dispositivi mobili

I criteri di assegnazione per i dispositivi mobili sono regolamentati sul Disciplinare per l'assegnazione e l'utilizzo di utenze di telefonia fissa e mobile della Giunta della Regione Emilia-Romagna (delibera n. 1465/2011).

Le richieste di assegnazione debbono essere effettuate unicamente dal Responsabile della struttura di appartenenza dell'utente o, nel caso delle strutture speciali, dal politico di riferimento. Tutte le richieste vanno compilate online su Internos: Home → Servizi online → Richieste online → Telefonia mobile.

Ogni richiesta deve essere autorizzata dal Direttore di riferimento e quindi inoltrata alla DG centrale Organizzazione, personale, sistemi informativi e telematica. Quest'ultima può approvare o rifiutare l'istanza, a seguito di una valutazione, sulla base del regolamento (comma 3 articolo 9).

Rispetto delle policy di sicurezza

Tutti gli strumenti portatili, pena la decadenza del diritto all'utilizzo, dovranno essere utilizzati nel pieno rispetto delle policy di sicurezza dell'amministrazione; a titolo di esempio non esaustivo, i portatili dovranno essere collegati alla rete regionale per gli aggiornamenti di sicurezza con cadenza almeno mensile. Strumenti portatili che risultino non aggiornati da oltre tre mesi, e per i quali non sia stata preventivamente concordata una motivata deroga di utilizzo con il Servizio SIIR, dovranno essere restituiti.

Gli assegnatari a qualunque titolo di personal computer portatili sono tenuti a riconsegnarli alla struttura informatica centrale nel momento in cui decadano le motivazioni che ne hanno determinato l'assegnazione, affinché possano essere utilizzati per altre necessità.

Composizione della postazione di lavoro

Lo strumento assegnato è conforme agli standard adottati e supportati dall'Ente, si basa su sistemi operativi Microsoft, è corredato da un prodotto di Office Automation Open Source, è dotato di software antivirus e di eventuali prodotti software aggiuntivi necessari per i progetti core dell'Ente o per supportare funzioni specialistiche (ad esempio SAP, SAS, Adobe, prodotti Autocad 3D, Microsoft Lync, Citrix XenAPP) la cui diffusione e gestione, governata da appositi gruppi di progetto, è commisurata alle effettive necessità di utilizzo ed alla disponibilità delle licenze acquisite dall'Amministrazione. Eventuali evoluzioni nelle piattaforme software adottate e supportate saranno studiate, vagliate e proposte a cura del Servizio SIIR, previo coinvolgimento del settore responsabile della formazione informatica. Postazioni di lavoro dotate di sistemi operativi non Microsoft dovranno essere preventivamente autorizzate.

Eventuali prodotti di informatica individuale aggiuntivi dovranno essere richiesti e concordati preventivamente per verificare la disponibilità di prodotti Open source equivalenti (come previsto dall'art. 9bis del D.L. 179/2012) o programmare l'acquisto nei casi di provata necessità ed in base alle disponibilità di risorse. Verrà comunque data priorità ad esigenze che si riconducano a prodotti già conosciuti e disponibili ed il più possibile standardizzati.

Tutti i monitor installati nelle postazioni di lavoro sono a norma, ancorché siano diversificati per tipologia e dimensioni; l'ampiezza standard dei monitor forniti sulle postazioni di lavoro desktop o aggiuntivi a portatili unici è pari a 17"; la fornitura di monitor di dimensioni maggiori devono essere motivate da comprovare necessità lavorative o da segnalazioni del Medico Competente.

Funzioni di stampa.

Le funzioni di stampa sono particolarmente critiche per l'Amministrazione, perché comportano costi molto elevati e sono fonte di criticità di gestione tecnica e di materiali di consumo; tali funzioni sono affidate a strumenti laser multifunzione a noleggio installati in corridoi o vani tecnici, dotati di configurazioni software in grado di assicurare la riservatezza delle stampe prodotte; in presenza di strumentazioni di corridoio insufficienti, sarà valutata la possibilità di fornire stampanti inkjet di rete regionali dotate di funzioni di stampa fronte/retro.

Le stampanti individuali saranno consentite, in deroga, unicamente per fornire funzioni di stampa a fronte di eventuale impedimenti fisici o logistici. Una unica stampante individuale potrà essere conservata in deroga presso ciascun Assessore o ciascun Direttore per assicurare continuità di stampa in caso di disservizi al di fuori degli orari di presidio (8-18) assicurati dalla struttura informatica.

Non potranno essere installate stampanti laser nelle stanze adibite ad ufficio, in quanto ritenute in contrasto con le norme di salubrità degli ambienti di lavoro.

Periferiche aggiuntive.

Periferiche di lettura di smart card sono attualmente installate su postazioni di Dirigenti, di responsabili di Posizione Organizzativa, presso alcune postazioni di lavoro con esigenze

specifiche. L'introduzione della firma digitale remota le renderà a breve superflue.

Eventuali periferiche ritenute necessarie seguiranno un iter di richiesta motivata e di programmazione di acquisto analogo a quello del software aggiuntivo.

Si richiama la necessità di porre attenzione all'uso di strumenti di scrittura e salvataggio di dati (dischi portatili, masterizzatori, PenDrive ecc.) che da un lato facilitano la condivisione di documenti ma dall'altro presentano, analogamente ai personal computer portatili, problematiche legate alla sicurezza dei dati e di controllo di accesso agli stessi.

14.2 Adempimenti in caso di cessazione del rapporto di lavoro

In caso di cessazione del rapporto di lavoro, il collaboratore regionale assegnatario deve riconsegnare tutta la propria dotazione strumentale entro l'ultimo giorno lavorativo, secondo le modalità sotto descritte.

Le dotazioni di telefonia mobile dovranno essere riconsegnate presso gli uffici del SIIR a cura del collaboratore stesso.

Il referente informatico della struttura dovrà essere informato dal lavoratore o dal Responsabile di Servizio, affinché possa programmare per tempo il recupero di eventuali dati di pertinenza dell'amministrazione dagli strumenti assegnati al collaboratore.

Entro il giorno lavorativo successivo alla cessazione del rapporto di lavoro il referente dovrà effettuare al Service Desk la richiesta di ritiro di tutti gli strumenti di lavoro individuali di qualunque tipologia, che dovranno essere ritirati e conservati inalterati dal Servizio SIIR per ulteriori due settimane dal ritiro, dopodiché saranno completamente resettati. In mancanza di gestione proattiva, l'attività di ritiro sarà disposta dal personale del Servizio SIIR al ricevimento delle segnalazioni di cessazione dal database del personale.

14.3 Modalità di utilizzo

Le attrezzature individuali assegnate al collaboratore devono essere usate esclusivamente quale supporto all'attività lavorativa in modo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e di sicurezza della rete e dei sistemi. In particolare sulle postazioni di lavoro deve essere usato esclusivamente il software autorizzato e fornito dall'Ente. Eventuale software aggiuntivo ritenuto necessario, sia da acquistare sia disponibile gratuitamente, deve essere richiesto al proprio referente informatico o al proprio dirigente responsabile funzionale; riscontrata l'utilità per le attività di lavoro da parte del dirigente, il referente informatico chiederà il supporto dell'assistenza utenti del Servizio SIIR per la valutazione tecnica del software sotto il profilo della sicurezza, della rispondenza ai requisiti di accessibilità e per programmare l'eventuale acquisto ed installazione.

Per maggiori dettagli si faccia riferimento al Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta della Regione Emilia-Romagna approvato con determinazione 14852 del 2011.

Come misure preventive verranno individuate *policy* di sistema che blocchino alcune opzioni potenzialmente pericolose per la sicurezza. Le operazioni che l'utente non potrà più compiere in autonomia, qualora necessarie, potranno essere svolte dagli amministratori veri e propri, ed in particolare dai referenti informatici (presso la postazione utente) e dai tecnici dell'assistenza utenti (sia presso l'utente sia in modalità remota).

14.4 Modalità di richiesta

Per le necessità di strumenti che si riconducano alle modalità standard (personal computer desktop o portatile motivato da comprovate esigenze di lavoro, eventuali periferiche, software di uso comune) la richiesta va inoltrata tramite il Catalogo dei servizi informatici linkato sul sito Internos nella sezione "Sapere e fare/funziona così/software computer e applicazioni/Numeri e link utili per utenti della Giunta" o raggiungibile direttamente all'indirizzo <https://rt.regione.emilia-romagna.it/rt/>. Può essere anche inoltrata via posta elettronica dal referente informatico alla casella di posta ServiceDesk@regione.emilia-romagna.it; la possibilità di evasione ed i relativi tempi sono comunicati dal Servizio SIIR con le medesime modalità.

In caso di necessità di personal computer portatili aggiuntivi o di strumenti di tipologia particolare (workstation, plotter, applicativi non standard) è necessario venga inoltrata una richiesta motivata indirizzata al Responsabile del Servizio SIIR; la richiesta verrà valutata alla luce delle risorse disponibili.

14.5 Modalità di aggiornamento catasto attrezzature informatiche individuali

Le attrezzature individuali sono soggette a numerose variazioni, dovute ad attività tecniche attuate sia da tecnici informatici della struttura informatica centrale sia da tecnici informatici di alcune Direzioni o Agenzie, ad assunzioni o dimissioni di collaboratori - regionali e non - presso le varie strutture.

Le informazioni relative alle attrezzature individuali consentono all'ente di avere dati aggiornati sulla consistenza patrimoniale, alla struttura informatica centrale di gestire le verifiche di sicurezza in osservanza dell'apposito disciplinare e rendono possibile quantificare la spesa per la gestione. Mantenere aggiornate nel tempo tali informazioni richiede un impegno costante che non può essere assicurato dalla sola struttura informatica centrale.

Per tale motivo tutte le Direzioni e Agenzie concorrono all'aggiornamento e alla validazione di tali informazioni, che risiedono nell'ambiente di gestione del dominio regionale e nel catasto delle attrezzature informatiche CMDBuild. Gli aggiornamenti dell'ambiente di dominio regionale devono essere assicurati con continuità da tutti gli utenti abilitati alla delega; gli aggiornamenti del catasto delle attrezzature informatiche devono essere garantiti con la massima tempestività, in subordine con cadenza almeno bimestrale e con informazioni attendibili da parte di tutte le strutture.

14.6 Modalità di presa in carico di attrezzature

Le attrezzature acquistate in autonomia dalle Direzioni Generali potranno essere utilizzate nella rete dell'Ente solo previa verifica da parte delle strutture tecniche del Servizio SIIR.

La verifica dovrà accertare la rispondenza degli strumenti agli standard tecnologici in uso e alle policy adottate e la possibilità di gestione da parte dei tecnici dell'assistenza. Gli strumenti dovranno essere resi disponibili per i controlli dei tecnici corredati di tutte le informazioni relative al fornitore, alla tipologia e durata della garanzia.

Qualora il riscontro non fosse positivo o i tempi di presa in carico non potessero essere brevi, gli strumenti dovranno essere utilizzati in modalità non in rete.

14.7 Modalità di supporto ed assistenza

In caso di guasti o malfunzionamenti gli utenti sono tenuti ad utilizzare le seguenti modalità di segnalazione:

- inoltrandola tramite il Catalogo dei servizi informatici fruibile sul sito Internos nella sezione "Sapere e fare/funziona così/software computer e applicazioni/Numeri e link utili per utenti della Giunta" o raggiungibile direttamente all'indirizzo <https://rt.regione.emilia-romagna.it/rt/>.
- inoltrandola via posta elettronica dal referente informatico alla casella di posta ServiceDesk@regione.emilia-romagna.it;
- chiamando il numero telefonico 051 527 5850.

Le problematiche verranno prese in considerazione in tempo reale, ma subiranno un vaglio per stabilire le priorità di intervento tecnico secondo i seguenti criteri di priorità:

- guasto bloccante ad una postazione pc di segreteria, ad una casella di posta elettronica di struttura, ad una postazione che necessita di essere operativa per necessità progettuali essendo unica o particolare (ad es. portineria, postazione di economo centrale o periferico, postazione di protocollo, postazione a disposizione del pubblico)
- guasto bloccante a stampante di rete condivisa
- guasto bloccante a strumento o applicazione individuale
- guasto non bloccante

In caso di guasti o malfunzionamenti di strumenti di telelavoro che non possano essere risolti con il supporto telefonico, e salvo impedimenti legati allo stato di salute del telelavoratore, lo strumento da ripristinare dovrà essere riportato a cura del collaboratore interessato presso il presidio di Help Desk specialistico dell'area client, posto nella sede di Viale Aldo Moro 30 a Bologna o se assegnato a strutture periferiche, presso la propria sede di lavoro, dove sarà possibile effettuare la riparazione o l'eventuale sostituzione.

In caso di eventuali problemi che si riscontrassero nella gestione di un intervento di malfunzionamento i collaboratori sono tenuti ad informare il referente informatico di riferimento, qualora non fosse già stato avvisato, per una gestione più efficace della problematica insieme ai responsabili dell'assistenza tecnica agli utenti.

15. Servizi di rete

In generale, tutte le postazioni di lavoro, al momento dell'installazione, vengono collegate all'infrastruttura di rete a servizio degli uffici regionali.

Le postazioni non connesse sono ormai in numero ridottissimo, e devono esserci motivazioni importanti per configurarle in questo modo, o mantenerle in questa condizione. Ricordiamo che attraverso l'infrastruttura di rete tutte le postazioni di lavoro vengono periodicamente aggiornate con l'installazione degli aggiornamenti di sicurezza e dell'antivirus; le postazioni non connesse richiedono quindi un'attività aggiuntiva e costosa di aggiornamento manuale da parte dei tecnici informatici.

Ogni Personal Computer nasce quindi, di default, come postazione connessa in rete locale (LAN). Dovunque ciò è possibile, anche le stampanti vengono collegate alla LAN, in modo da permetterne l'uso condiviso tra più utenti; inoltre è possibile garantirne il monitoraggio e l'aggiornamento ai fini della sicurezza da parte dei tecnici, con evidenti economie di gestione. Le LAN degli uffici regionali sono in genere realizzate in tecnologia Fast Ethernet. Ad oggi – febbraio 2016 – le tecnologie Gigabit Ethernet e 10 Gigabit Ethernet vengono utilizzate per collegare i server presso il CED e nelle interconnessioni di dorsale, all'interno dei palazzi o tra le sedi collegate in fibra ottica attraverso la rete Lepida.

Tutte le LAN a servizio delle sedi degli uffici sono tra loro connesse attraverso circuiti

geografici di varie tecnologie; i circuiti sono monitorati con regolarità per verificarne l'occupazione di banda, e vengono potenziati non appena gli utenti ne presentano la necessità, se sono attivabili circuiti con migliori prestazioni.

Per quanto riguarda le postazioni di lavoro non presenti nelle sedi, la rete regionale consente collegamenti di vario genere per gli utenti remoti, e propone soluzioni particolari per i telelavoratori e gli utenti mobili.

Ricordiamo che l'accesso alla posta elettronica, alle informazioni personali per i dipendenti ed alle cartelle personali contenenti i propri dati sui server del CED è permesso a tutti, da qualsiasi postazione di lavoro connessa ad Internet, attraverso il protocollo di comunicazione criptato https, con le stesse modalità utilizzate presso gli uffici regionali.

15.1 Accesso alla rete per i telelavoratori

Presso l'abitazione dei collaboratori regionali con contratto di telelavoro può venire attivato, a spese dell'amministrazione, un circuito affittato (in genere ADSL) su rete fissa o su rete cellulare (APN), interconnesso in entrambi i casi alla Intranet regionale; l'utente può quindi accedere, anche dalla propria abitazione, a tutti i dati e servizi a cui accede normalmente in ufficio. Per comunicare con i colleghi o gli utenti, vengono anche forniti una normale linea telefonica ed il relativo telefono, rispettivamente fisso o cellulare.

In alternativa, il telelavoratore che già posseda un proprio collegamento ad Internet può scegliere di configurare su di esso una connessione VPN secondo gli standard regionali, attraverso cui svolgere la propria attività in telelavoro, come meglio precisato nel paragrafo seguente. In questo caso la Regione non fornisce né installa apparecchiature di rete né telefono fisso presso il domicilio del telelavoratore, né è tenuta a fornire un telefono cellulare.

Le Direzioni Generali interessate dovranno inviare al SIIR una comunicazione sollecita, in generale non appena deciso di sottoscrivere un contratto di telelavoro, per consentire la predisposizione di tutto il necessario: infatti i tempi di attivazione delle linee ADSL di collegamento sono lunghi e spesso imprevedibili, in quanto dipendono dalla disponibilità di risorse sul territorio da parte del fornitore di connettività.

15.2 Accesso alla rete via VPN client

Per telelavoratori o altri utenti mobili, dotati di collegamento ad Internet in banda larga, è possibile realizzare un collegamento alla Intranet:

- attraverso una configurazione VPN Client in modalità Office Mode
- oppure tramite VPN SSL.

Nel primo caso sul Personal Computer dell'utente è necessario installare un apposito software, che dopo l'immissione delle credenziali (la stessa coppia di userid e password normalmente usata per accedere alla LAN) realizza una connessione criptata con il Firewall regionale.

Nel secondo caso l'analogo SW che istituisce la connessione con il firewall regionale viene scaricato e configurato accedendo ad apposite pagine attraverso un normale browser, al primo accesso. L'autenticazione avviene utilizzando un sistema di autenticazione a due fattori:

- un certificato, generato ed installato sulla postazione di lavoro dell'utente dai tecnici del SIIR al momento dell'attivazione della VPN;

- una One Time Password, generata al momento dell'accesso ed inviata all'utente via mail.

Ricordiamo che i costi relativi al collegamento ad Internet sono a carico dell'utente, e che nessun rimborso potrà essere richiesto alla Regione per questo servizio; pertanto è consigliabile sottoscrivere con il fornitore di connettività un contratto ADSL a banda larga, a tariffa flat, via cavo.

Va tenuto presente che le prestazioni nell'accesso ai servizi saranno limitate dalla banda massima disponibile sull'intero percorso d'interconnessione e che esse possono cambiare nel tempo in modo imprevedibile, in particolare se si transita da Internet.

Utilizzare un collegamento via VPN impone, sul Personal computer, stringenti politiche di sicurezza, in quanto il Personal Computer, una volta connesso, può accedere a tutti i servizi e le risorse alla stessa maniera delle postazioni connesse in rete locale; quindi:

- la configurazione è consentita unicamente su Personal Computer portatili di proprietà regionale, configurati con certificazione al dominio obbligatoria;
- il PC deve essere configurato in modo adeguato: il firewall locale deve essere attivo, l'antivirus attivo ed aggiornato, il sistema operativo aggiornato;
- quando la VPN è attiva, sono disponibili tutti i servizi della rete Intranet regionale; la navigazione Internet via browser è possibile unicamente attraverso il proxy; solo in questo caso è protetta e controllata;
- quando il Personal Computer non è connesso in VPN, la responsabilità di ogni accesso illegale ricade sull'utente; perciò l'amministrazione regionale non si assume alcuna responsabilità per danni eventualmente arrecati a terzi in questa modalità.

Il collegamento su VPN ha un costo per l'Ente ed il numero di licenze disponibili è limitato, pertanto viene utilizzato solo nei casi effettivamente necessari, in cui non è possibile ricorrere ad altri tipi di collegamento. I collegamenti VPN debbono essere richiesti dai Responsabili di struttura e i tecnici del SIIR concorderanno con i referenti informatici della struttura stessa, il numero delle connessioni possibili e le modalità della loro attivazione, fino all'esaurimento delle risorse disponibili.

15.3 Accesso alla rete per fornitori di servizi di teleassistenza

Ove siano presenti sistemi connessi nella rete Intranet regionale, su cui siano installate soluzioni complesse, può presentarsi la necessità di permettere a ditte esterne di accedere ai sistemi stessi, per fornire servizi di assistenza e manutenzione da remoto.

Ricordiamo che il contratto stipulato col fornitore dovrà in ogni caso contemplare la designazione dei tecnici incaricati di questa attività quali responsabili esterni per il trattamento di dati personali, ed i conseguenti adempimenti previsti. Sarà inoltre opportuno prevedere nel contratto particolari clausole, quali richieste di penali, nel caso di violazioni delle norme di sicurezza attraverso gli accessi remoti configurati.

Sono previste due principali modalità di collegamento:

- 1) accesso via Internet: se il sistema è dotato di un indirizzo IP pubblico, è posizionato in un'area di rete accessibile da Internet, ed è configurato con le opportune policies di sicurezza, è possibile consentirne l'accesso attraverso una regola da predisporre sul firewall regionale, che identificherà in modo preciso:

- la porta o le porte attraverso cui avverrà l'accesso; è necessario usare protocolli criptati ogni qualvolta vengano trattati dati personali; le porte consigliate sono ssh, https o similari;
- l'indirizzo / gli indirizzi di provenienza; si potrà trattare di un singolo IP pubblico assegnato al firewall/proxy della ditta fornitrice, oppure di una sottorete IP pubblica assegnata ufficialmente alla ditta stessa oppure ad una sua consociata; faranno fede gli appositi database delle autorità di rilascio degli indirizzi IP, come il RIPE per il nostro territorio;
- la regola sarà temporizzata, consentendo l'accesso solo in giorni ed orari preventivamente concordati; a meno di particolari esigenze, si sconsiglia di permettere l'accesso nelle fasce notturne o nei giorni festivi.

2) attraverso la modalità VPN SSL (vedi par. 12.2) configurata in modo da permettere al fornitore esclusivamente l'accesso ai sistemi sui quali è prevista l'assistenza o la manutenzione. In questo caso la responsabilità del collegamento sarà affidata ai singoli utenti esterni, appositamente autenticati, che useranno le credenziali normalmente utilizzate per accedere ai sistemi Intranet anche per accedere alla rete.

Ricordiamo che, qualora il contratto con la ditta fornitrice non fosse più valido per scadenza dei termini o inosservanza delle condizioni stabilite, è indispensabile segnalarlo tempestivamente al SIIR, in modo da impedire da quel momento in poi l'accesso da parte del fornitore al sistema interessato.

15.4 Accesso alle caselle di posta regionale tramite dispositivi mobili

Esiste la possibilità di accedere alla casella di posta regionale attraverso dispositivi mobili smartphone o tablet; questo accesso offre inoltre la possibilità di sincronizzare anche altri dati come rubrica, agenda e note tra il dispositivo mobile e il server di posta regionale Exchange.

Tale funzionalità è subordinata all'accettazione da parte dell'utente della possibilità che gli amministratori del server di posta regionale possano cancellare tutti i dati dell'utente dal dispositivo mobile (wipe).

- abilitazione sul sistema di posta regionale del servizio per il singolo utente, contestuale alla richiesta di un dispositivo regionale o, in fase successiva, solo se il dispositivo in possesso dell'utente lo permette;
- sistema operativo Android, IOS/Windows Phone, o Symbian con software Mail for Exchange che sono attualmente pienamente integrati con la piattaforma di posta esistente, nella quale risiedono le caselle regionali;
- nel caso di perdita di un dispositivo mobile è indispensabile che l'utente ne dia tempestivamente comunicazione all'Ente, per autorizzare il blocco del servizio fornendo poi in tempi brevi anche la denuncia all'autorità competente;
- l'assistenza e la configurazione della sincronizzazione del dispositivo mobile con il server di posta regionale è garantita solo per gli apparati di proprietà dell'ente.

Oltre ai servizi di posta elettronica, per quanto riguarda l'accesso ad altri servizi di rete da telefoni cellulari e tablet è possibile accedere solo ai servizi che la regione rende disponibili sulla rete Internet.

Normativa di riferimento

D.lgs. 82/2005 “Codice dell'Amministrazione Digitale”

D.Lgs. 235/2010 “Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69”

Art. 53 (Caratteristiche dei siti): *“Le pubbliche amministrazioni centrali realizzano siti istituzionali su reti telematiche che rispettano i principi di accessibilità, nonché di elevata usabilità e reperibilità, anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità di consultazione, qualità, omogeneità ed interoperabilità”*

Legge 4/2004 “Disposizioni per favorire l'accesso ai soggetti disabili agli strumenti informatici”

Art. 4 (Obblighi per l'accessibilità) comma 1: *“Nelle procedure svolte dai soggetti ... per l'acquisto di beni e per la fornitura di servizi informatici, i requisiti di accessibilità ... costituiscono motivo di preferenza a parità di ogni altra condizione nella valutazione dell'offerta tecnica, tenuto conto della destinazione del bene o del Servizio. La mancata considerazione dei requisiti di accessibilità o l'eventuale acquisizione di beni o fornitura di servizi non accessibili è adeguatamente motivata”*

Art. 4 (Obblighi per l'accessibilità) comma 2: *“I soggetti ...non possono stipulare, a pena di nullità, contratti per la realizzazione e la modifica di siti Internet quando non è previsto che essi rispettino i requisiti di accessibilità.... I contratti in essere, in caso di rinnovo, modifica o novazione, sono adeguati, a pena di nullità...”*

Art. 9 (Responsabilità): *“L'inosservanza delle disposizioni della presente legge comporta responsabilità dirigenziale e responsabilità disciplinare.... Ferme restando le eventuali responsabilità penali e civili previste dalle norme vigenti”*

DM 20/3/2013 “Modifiche all'allegato A del decreto 8 luglio 2005 del Ministro per l'innovazione e le tecnologie, recante: «Requisiti tecnici e i diversi livelli per l'accessibilità agli strumenti informatici»”.

Premessa: I requisiti tecnici si applicano a tutti i casi in cui i soggetti di cui all'articolo 3, comma 1, della legge n. 4/2004 forniscono informazioni o servizi su reti internet, intranet o extranet, su supporti informatici removibili (quali ad esempio CD-ROM, DVD) che possono essere utilizzati anche in stazioni di lavoro non collegate ad una rete telematica.

Le informazioni ed i servizi erogati possono essere resi fruibili mediante:

- siti web;
- applicazioni realizzate con tecnologie web;
- documenti resi disponibili sui siti web;
- documenti di cui al requisito 11 dell'allegato D del d.m. 8 luglio 2005.

D. Lgs. 196/2003 “Codice in materia di protezione dei dati personali”

Gli obblighi in materia di sicurezza dei dati e dei sistemi sono contenuti principalmente nel Titolo V del Codice e in particolare nell' **Art. 31 (Obblighi di sicurezza)**, **Art. 33 (Misure minime)**, **Art. 34 (Trattamenti con strumenti elettronici)**.

Legge finanziaria 2007: I commi 892 e 895 della Finanziaria prevedono 30 m€ per il sostegno agli investimenti per l'innovazione negli EELL con priorità a chi utilizza o sviluppa applicazioni software a codice aperto.

Direttiva n.8/2009 del Ministro per la pubblica amministrazione e l'innovazione “per la riduzione dei siti web delle PA e per il miglioramento della qualità dei servizi e delle informazioni online al cittadino”

(http://www.innovazionepa.gov.it/media/339253/dir_n_8_09.pdf)

“Linee Guida per i siti web della PA” del Ministro per la pubblica amministrazione e l'innovazione (<http://www.innovazionepa.gov.it/lazione-del-ministro/linee-guida-siti-web-pa/presentazione.aspx>)

Provvedimento del Garante Privacy del 2014 “Individuazione delle modalità semplificate per l'informatica e l'acquisizione del consenso per l'uso dei cookie”

(<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884>)

D.lgs. 33/2013 “Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.”

D.L. 66/2014 "Misure urgenti per la competitività e la giustizia sociale”

Il provvedimento ha previsto norme in materia di tempi di pagamento, fattura elettronica e monitoraggio dei debiti della PA.

D.P.C.M. 3-12-2013 pubblicato sulla **Gazzetta Ufficiale il 12-03-2014** “Regole tecniche in materia di conservazione e protocollo informatico”

D.P.C.M. 13-11-2014 pubblicato sulla **Gazzetta Ufficiale il 12-01-2015** “Regole tecniche in materia di documenti informatici”

Regolamento (UE) n. 910/2014 “*Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*”

Il regolamento, pubblicato il 28 agosto 2014 nella Gazzetta Ufficiale dell'Unione Europea (EU Official Journal L 257), noto con l'acronimo di **eIDAS** (*electronic IDentification Authentication and Signature*), abroga la direttiva 1999/93/CE e stabilisce le condizioni per il riconoscimento reciproco in ambito di identificazione elettronica e le regole comuni per le firme elettroniche, l'autenticazione web ed i relativi servizi fiduciari per le transazioni elettroniche.

Legge 124/2015 “*Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche*”

Art. 1 (Carta della cittadinanza digitale): “1. Al fine di garantire ai cittadini e alle imprese, anche attraverso l'utilizzo delle tecnologie dell'informazione e della comunicazione, il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale, nonché al fine di garantire la semplificazione nell'accesso ai servizi alla persona, riducendo la necessità dell'accesso fisico agli uffici pubblici, il Governo è delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente legge, con invarianza delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente, uno o più decreti legislativi volti a modificare e integrare, anche disponendone la delegificazione, il codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, di

seguito denominato «CAD», nel rispetto dei seguenti principi e criteri direttivi:

a) individuare strumenti per definire il livello minimo di sicurezza, qualità, fruibilità, accessibilità e tempestività dei servizi on line delle amministrazioni pubbliche; prevedere, a tal fine, speciali regimi sanzionatori e premiali per le amministrazioni stesse;

b) ridefinire e semplificare i procedimenti amministrativi, in relazione alle esigenze di celerità, certezza dei tempi e trasparenza nei confronti dei cittadini e delle imprese, mediante una disciplina basata sulla loro digitalizzazione e per la piena realizzazione del principio «innanzitutto digitale» (digital first), nonché l'organizzazione e le procedure interne a ciascuna amministrazione;

c) garantire, in linea con gli obiettivi dell'Agenda digitale europea, la disponibilità di connettività a banda larga e ultralarga e l'accesso alla rete internet presso gli uffici pubblici e altri luoghi che, per la loro funzione, richiedono le suddette dotazioni, anche attribuendo carattere prioritario, nei bandi per accedere ai finanziamenti pubblici per la realizzazione della strategia italiana per la banda ultralarga, all'infrastrutturazione con reti a banda ultralarga nei settori scolastico, sanitario e turistico, agevolando in quest'ultimo settore la realizzazione di un'unica rete wi-fi ad accesso libero, con autenticazione tramite Sistema pubblico per la gestione dell'identità digitale (SPID), presente in tutti i luoghi di particolare interesse turistico, e prevedendo la possibilità di estendere il servizio anche ai non residenti in Italia, nonché prevedendo che la porzione di banda non utilizzata dagli uffici pubblici sia messa a disposizione degli utenti, anche non residenti, attraverso un sistema di autenticazione tramite SPID; garantire l'accesso e il riuso gratuiti di tutte le informazioni prodotte e detenute dalle amministrazioni pubbliche in formato aperto, l'alfabetizzazione digitale, la partecipazione con modalità telematiche ai processi decisionali delle istituzioni pubbliche, la piena disponibilità dei sistemi di pagamento elettronico nonché la riduzione del divario digitale sviluppando le competenze digitali di base;

d) ridefinire il Sistema pubblico di connettività al fine di semplificare le regole di cooperazione applicativa tra amministrazioni pubbliche e di favorire l'adesione al Sistema da parte dei privati, garantendo la sicurezza e la resilienza dei sistemi;

e) definire i criteri di digitalizzazione del processo di misurazione e valutazione della performance per permettere un coordinamento a livello nazionale;

f) coordinare e razionalizzare le vigenti disposizioni di legge in materia di strumenti di identificazione, comunicazione e autenticazione in rete con la disciplina di cui all'articolo 64 del CAD e la relativa normativa di attuazione in materia di SPID, anche al fine di promuovere l'adesione da parte delle amministrazioni pubbliche e dei privati al predetto SPID;

g) favorire l'elezione di un domicilio digitale da parte di cittadini e imprese ai fini dell'interazione con le amministrazioni, anche mediante sistemi di comunicazione non ripudiabili, garantendo l'adozione di soluzioni idonee a consentirne l'uso anche in caso di indisponibilità di adeguate infrastrutture e dispositivi di comunicazione o di un inadeguato livello di alfabetizzazione informatica, in modo da assicurare, altresì, la piena accessibilità mediante l'introduzione, compatibilmente con i vincoli di bilancio, di modalità specifiche e peculiari, quali, tra le altre, quelle relative alla lingua italiana dei segni;

h) semplificare le condizioni di esercizio dei diritti e l'accesso ai servizi di interesse dei cittadini e assicurare la conoscibilità della normativa e degli strumenti di sostegno della maternità e della genitorialità corrispondenti al profilo dei richiedenti, attraverso

l'utilizzo del sito internet dell'Istituto nazionale della previdenza sociale collegato con i siti delle amministrazioni regionali e locali, attivabile al momento dell'iscrizione anagrafica della figlia o del figlio nato o adottato, secondo modalità e procedure che garantiscano la certezza e la riservatezza dei dati;

i) razionalizzare gli strumenti di coordinamento e collaborazione delle amministrazioni pubbliche al fine di conseguire obiettivi di ottimizzazione della spesa nei processi di digitalizzazione favorendo l'uso di software open source, tenendo comunque conto di una valutazione tecnico-economica delle soluzioni disponibili, nonché obiettivi di risparmio energetico;

l) razionalizzare i meccanismi e le strutture deputati alla governance in materia di digitalizzazione, al fine di semplificare i processi decisionali;

m) semplificare le modalità di adozione delle regole tecniche e assicurare la neutralità tecnologica delle disposizioni del CAD, semplificando allo stesso tempo il CAD medesimo in modo che contenga esclusivamente principi di carattere generale;

n) ridefinire le competenze dell'ufficio dirigenziale di cui all'articolo 17, comma 1, del CAD, con la previsione della possibilità di collocazione alle dirette dipendenze dell'organo politico di vertice di un responsabile individuato nell'ambito dell'attuale dotazione organica di fatto del medesimo ufficio, dotato di adeguate competenze tecnologiche e manageriali, per la transizione alla modalità operativa digitale e dei conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;

o) adeguare il testo delle disposizioni vigenti alle disposizioni adottate a livello europeo, al fine di garantirne la coerenza, e coordinare formalmente e sostanzialmente il testo delle disposizioni vigenti, anche contenute in provvedimenti diversi dal CAD, apportando le modifiche necessarie per garantire la coerenza giuridica, logica e sistematica della normativa e per adeguare, aggiornare e semplificare il linguaggio normativo e coordinare le discipline speciali con i principi del CAD al fine di garantirne la piena esplicazione;

p) adeguare l'ordinamento alla disciplina europea in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche;

q) prevedere che i pagamenti digitali ed elettronici effettuati con qualsiasi modalità di pagamento, ivi incluso l'utilizzo per i micropagamenti del credito telefonico, costituiscano il mezzo principale per i pagamenti dovuti nei confronti della pubblica amministrazione e degli esercenti servizi di pubblica utilità;

r) indicare esplicitamente le norme abrogate, fatta salva l'applicazione dell'articolo 15 delle disposizioni sulla legge in generale premesse al codice civile.”

Schema di D.lgs. 20 gennaio 2016 “Schema di Decreto Legislativo recante modifiche e integrazioni al Codice dell'Amministrazione Digitale di cui al Decreto Legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della Legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche”

Legge Regionale 11/2004: “Sviluppo regionale della società dell'informazione”

Art. 5 (Pluralismo informatico) comma 1:

Al fine di garantire ai cittadini la massima libertà di accesso all'informazione pubblica, la Regione promuove attivamente l'uso di formati di documentazione elettronica e di

basi dati su formati non proprietari. La Regione promuove la competitività e la trasparenza del mercato, assumendo quali linea-guida il principio del pluralismo informatico e di libera scelta nella realizzazione di piattaforme informatiche; promuove il riuso di software di cui le pubbliche amministrazioni sono proprietarie ed è impegnata alla riduzione di barriere dovute a diversità di formati non standard nella realizzazione di programmi e delle piattaforme e all'impiego ottimale sia del software a sorgente aperto che di quello a sorgente chiuso nella pubblica amministrazione.

Art. 13 (Sistema informativo della Regione (SIR-ER)):

1. Il Sistema informativo della Regione (SIR-ER) è costituito dal complesso delle basi di dati, dei servizi e delle procedure, finalizzati all'esercizio delle funzioni di governo, di programmazione, di legislazione e di amministrazione della Regione, ed al loro coordinamento con le attività degli enti pubblici operanti nel territorio regionale. Il trattamento dei dati compresi nel SIR-ER è effettuato nel rispetto del decreto legislativo n. 196 del 2003.

2. Il SIR-ER è articolato nei diversi settori di intervento e per i differenti ambiti di conoscenze idonee ad una adeguata rappresentazione della realtà regionale, ivi inclusa la rilevazione grafica delle caratteristiche fisiche del territorio; il sistema è strutturato secondo un'architettura unitaria dei servizi in rete e dei flussi informativi, che ne assicura omogeneità, interoperabilità ed integrazione.

Art. 16 (Modalità di coordinamento e ottimizzazione delle risorse):

1. La Giunta regionale, in coerenza con i criteri generali di cui all'articolo 20, adotta modalità organizzative finalizzate a garantire la programmazione unitaria e integrata degli obiettivi e delle risorse finanziarie destinate allo svolgimento delle attività di cui all'articolo 13. Assicura altresì, tramite le strutture della direzione generale competente, le funzioni di programmazione, sviluppo, coordinamento generale e monitoraggio di cui al comma 2.

2. Le funzioni di programmazione, sviluppo, coordinamento generale e monitoraggio assicurano, in particolare:

a) il supporto alla programmazione delle iniziative per la società dell'informazione, provvedendo all'istruttoria dei documenti di pianificazione, al monitoraggio e al controllo delle iniziative anche locali e settoriali;

b) il supporto alle iniziative di altri enti, l'attuazione per quanto di competenza, il monitoraggio e il controllo;

c) il presidio della coerenza dell'architettura del SIR-ER, l'unitarietà di impostazione delle funzioni tecniche, sia trasversali che settoriali;

d) la programmazione e il coordinamento dell'introduzione del software libero e open source e dell'uso di formati di dati e protocolli di comunicazione aperti o liberi, nonché degli standard indicati dagli enti internazionali preposti;

e) la cura, nell'ambito della lettera b), dello sviluppo e gestione delle infrastrutture e dei servizi di garanzia, della progettazione e realizzazione dei progetti trasversali, degli standard generali di riferimento, dell'assistenza tecnica e della collaborazione per lo sviluppo dei servizi e dei sistemi informativi settoriali e locali, anche su richiesta.

3. I soggetti di cui all'articolo 19, comma 5, lettera a) sono obbligati ad utilizzare le funzioni di archiviazione e conservazione digitale dei documenti informatici svolte secondo quanto disposto dall'articolo 2, comma 1, lettera f bis), della legge regionale n. 29 del 1995.

4. I soggetti di cui all'articolo 19, comma 5, lettera b) hanno la facoltà di utilizzare le funzioni di cui al comma 3.

Determinazione del Direttore Generale all'Organizzazione, Personale, Sistemi Informativi e Telematica n. 4137/2014: "Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna"

Determinazione del Direttore Generale all'Organizzazione, Personale, Sistemi Informativi e Telematica n. 14852/2011: "Disciplinare Tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna"

Delibera di Giunta 2416/2010 "Riorganizzazione della comunicazione web della Regione Emilia-Romagna"

Delibera di Giunta 1394/2010 "Riorganizzazione della comunicazione web della Regione Emilia-Romagna"

Delibera di Giunta 1567/2011 "Linee guida per la comunicazione web regionale"

Delibera di Giunta 1783/2012 "Modello organizzativo per la Governance dei sistemi informativi regionali"

Linee guida per l'integrazione dei sistemi verticali con il sistema documentale regionale:

<https://internos.regione.emilia-romagna.it> (nella sezione "Il protocollo informatico: il sistema di gestione documentale" in Sapere e fare/Funziona così/gestione documentale)

Regole tecniche del Sistema Pubblico per la gestione dell'Identità Digitale - SPID (<http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid>)

Allegati tecnici

Allegato 1: Stack tecnologico delle filiere applicative supportate.

Allegato 1a: Stack tecnologico delle architetture GIS supportate.

Allegato 2: Tecnologie a supporto delle filiere applicative.

Allegato 3: Linee guida per lo sviluppo .NET sui sistemi della Regione Emilia-Romagna.

Allegato 4: Strumenti di supporto e linee guida per sviluppo applicazioni Java EE.

Allegato 5: Clausola “accessibilità” per contratti e capitolati tecnici

Allegato 6: Lista dei requisiti di accessibilità

Allegato 7: Liste di controllo per le misure minime di sicurezza

Allegato 8: Clausola “Sicurezza, privacy e riservatezza” per contratti e capitolati tecnici

Allegato 9: Specifiche tecniche per l'utilizzo del sistema di autenticazione centralizzato

Allegato 9a: Specifiche tecniche per l'utilizzo del sistema di autenticazione federata (fedERa)

Allegato 10: Repository dei sorgenti e tracking

Allegato 11: Linee guida sulla grafica condivisa dei siti web

Allegato 12: Scheda tecnica per nuovo servizio da erogare o fruire tramite Porta di Dominio IcarER

Allegato 13: Specifiche tecniche per l'utilizzo dei web services di consultazione dei dati di personale e strutture

Allegato 14: Schede tecniche: applicativa e sistemi

Allegato 15: Livelli di servizio

Allegato 16: Cookie - normativa e istruzioni operative

Allegato 17: Regole per Sistemi di Riferimento dei dati geografici e nelle applicazioni GIS

Allegato 18: Linee guida per l'integrazione dei sistemi verticali con il sistema documentale regionale

Allegato 1: Stack tecnologico delle filiere applicative supportate.

	Piattaforma Microsoft (Windows Server)	Piattaforma Linux
<u>FILIERA A</u> <u>Applicazioni su</u> <u>tecnologia JAVA</u> <u>(specifiche JEE)</u>		WS: Apache/LBL AS: JBoss DB: PostgreSQL Oracle (anche su Windows Server)
<u>FILIERA B</u> <u>Applicazioni su</u> <u>tecnologia Microsoft</u>	WS: Microsoft IIS/LBL AS: Microsoft .NET DB: MS SQL Server	-
<u>FILIERA C</u> <u>Applicazioni su</u> <u>tecnologia OpenSource</u>	-	WS: Apache/LBL AS: PHP, Python, Perl Tomcat, Ruby Plone (Zope) DB: MySQL, PostgreSQL, Plone (Zeo)
<u>Legenda:</u> WS: Web Server/Bilanciatore di carico – AS: Application Server – DB: Database Server		

Nel caso sia necessario fornire il dettaglio (ad esempio nei capitolati o nei contratti) delle versioni supportate dell'application server, web server e db server è possibile richiedere le informazioni al Servizio SIIR.

Le versioni dei prodotti indicati in tabella, essendo soggetti ad aggiornamenti periodici, verranno comunicate su richiesta.

Allegato 1a: Stack tecnologico delle architetture GIS supportate.

Architettura GIS proprietaria	<u>WEB SERVER</u>	<u>APPLICATION SERVER</u>	<u>SERVER GIS</u>	<u>DB GIS</u>
<u>Piattaforma Linux</u>	<i>LBL</i>	<i>JBOSS</i>	<i>ArcSDE</i>	<i>PostgreSQL (+/- PostGis)</i>
<u>Piattaforma Microsoft (Windows Server)</u>	-	-	<i>ArcSDE ArcGis Server for Java / ArcIMS Tomcat (gestione interna/Handler)</i>	<i>Oracle</i>

Architettura GIS Open Source	<u>WEB SERVER</u>	<u>APPLICATION SERVER</u>	<u>SERVER GIS</u>	<u>DB GIS</u>
<u>Piattaforma Linux</u>	<i>LBL</i>	<i>JBOSS</i>	<i>GeoServer su Jboss</i>	<i>Oracle Spatial o PostGis + Post- greSQL</i>
<u>Piattaforma Microsoft (Windows Server)</u>	-	-	-	<i>Oracle Spatial</i>

Nel caso sia necessario fornire il dettaglio (ad esempio nei capitolati o nei contratti) delle versioni supportate è possibile richiedere le informazioni al Servizio SIIR.

Le versioni dei prodotti indicati in tabella, essendo soggetti ad aggiornamenti periodici, verranno comunicate su richiesta.

Allegato 2: Tecnologie a supporto delle architetture e filiere applicative

1. Introduzione.....	2
2. Tecnologie di storage.....	2
3. Tecnologie di virtualizzazione.....	2
4. Tecnologia vCloud.....	3
5. Tecnologie di backup.....	6
6. Tecnologie di monitoring e management.....	6
7. Tecnologia Blade.....	6

1. Introduzione

Scopo di questo documento è quello di fornire un quadro sintetico delle tecnologie hardware e software adottate nel Datacenter regionale di Viale Aldo Moro 52 relativamente alle infrastrutture Server e Storage con un focus privilegiato sulle architetture di virtualizzazione.

2. Tecnologie di storage

Al fine di conseguire una maggiore disponibilità dei dati, una metodologia di accesso standardizzata, una maggiore sicurezza ed una centralizzazione della gestione e del controllo, è stata introdotta una infrastruttura di Storage Area Network (SAN) per i dati delle filiere applicative. Unitamente alla SAN è stata adottata la tecnologia di virtualizzazione dello storage che consente un notevole efficientamento sia nelle prestazioni che nella gestione. La gestione centralizzata che ne deriva comporta tutta una serie di vantaggi operativi rispetto allo storage locale, in particolare:

- **Scalabilità:** dell'ordine delle centinaia di TeraByte
- **Performance:** connessioni veloci grazie alla tecnologia Fibre Channel
- **Flessibilità:** espansione dinamica dello storage, nessun downtime per l'aggiunta di dischi
- **Backup:** ridotto tempo di ripristino dei dati in caso di failure
- **Fault Tolerance:** funzionalità avanzate di mirroring dei dischi
- **Availability:** affidabilità e continuità di Servizio basate su ridondanza di bus, alimentazioni, controller, ..
- **Virtualizzazione:** funzionalità che permette di separare completamente lo strato fisico da quello logico andando a creare, on-demand e con poche operazioni da interfaccia utente, spazio disponibile ai server
- **Security:** maggiore sicurezza nella protezione dei dati a livello fisico ed applicativo

3. Tecnologie di virtualizzazione

Per i 3 livelli fisici di una infrastruttura applicativa di test / sviluppo 3-tier si è optato per la tecnologia di virtualizzazione Vmware su sistemi dipartimentali High Level. Una soluzione su tale piattaforma tecnologica comporta numerosi vantaggi, in particolare:

- **Indipendenza dall'hardware:** il layer VMWARE maschera il tipo di hardware fisico presente sul server, per cui il sistema operativo ospite vede e usa quello standard virtualizzato
- **Isolamento dell'ambiente applicativo:** gli ambienti sono completamente indipendenti (sistema operativo, registry, dati, ecc.) per cui un crash o errore applicativo su un server virtuale non compromette in alcun modo l'integrità degli altri
- **Incapsulamento:** l'intero stato di una macchina virtuale (memoria, dischi, ecc.) risiede su dei files che possono essere gestiti agevolmente ripristinando velocemente la configurazione voluta
- **Management:** possibilità di management centralizzato di tutte le macchine virtuali. Riconfigurazione e riallocazione dinamica delle macchine virtuali su altre macchine fisiche senza interruzione di Servizio
- **Clustering:** possibilità di configurare ambienti cluster tra macchine virtuali usando soluzioni di clustering industry-standard. Si possono creare cluster tra macchine virtuali dello stesso server fisico o di server fisici diversi o ancora tra server fisico e macchina virtuale
- **Ottimizzazione:** tramite la tecnologia di virtualizzazione si ottiene un utilizzo ottimale delle risorse hardware assegnate ai progetti di sviluppo
- **Provisioning:** la tecnologia di virtualizzazione permette di accelerare notevolmente l'assegnazione degli ambienti di test/sviluppo alle strutture di sviluppo
- **Business Continuity e Disaster Revocery:** ottenibile agevolmente andando a replicare l'infrastruttura fisica su un sito secondario a garanzia della continuità operativa o per la ripartenza dopo eventi disastrosi
- **Cloud:** tutte le caratteristiche della virtualizzazione rese disponibili alle strutture in autonomia, ovvero partizionamenti del data center virtualizzato e reso disponibile attraverso un portale intranet in modo da poter creare e gestire autonomamente macchine virtuali, gruppi di macchine e sottoreti

4. Tecnologia vCloud

L'Ente Regione ha scelto il Cloud Computing per la fornitura di risorse IT "classiche" (ad esempio, Capacità computazionale, memoria, storage, piattaforme operative, ecc.) mettendo a disposizione un ambiente di virtualizzazione in grado di offrire ai clienti interni (Cloud consumers) una Cloud Farm in grado di garantire i principali punti di forza del Cloud:

- Self-service;
- Risorse condivise;
- Elasticità;
- Servizi monitorati.

Self-service

Il Servizio Informativo-Informatico regionale (SSIIR) ha attivato un portale web ove gli utenti abilitati possono creare e gestire le proprie macchine virtuali all'interno di slot resi disponibili nel proprio spazio, secondo gli accordi presi tra il Servizio richiedente, Cloud consumer, ed il SSIIR, Cloud provider. Il portale self-service permette la scelta del sistema operativo, della capacità elaborativa, della memoria e di ogni altro aspetto tecnico della macchina virtuale. Il deploy della stessa avviene attraverso un processo automatico, richiesto dal Cloud consumer alla fine della procedura ed approvato da un Amministratore di sistema.

Risorse condivise

Le risorse hardware dedicate alla Cloud Farm sono state scelte in base a diversi criteri tecnici ed economici, tra i quali: affidabilità, scalabilità, costo di acquisto, semplicità di gestione, protezione dell'investimento.

Ad oggi la Farm si avvale di server blade e storage di classe midrange, ottimali per garantire dinamicità, ridondanza e resilienza.

Attraverso l'utilizzo di hypervisors di ultima generazione è stato attivato il substrato di virtualizzazione necessario alla creazione della Cloud Farm; tale substrato è quello preposto alla condivisione delle risorse.

Elasticità

All'interno della proprio spazio Cloud, gli utenti abilitati possono gestire le risorse rilasciate in autonomia. Gli slot disponibili per le macchine virtuali possono quindi essere customizzati nel rispetto dei limiti massimi di capacità elaborativa, memoria, storage e di tutti gli altri parametri previsti. Le risorse possono quindi essere fornite alle macchine virtuali anche elasticamente, ovvero in modalità on-demand.

Servizi monitorati

Uno dei motori primi che hanno dato vita alla filosofia Cloud è proprio la capacità intrinseca di misurare le risorse utilizzate da ogni singolo Cloud consumer. La misurazione è quindi aspetto fondamentale perché abilitante alla rendicontazione. Quest'ultima è attualmente in fase di sviluppo da parte del SSIIR.

L'introduzione delle tecnologie di Cloud Computing trasforma l'Ente Regione in un vero e proprio Service Provider in grado di erogare ai propri clienti server virtuali, storage, piattaforme applicative delegandone la gestione al cliente stesso nell'ambito di un pool di risorse definito.

La scelta di un Cloud Privato interno all'Ente piuttosto che uno esterno Privato o Pubblico, è legata alla notevole complessità normativa in fatto di responsabilità e garanzia della privacy di cui tenere conto nel momento in cui ci si avvale di Cloud Provider esterni.

In fatto di privacy la scelta di una Cloud Farm interna apporta una notevole semplificazione vedendo coincidere il soggetto che tratta i dati con il proprietario delle infrastrutture.

L'Ente Regione ha quindi attivato una Cloud Farm integrata nell'infrastruttura di virtualizzazione preesistente e già utilizzata dalla Giunta e dall'Assemblea Legislativa. I principali vantaggi sono:

- Soluzioni standardizzate per la Business Continuity e il Disaster Recovery;
- Maggiore efficienza ed efficacia nei processi di change management, patch management, hardening, incident management, security assessment e security testing.

Ad oggi è possibile attivare la fornitura di soluzioni *IaaS, PaaS e Custom*

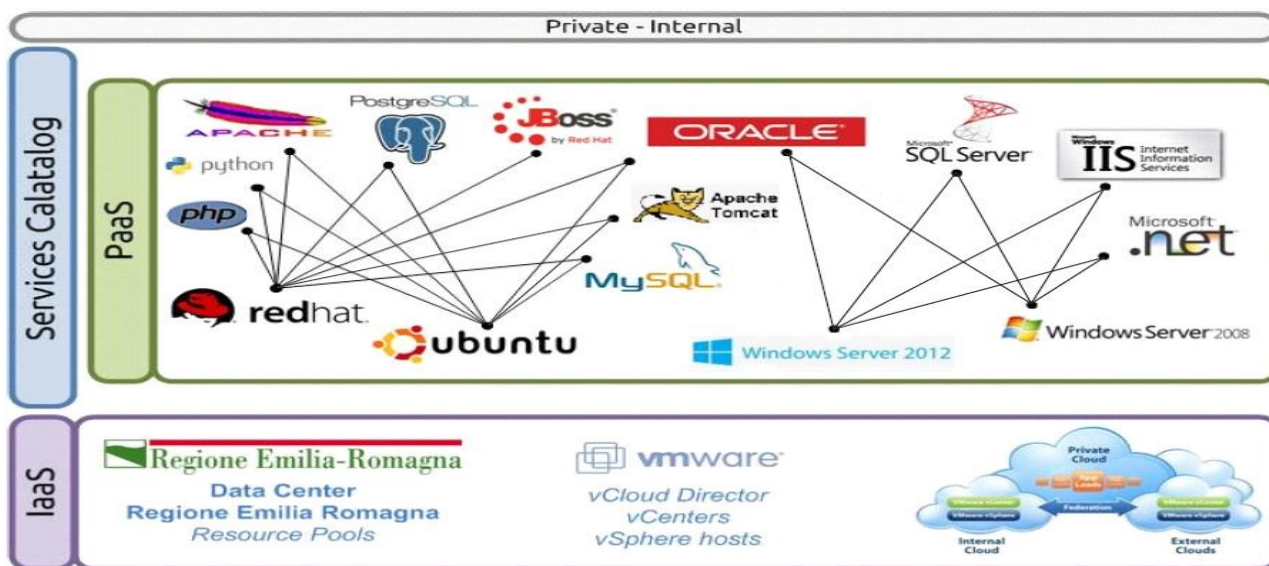
Le soluzioni IaaS e PaaS debbono essere riconducibili alla matrice sotto riportata e si possono applicare agli:

- Ambienti di sviluppo, test e collaudo.
- Ambienti di produzione.

Per le soluzioni che prevedono **piattaforme riconducibili alla Filiera B** il “cliente” dovrà preventivamente dotarsi delle licenze software necessarie.

	Piattaforma Microsoft (Windows Server)	Piattaforma Linux
FILIERA A <u>Applicazioni su tecnologia JAVA (specifiche JEE)</u>		WS: Apache AS: JBoss DB: PostgreSQL Oracle (anche su Windows Server)
FILIERA B <u>Applicazioni su tecnologia Microsoft</u>	WS: Microsoft IIS AS: Microsoft .NET DB: MS SQL Server	-
FILIERA C <u>Applicazioni su tecnologia OpenSource</u>	-	WS: Apache/LBL AS: PHP, Python, Perl Tomcat, Ruby Plone (Zope) DB: MySQL, PostgreSQL
Custom	Tecnologie custom anche non in filiera che richiedono analisi di fattibilità.	
Legenda: WS: Web Server/Bilanciatore di carico – AS: Application Server – DB: Database Server		

Si configura pertanto una vera e propria offerta di servizi IaaS e PaaS così articolata:



Condizioni per l'accesso alla piattaforma cloud

L'accesso ai servizi di Cloud Computing è sottoposto all'analisi, da parte del SSIIR, delle caratteristiche delle applicazioni e piattaforme operative che il richiedente intende implementare. Normalmente l'accesso alla Cloud Farm è consentito per le seguenti casistiche:

- *struttura organizzativa del richiedente dotata di una o più figure professionali in grado di gestire in autonomia server virtuali, storage e middleware a fronte di un Catalogo di risorse e servizi da cui si può attingere per predisporre l'ambiente operativo. Le soluzioni applicative debbono privilegiare il rispetto delle Filiere applicative standard di cui alla matrice precedente (filiera A, B, C) e su cui sono costruiti i servizi IaaS e PaaS;*

- soluzioni transitorie per sviluppo e testing di servizi ad hoc, prodotti di mercato e progetti pilota. Si accetta la deroga dalle filiere applicative standard e possono essere implementate soluzioni *Custom*. Per tali soluzioni deve essere definita una durata temporale al termine della quale le macchine virtuali vengono spente ed eliminate (pervio backup);
- soluzioni di mercato che non rientrano nell'ambito delle filiere applicative standard e che si configurano come soluzioni *Custom*.

A seguito della verifica dei prerequisiti tecnologici e funzionali per l'accesso alla Cloud Farm, la struttura richiedente può scegliere anche la tipologia di servizio per la gestione delle macchine virtuali (PaaS) e della propria infrastruttura (IaaS). Tale livello di servizio può comprendere alcune operazioni di amministrazione dei sistemi che l'organizzazione richiedente può scegliere di "esternalizzare" demandandole al Servizio Informatico, ad esempio:

- Deploy e configurazione del sistema operativo;
- Patching di sistema operativo;
- Hardening;
- Manutenzione ordinaria programmata;
- Manutenzione straordinaria;

Il Service Provider, ovvero il SSIIR, si impegna a mantenere aggiornato il Catalogo dei Servizi sulla piattaforma Cloud e garantisce il backup e la restore degli ambienti operativi attivati dal Cliente.

Inoltre, a fronte di richiesta motivata, il Service Provider si impegna a valutare la possibilità di ampliare il pool di risorse computazionali e di storage messe inizialmente a disposizione del Cloud Consumer ed a procedere nel caso ciò sia possibile (anche per periodi limitati nel tempo).

Cosa si può fare dal Portale Self-Service

I Cloud consumers abilitati al portale self-service possono accedere alla console web-based, raggiungibile utilizzando browser certificati come Mozilla Firefox oppure Microsoft Internet Explorer, per la gestione della propria infrastruttura virtuale, essendo gli utenti autonomi per le attività ordinarie da eseguire sui server virtuali. L'accesso alla console è garantito attraverso la definizione di ruoli, in modo da differenziare gli utenti di uno stesso gruppo, ed ogni Servizio o organizzazione che accede ai servizi in Cloud, ha un proprio URL riservato.



Dal pannello principale è possibile verificare e gestire lo stato delle proprie macchine virtuali, oltre che gestirne la configurazione e le performance attraverso apposita sezione. Le macchine virtuali vengono raggruppate in "contenitori" chiamati vApp nei quali potremmo inserire diversi server virtuali che compongono a loro volta i servizi; ad esempio potremmo avere un web server ed un database server che erogano servizi web. Essendo questi ultimi all'interno della stessa vApp, l'utente può impostare dei meccanismi automatici in modo tale da avviare prima le macchine virtuali propedeutiche al servizio, ad esempio un database server, poi la macchina che ospita il web server. Dal portale è possibile creare nuove vApp utilizzando template di server virtuali già pronte. Il Cloud consumer ha inoltre la possibilità di caricare template di server virtuali ad-hoc in formato OVF (standard per la creazione e la distribuzione di sistemi virtuali). Vi è inoltre la possibilità di dare una "scadenza" alle vApp al termine della quale non saranno più disponibili e si potrà decidere se eliminarle definitivamente o rimetterle in produzione (utile per gli ambienti di test e collaudo temporanei). Oltre alla gestione dei server virtuali è possibile monitorarne l'utilizzo delle risorse, cosa fondamentale vista la filosofia di base sulla

rendicontazione delle stesse.

5. Tecnologie di backup

Da diversi anni è stata implementata una soluzione IBM di backup centralizzato per tutti i sistemi server dipartimentali presenti al CED. Si tratta di una soluzione integrata per la gestione dello storage distribuito che opera con funzioni di backup/restore di files, database ed applicazioni. Questa soluzione protegge files, database ed applicazioni per i server in ambiente fisico e virtuale.

Dal 2015 è attiva una nuova soluzione di backup centralizzato, Commvault, che affianca alla soluzione IBM e viene al momento utilizzata per il backup dei server virtuali. Tale soluzione si integra con gli Hypervisor di virtualizzazione (vmware, microsoft hyper-v) e consente il backup dell'intera macchina virtuale rendendo i tempi di restore significativamente contenuti.

6. Tecnologie di monitoring e management

Per le piattaforme di produzione e di test / sviluppo dedicate alle filiere applicative sono implementati strumenti di monitoring e di management per la gestione dei livelli di servizio hardware / software. Queste tecnologie comprendono il monitoraggio in tempo reale ma anche l'analisi d'infrastruttura ed il capacity management.

7. Tecnologia Blade

Per i 3 livelli fisici di una infrastruttura applicativa di produzione 3-tier (in pratica web server, application server e database server) si è optato per la tecnologia Blade. I blade sono dei server particolarmente sottili costruiti per essere inseriti nei bay di chassis appositamente predisposti che si connettono ad un backplane comune. Tali server sono dotati di propri processori, RAM, controller di rete, dischi e sono dunque indipendenti, ma condividono i componenti di alimentazione e raffreddamento, i floppy drive e gli switch con gli altri blade.

Una soluzione su tale piattaforma tecnologica comporta numerosi vantaggi che risultano abilitanti verso gli obiettivi di scalabilità e fault tolerance, in particolare:

- **Elevati livelli di densità:** un numero elevato di blade server è allocabile in un singolo chassis (o enclosure) consentendo di raggiungere un grado di densità molto più elevato rispetto ai server tradizionali. I blade costituiscono l'elemento ideale per la realizzazione di infrastrutture che implementino architetture avanzate di tipo clustered ed in generale per il load balancing
- **Deployment veloce:** la tecnologia blade consente di operare il deployment di un nuovo server con estrema rapidità: da un punto di vista fisico si inserisce un nuovo blade nel rack con necessità di cablaggio ridotte al minimo; da un punto di vista software l'ausilio di sofisticati strumenti di management consente di caricare l'immagine del sistema operativo e dell'applicazione in modo automatizzato.
- **Facilità di manutenzione:** la manutenzione fisica dei server blade risulta facilitata dal fatto che in caso di failure un blade è estraibile dal rack in modo non dissimile da un disco hot swap. La tecnologia blade si accompagna a sistemi di manutenzione che consentono di gestire intere batterie di server da console amministrative centralizzate con possibilità di generare in automatico messaggistica relativa a malfunzionamenti hardware/software e in alcuni casi di operare "predictive failure management".
- **Scalabilità modulare:** la scalabilità di un sistema basato su di un'architettura blade si basa sul concetto di "scale out" in luogo del tradizionale "scale up". Operare in "scale up" significa dover potenziare l'unico server di cui si dispone nell'ambito dell'espandibilità da esso consentita e, una volta raggiunti i limiti massimi, è necessario ricorrere ad un server di fascia più alta. Lo "scale out" è una modalità estremamente più flessibile in quanto ad un'accresciuta esigenza di risorse elaborative consente di rispondere semplicemente aggiungendo moduli standard (blade) uguali a quelli già impiegati e di costo contenuto, fino al raggiungimento dell'obiettivo di performance prefissato.

Allegato 3: Linee guida per lo sviluppo .NET sui sistemi della Regione Emilia-Romagna.

1	Introduzione	2
2	Autenticazione e autorizzazione	2
3	Il namespace <i>RER.Tools</i>	2
4	Utilizzo del DB Server	2
4.1	Creazione di connessioni	2
4.1.1	Configurazione di SqlConnectionBroker	3
4.2	Chiusura delle connessioni e “data readers”	3
4.3	SQL Injection e creazione di statement SQL dinamici	4
5	Gestione delle eccezioni	5
5.1.1	Utilizzo in una Web Application	5
5.1.2	Utilizzo in una Console application	6
5.1.3	Utilizzo in una Windows Form application	7
6	Invio di email	7
6.1	<i>RER.Tools.Mail</i>	7
6.1.1	Recipient	8
6.1.2	SmtMail	8
6.1.3	Metodi d'utilità	9
7	<i>RER.Tools.DirectoryServices</i>	10
7.1	AdsiHelper	10
7.2	AdsiUserHelper	10
7.3	AdsiGroupHelper	13
7.4	AdsiComputerHelper	13
7.5	AdsiOrganizationalUnitHelper	14
8	Altro	14
8.1	<i>RER.Tools.Sql</i>	14
8.2	<i>RER.Tools.StringWriterWithEncoding</i>	15
8.3	<i>RER.Tools.Security.ImpersonateUser</i>	16
8.4	<i>RER.Toos.UrlNormativa</i>	16
8.5	Creazione di documenti PDF lato server	17
8.6	Generazione di reportistica lato server	17
9	Installazione e configurazione di <i>RER.Tools</i>	17
9.1	DB per l'ApplicationLogger	18

1 Introduzione

Questo documento ha lo scopo definire le linee guida per lo sviluppo di applicazioni .NET che dovranno essere ospitate sui server della Regione Emilia-Romagna.

Data l'inerente flessibilità/varietà delle soluzioni realizzabili tramite il software, ci si rende conto che quanto scritto in questo documento può non prevedere situazioni per cui i requisiti qui descritti risultino non soddisfacenti o rendano impossibile raggiungere gli obiettivi che il sistema si propone di raggiungere. In questi casi è comunque necessario comunicare al personale tecnico della Regione la situazione affinché si possa discutere insieme la soluzione migliore da adottare.

2 Autenticazione e autorizzazione

In Regione Emilia-Romagna sono presenti due domini "Active Directory", uno contenente gli account degli utenti regionali (dominio intranet: RERSDM) e l'altro contenente account di utenti esterni alla regione (dominio extranet: EXTRARER), e un sistema centralizzato di autenticazione (vedi Allegato 9). Deve essere prevista la gestione delle autorizzazioni ad un livello precedente a quello del DB: quindi nella pagine ASP.NET o nei componenti della business logic.

I meccanismi di autenticazione integrata verranno supportati per applicazioni disponibili all'interno del dominio regionale, le applicazioni esposte su Internet/CNER useranno meccanismi di autenticazione base su protocollo sicuro HTTPS.

3 Il namespace RER.Tools

RER.Tools è il namespace che contiene una serie di componenti da utilizzare affinché le applicazioni siano conformi ai requisiti oggetto di questo documento.

Per i dettagli sistemistici relativi a come eseguire l'installazione degli assemblies che compongono RER.Tools si veda il capitolo apposito.

4 Utilizzo del DB Server

4.1 Creazione di connessioni

Per ragioni di sicurezza, di gestione delle stringhe di connessione in fase di deployment, e di problemi di *delegation* tra il web server e il DB server; qualsiasi connessione al DB server (SQL Server) deve avvenire attraverso il componente **RER.Tools.SqlConnectionBroker**.

L'utilizzo di tale componente è banale, basta passare il nome del DB:

```
SqlConnection cn = RER.Tools.SqlConnectionBroker.GetConnection("NomeDB");
```

oppure

```
SqlConnection cn = RER.Tools.SqlConnectionBroker.GetConnection("NomeDB", true);
```

per ottenere una connessione già aperta.

Al fine di rendere minimi gli interventi nel caso di modifiche sul DB server è opportuno centralizzare, il nome del database. Occorre creare una classe di nome *Global* in cui mettere informazioni globali, come è il nome del database:

```
public class Global
```

```
{
    public const string DBName = "NomeDB";
}
```

pertanto gli esempi sopra indicati diventano:

```
SqlConnection cn = RER.Tools.SqlConnectionBroker.GetConnection(Global.DBName);
SqlConnection cn = RER.Tools.SqlConnectionBroker.GetConnection(Global.DBName, true);
```

4.1.1 Configurazione di SqlConnectionBroker

La configurazione del SqlConnectionBroker (da inserire nel .config file dell'applicazione) avviene applicazione per applicazione e deve essere concordata con il personale tecnico della Regione. Comunque il componente decide con quali credenziali creare la connessione al DB in base al gruppo di appartenenza dell'utente che sta facendo la richiesta.

La configurazione più semplice (che permette a tutti l'accesso, i.e. *allowAnonymous="true"*) ha il seguente aspetto:

```
<RER>
  <SqlConnectionBrokerSettings version="1.2">
    <DB
      name="Comunicati"
      catalog="Comunicati"
      applicationName="Gestione comunicati stampa"
    >
      <Credential
        allowAnonymous="true"
        userName="..."
        password="..."
        isCrypted="false" />
    </DB>
  </RER>
```

Il componente permette configurazioni più sofisticate e anche che un'applicazione acceda a più di un database (sempre SQLServer), ma come già detto, la creazione di questa configurazione va concordata con il personale tecnico della Regione.

4.2 Chiusura delle connessioni e "data readers"

E' tassativo chiudere sempre le connessioni. Per maggiore sicurezza si richiede anche l'utilizzo del costrutto *using* tipico di C#. Esso garantisce la chiamata all'interfaccia *IDisposable*, e ciò assicura che le risorse siano liberate il prima possibile e non solo durante la Garbage Collection.

Esempio:

```
public static bool IsProtocollato(int idComunicato)
{
    using (SqlConnection sqlConnection = SqlConnectionBroker.GetConnection(Global.DBName,
true))
    {
        SqlCommand cmd = new SqlCommand("Comunicato_IsProtocollato", sqlConnection);
        cmd.CommandType = CommandType.StoredProcedure;

        cmd.Parameters.Add("@id_comunicato", SqlDbType.Int).Value = idComunicato;
        cmd.Parameters.Add("@protocollato", SqlDbType.Bit);

        cmd.Parameters["@protocollato"].Direction = ParameterDirection.InputOutput;

        cmd.ExecuteNonQuery();
        cmd.Connection.Close();
    }
}
```

```
        return (bool) cmd.Parameters["@protocollato"].Value;
    }
}
```

Nel caso si debba restituire un `SqlDataReader` o `IDataReader`, la connessione deve essere chiusa dal "client". In questi casi assicurarsi di aggiungere l'opzione `CommandBehavior.CloseConnection` nel metodo di esecuzione del `SqlCommand`.

NB: non restituire esattamente un oggetto di tipo `SqlDataReader` bensì l'interfaccia `IDataReader` (da esso implementata). Ciò al fine di minimizzare gli interventi in caso di cambiamento del database server.

```
public static IDataReader ElencaUltimi(
    string idStruttura,
    int nrOre,
    bool soloProtocollati)
{
    using (
        SqlCommand cmd = new SqlCommand(
            "Comunicato_ElencaUltimi",
            SqlConnectionBroker.GetConnection(Global.DBName, true)
        )
    )
    {
        cmd.CommandType = CommandType.StoredProcedure;

        cmd.Parameters.Add("@id_struttura", SqlDbType.VarChar, 10).Value = idStruttura;
        cmd.Parameters.Add("@nr_ore", SqlDbType.Int).Value = nrOre;
        cmd.Parameters.Add("@solo_protocollati", SqlDbType.Bit).Value = soloProtocollati;

    }

    return
        cmd.ExecuteReader(CommandBehavior.CloseConnection|CommandBehavior.SingleResult);
}
}
```

Per quanto detto sopra, l'interfaccia `IDataReader` deve essere usata anche dal "client", rispetto all'esempio precedente, il "client" dovrà eseguire qualcosa del genere:

```
IDataReader reader = ComunicatoManager.ElencaUltimi(idStruttura, nrOre, false);
while (reader.Read())
{
    // ...
}
reader.Close();
```

oppure

```
myGrid.DataSource = ComunicatoManager.ElencaUltimi(idStruttura, nrOre, false);
((IDataReader) myGrid.DataSource).Close();
```

4.3 SQL Injection e creazione di statement SQL dinamici

La regola generale è di utilizzare sempre e solo delle stored procedure, ovvero non creare mai delle stringhe SQL a livello di logica applicativa. A volte questo non è però possibile. La situazione tipica sono i moduli di ricerca libera e/o avanzata, quelli in cui l'utente può mettere diversi tipi di parametri di ricerca. In quei casi creare una SP i cui parametri riescano a soddisfare tutte le possibili richieste è molto difficile se non impossibile.

In tal caso occorrerà comporre lo statement SQL dinamicamente (all'interno della logica applicativa), però tramite ADO.NET ciò può essere fatto in maniera più elegante e soprattutto in maniera sicura rispetto ai problemi di Sql Server Injection, in quanto è possibile definire nei SqlCommand di tipo CommandText dei parametri formali (non i semplici "?" che dava a disposizione ADO). Un esempio chiarisce subito: anziché scrivere una cosa del genere:

```
cmd.CommandText += " AND campo LIKE '%" + valoreDaCercare.Replace("'", "") + "'";
```

si può scrivere:

```
cmd.CommandText += " AND campo LIKE @valoreDaCercare";  
cmd.Parameters.Add("@valoreDaCercare", SqlDbType.VarChar, 255).Value =  
    "%" + valoreDaCercare + "%";
```

Nonostante ci sia più codice da scrivere ci sono i seguenti vantaggi:

non occorre raddoppiare l'apice singolo (è quindi immediatamente "Sql Injection Safe")

si associa un tipo al parametro (in questo caso VarChar) e ciò rende più robusto il sistema (sempre più "Sql Injection Safe")

lo stesso parametro può essere usato più volte nel commandText senza per questo doverlo

aggiungere più volte alla collection dei parameters (cosa che succedeva con ADO)

l'esecuzione è più veloce in quanto Sql Server genera una SP temporanea che riesce anche a riutilizzare

il codice è più leggibile.

NB: Nel caso ci si trovasse comunque nella condizione di dovere esplicitamente raddoppiare l'apice per mettere un valore in una stringa rappresentante dell'SQL utilizzare, anziché il metodo *string.Replace*, la funzione *RER.Tools.Sql.MakeSafe*. Al momento, essa, non fa altro che raddoppiare l'apice singolo, ma in futuro, per garantirsi contro nuovi tipi di attacchi di tipo Sql Injection, l'aver utilizzato questa funzione, permette di intervenire velocemente su tutte le applicazioni.

5 Gestione delle eccezioni

Come indicato dalla Microsoft, tutte le eccezioni specifiche dell'applicazione *devono* essere delle ApplicationException o derivare da essa.

La gestione delle eccezioni deve avvenire utilizzando i servizi dei componenti definiti in ***RER.Tools.ApplicationLogger***.

In questo namespace sono definite le classi da usare per ottenere un sistema centralizzato per la raccolta degli errori delle applicazioni in produzione (durante lo sviluppo non lo si attiva, ma deve essere comunque previsto). Gli errori vengono registrati su un DB e il responsabile dello sviluppo viene avvisato via email.

Tutto questo serve per monitorare il funzionamento dell'ambiente in produzione (per esempio per rendersi conto nel caso ci sia un tentativo d'attacco di un hacker) e per nascondere all'utente finale i dettagli degli errori non previsti (gli si dà solo una comunicazione generica).

5.1.1 Utilizzo in una Web Application

Per utilizzare il componente in una web application è sufficiente gestire l'evento globale (definito nel file Global.asax) Application_Error:

```
protected void Application_Error(Object sender, EventArgs e)  
{  
    #if(!DEBUG)  
        Exception exception = Server.GetLastError();  
        // Server.GetLastError() ritorna sempre una "HttpException",
```

```

// per accedere all'eccezione vera e propria occorre recuperare l'InnerException
if (exception != null && exception.InnerException != null)
    exception = exception.InnerException;
try
{
    RER.Tools.ApplicationLogger.WebApplicationLogger.LogEvent(
"Interfaccia per la gestione dei comunicati stampa",
this,
exception
);
    Server.ClearError();
    if (exception is ApplicationException)
        Response.Redirect(
string.Format("ErroreApplicazione.aspx?msg={0}", Server.UrlEncode(exception.Message));
    else
        Response.Redirect("ErroreSistema.htm");
}
catch
{
    // Se si è riusciti a loggare non resta che mostrare l'errore anche all'utente
    throw exception;
}
#endif
}

```

Come si vede il codice viene compilato solo se non si è in debug.

Si estrae da `Server.GetLastError` l'InnerException perchè questa funziona "wrappa" l'eccezione vera e propria in una `HttpUnhandledException`.

Si passa l'eccezione al logger assieme al riferimento alla `HttpApplication` (`this`).

Si controlla quindi se l'eccezione è una `ApplicationException`, in questo caso se ne mostra la descrizione all'utente (tramite un redirect alla pagina `ErroreApplicazione.aspx` che deve essere prevista). Quindi in pratica occorre generare delle `ApplicationException` al fine di fornire all'utente una segnalazione di errori coerenti. Per tutte le altre eccezioni (quelle generate dal CLR) si mostra una pagina d'errore generica (`ErroreSistema.htm`, che deve essere prevista) in cui si avvisa che c'è stato un problema e che gli amministratori sono stati avvisati.

NB: E' necessario che la pagina di segnalazione di un'eccezione non di tipo `ApplicationException` sia una pagina statica HTML. Se fosse una pagina ASPX, lo stesso inconveniente che ha generato l'eccezione potrebbe ripresentarsi all'esecuzione della pagina di segnalazione dello stesso.

5.1.2 Utilizzo in una Console application

In una console application (tipicamente si tratterà di job non interattivi) l'approccio è simile a quello delle web application, ma esiste un'altra classe. Al fine di intrappolare tutte le eccezioni non gestite usare l'evento `AppDomain.CurrentDomain.UnhandledException`. Segue l'esempio:

```

[STAThread]
static int Main(string[] args)
{
    #if(!DEBUG)
        AppDomain.CurrentDomain.UnhandledException +=
new UnhandledExceptionHandler(GestoreEccezioni);
    #endif
    // Per il formato di output delle date (utile se questo prg è schedulato)
    RER.Tools.Globalizer.SetThreadSpecificCulture("it-IT");

    Console.WriteLine("---- INIZIO ELABORAZIONE ({0}) ----", DateTime.Now);
}

```



```
// ...

Console.WriteLine("---- FINE ELABORAZIONE ({0}) ----", DateTime.Now);
Console.WriteLine();
return 0;

}

static void GestoreEccezioni(object sender, UnhandledExceptionEventArgs args)
{
    Exception e = (Exception) args.ExceptionObject;
    Console.WriteLine(e.Message);
    Console.WriteLine("---- FINE ELABORAZIONE CON ERRORI ({0}) ----", DateTime.Now);
    Console.WriteLine();
    RER.Tools.ApplicationLogger.ConsoleApplicationLogger.LogEvent(e);
    Environment.Exit(1);
}
```

Al ConsoleApplicationLogger non occorre passare niente altro che l'eccezione in quanto tutte le informazioni che servono sono accessibili tramite la classe *Environment*.

5.1.3 Utilizzo in una Windows Form application

Per ora non è previsto nessun componente specifico per gli errori delle Windows Form application, utilizzare il componente ConsoleApplicationLogger.

6 Invio di email

Visto che in Regione Emilia-Romagna non è installata la libreria CDO, prima di inviare un'email è necessario impostare l'SMTP server: è sufficiente impostare la proprietà statica *SmtpServer* della classe *SmtpMail* col nome del nuovo server. Il nome dell'SMTP Server è stato comunque centralizzato, in pratica è sufficiente la seguente istruzione prima di inviare l'email:

```
SmtpMail.SmtpServer = RER.Tools.Configuration.SMTPServer;
```

Mail Multipart

La creazione di mail multipart (testo e HTML) avviene in modo automatico se è impostata ad HTML (tipo enum per *MailFormat*) la proprietà *BodyFormat* del *MailMessage*. In particolare viene generato sia il body in formato HTML, sia quello in plain-text rimuovendo i tag ipertestuali.

6.1 **RER.Tools.Mail**

Questo namespace contiene le classi per la gestione dell'invio di messaggi di posta elettronica. E' particolarmente utile quando si invia un'email a molti indirizzi, infatti il metodo *Send* della classe *SmtpMail* (in *RER.Tools.Mail*) spezza l'invio di un messaggio in tanti invii ognuno dei quali contiene al massimo un certo numero di indirizzi. Questo valore è di default *RER.Tools.Configuration.MaxRecipientsPerMessage* oppure lo si può passare esplicitamente. A seguito dell'invio è poi possibile ottenere in dettaglio (destinatario per destinatario) cosa è successo. Il tutto è basato sulla classe *Recipient*.

6.1.1 Recipient

Questa classe è utilizzata sia per indicare le informazioni di un destinatario (proprietà *Email* e *Name*) che per ottenere l'esito dell'invio (proprietà *Status* e *Exception*).

La proprietà *Status* è un'enumeration definita nel seguente modo:

```
public enum RecipientStatus
{
    Uninitialized,           // Stato iniziale
    InitializedAndChecked, // Inizializzato e indirizzo sintatticamente corretto
    Queued,                 // Messaggio trasmesso all'SMTP server
    Error                   // Problemi, vedere la proprietà 'Exception'
}
```

Quando occorre inviare un'email creare uno o più oggetti Recipient (nel caso si tratti di più indirizzo, raggrupparli in un ArrayList). Invocare quindi uno dei metodi della classe SmtMail definita più sotto), essa tenta l'invio e imposta la proprietà Status (ed eventualmente la proprietà Exception). Pertanto è possibile sapere cos'è successo all'invio.

Esempio:

```
ArrayList recipients = new ArrayList();
recipients.Add(new Recipient("tizio@dominio.com"));
recipients.Add(new Recipient("caio@dominio.com "));
System.Web.Mail.MailMessage message = new System.Web.Mail.MailMessage();
message.Body = "Prova (Corpo)";
message.Subject = "Prova";
RER.Tools.Mail.SmtMail.Send(message, recipients);
foreach (Recipient r in recipients)
if (r.Status != RecipientStatus.Queued)
    Console.WriteLine("{0}: {1}", r.Email, r.Exception.Message);
```

Nel caso un Recipient debba essere usato più volte chiamare il metodo ResetStatus per riazzere il suo stato.

6.1.2 SmtMail

Questa classe è un wrapper di System.Web.Mail.SmtMail, e ha i seguenti 4 metodi statici.

static Recipient Send(MailMessage message, string recipient)

Questo è il metodo più semplice per inviare il messaggio a un solo destinatario. Si crea il messaggio e si chiama questo metodo indicando il destinatario come stringa. Il metodo restituisce l'oggetto Recipient corrispondente al destinatario specificato. Con esso si può controllare l'esito dell'invio:

```
MailMessage msg = new MailMessage();
// composizione 'msg'...
if (RER.Tools.Mail.SmtMail.Send(msg, "tizio@caio.it").Status != RecipientStatus.Queued)
    Console.WriteLine("Errore...");
```

Naturalmente in questo modo non si riesce ad ottenere la descrizione dell'errore. Per farlo occorre memorizzare il risultato del metodo in una variabile di tipo Recipient:

```
MailMessage msg = new MailMessage();
// composizione 'msg'...
Recipient r = RER.Tools.Mail.SmtMail.Send(msg, "tizio@caio.it");
if (r.Status != RecipientStatus.Queued)
    Console.WriteLine(r.Exception.Message);
```

Oppure si usa direttamente il metodo seguente

static bool Send(MailMessage message, Recipient recipient)

Questo è come il precedente ma si aspetta, nella specificazione del destinatario, un oggetto Recipient

anziché una stringa:

```
MailMessage msg = new MailMessage();
// composizione 'msg'...
Recipient r = new Recipient("tizio@caio.it");
RER.Tools.Mail.SmtpMail.Send(msg, r);
if (r.Status != RecipientStatus.Queued)
    Console.WriteLine(r.Exception.Message);
```

static bool Send(MailMessage message, ArrayList bccRecipients, int maxBccRecipientsPerMail)

static bool Send(MailMessage message, ArrayList bccRecipients)

Usare questo metodo quando il messaggio deve essere inviato a più indirizzi.

- *message*: Messaggio da inviare (non impostare i destinatari BCC, saranno ignorati, usare invece il parametro *bccRecipients*)
- *bccRecipients*: Passare un Arraylist di oggetti di tipo `RER.Tools.Mail.Recipient` o di tipo stringa. Il metodo ha, in ogni caso, come "side-effect" la trasformazione degli oggetti string presenti *bccRecipients* in oggetti di tipo `Recipient`. Ciò permette, al chiamante, di poter ottenere il risultato dell'invio (interrogando le proprietà '`Recipient.Status`' e '`Recipient.Exception`') anche avendo passato delle stringhe
- *maxBccRecipientsPerMail*: Numero massimo di indirizzi per email (deve essere maggiore di 0). Se non specificato si usa il valore configurato a livello di server (`RER.Tools.Configuration.MaxRecipientsPerMessage`).

ritorna 'true' se tutto è andato bene, altrimenti occorre scorrere l'Arraylist interrogando la proprietà 'Status' degli oggetti. Se `Status != RecipientStatus.Queued` allora ci sono stati dei problemi, per i dettagli interrogare la proprietà 'Exception'.

Se si deve effettuare un invio massivo di email è consigliato riciclare la connessione all'SmtpServer, a seguire un esempio :

```
public void InviaNotifiche(List<MailMessage> mailMessages)
{
    SmtpClient smtpClient = null;

    foreach (MailMessage _mailMessages in mailMessages)
    {
        if (smtpClient == null || count % RER.Tools.Configuration.MaxBccRecipientsPerMail == 0)
        {
            // ogni n-inviati resetto la connessione SMTP
            if (smtpClient != null)
                smtpClient.ServicePoint.CloseConnectionGroup(null);
            smtpClient = new SmtpClient(RER.Tools.Configuration.SmtpServer);
        }
        smtpClient.Send(_mailMessages);
    }
}
```

6.1.3 Metodi d'utilità

La classe `SmtpMail` contiene anche il metodo:

static bool Split(MailMessage message, ArrayList bccRecipients)

Questa funzione cerca di spezzare una linea di testo in "tranci" di non più di 1000 caratteri. Il punto in cui "tranciare" è identificato da uno spazio. Serve perché l'SMTP vuole che il corpo del messaggio sia composto da linee di non più di 1000 caratteri. Per sicurezza questa funzione cerca un punto di

possibile "tranciatura" dall'800 carattere a ritroso.

Nel caso non ne trovi nessuno genera una `ArgumentException`.

NB: Eventuali spazi precedenti o successivi al punto di "tranciamento" sono eliminati.

7 RER.Tools.DirectoryServices

E' un namespace contenente 5 classi di utilità per accedere ai dati sul Active Directory

7.1 AdsiHelper

static DirectoryEntry GetDirectoryEntry(string path)

Restituisce la directory entry corrispondente al path indicato. Utile in quanto non richiede le credenziali di autenticazione (che sono definite centralmente).

7.2 AdsiUserHelper

Questa classe permette di avere informazioni sugli utenti del dominio RERSDM (utenti regionali) ed EXTRARER (utenti non regionali ma abilitati).

Per instanziare un oggetto di tipo `AdsiUserHelper` è possibile utilizzare i 2 costruttori:

- **public AdsiUserHelper(string valore, AdsiUserHelper.TipoIdentificatore tipoIdentificatore)** dove `TipoIdentificatore` è un enum che comprende i valori `account` e `matricola`;
- **public AdsiUserHelper(string domainName, string accountName).**

Di seguito vengono elencate le proprietà disponibili:

- **public string DistinguishedName:** restituisce il nome che identifica univocamente l'entry nella directory
- **public string EmployeeID:** restituisce la matricola di un dipendente regionale. Restituisce null se il valore non è presente.
- **public string EmployeeType:** restituisce il tipo di dipendente regionale. Restituisce null se il valore non è presente.
- **public string EmployeeNumber:** restituisce un numero univoco del dipendente regionale (es. Codice Fiscale). Restituisce null se il valore non è presente.
- **public string RERTipoIncarico:** restituisce il codice del tipo di incarico presso la regione per dipendenti regionali. Restituisce null se il valore non è presente.
- **public string RERPosLav:** restituisce la posizione lavorativa del dipendente regionale. Restituisce null se il valore non è presente.
- **public string Name:** restituisce l'account dell'utente all'interno del dominio (es. Formica_F)
- **public string FirstName:** restituisce il nome dell'utente.
- **public string LastName:** restituisce il cognome dell'utente.
- **public string FullName:** restituisce il nome completo (nome + cognome).

- public string **Description**: restituisce la descrizione dell'utente (es. Consulente software).
- public string **ManagedBy**: restituisce l'account del responsabile. Restituisce null se il valore non è presente.
- public string **EmailLDAP**: restituisce l'email regionale dell'utente. Restituisce null se il valore non è presente.
- public string **PianoStanza**: restituisce il piano e la stanza dell'ufficio dell'utente. Restituisce null se il valore non è presente.
- public string **Indirizzo**: restituisce l'indirizzo dell'ufficio dell'utente. Restituisce null se il valore non è presente.
- public string **Citta**: restituisce la città dell'ufficio dell'utente. Restituisce null se il valore non è presente.
- public string **TelephoneNumberLDAP**: restituisce il numero di telefono dell'ufficio dell'utente. Restituisce null se il valore non è presente.
- public string **Fax**: restituisce il numero di fax dell'ufficio dell'utente. Restituisce null se il valore non è presente.
- public string **Cellulare**: restituisce il numero di cellulare dell'utente. Restituisce null se il valore non è presente.
- public string **WorkHomeNumber**: restituisce il numero del telefono del telelavoro. Restituisce null se il valore non è presente.
- public StringCollection **AltriTelefoni**: restituisce una collection di numeri di telefono dell'utente. Restituisce null se il valore non è presente.
- public string **HomeDirectory**: restituisce il path della virtual directory personale dell'utente all'interno del dominio regionale.
- public string **HomeDrive**: restituisce il nome assegnato alla virtual directory personale.
- public StringCollection **Groups**: restituisce una collection di gruppi di dominio ai quali l'utente appartiene per gli utenti RERSDM. Restituisce null se il valore non è presente.
- public SortedList **ManagedGroups**: restituisce una collection di gruppi di dominio dei quali l'utente è il responsabile. Restituisce null se il valore non è presente.
- public SortedList **ManagedUsers**: restituisce una collection di utenti dei quali l'utente è il responsabile. Restituisce null se il valore non è presente.
- public SortedList **Computer**: restituisce una collection di computer dei quali l'utente è proprietario. Restituisce null se il valore non è presente.
- public SortedList **OrganizationalUnit**: restituisce l'unità organizzativa di appartenenza. Restituisce null se il valore non è presente.
- public SortedList **GroupsEXTRARER**: restituisce l'elenco dei gruppi di appartenenza per gli utenti del dominio EXTRARER. Restituisce null se il valore non è presente.

- public string **PathLDAP**: restituisce il percorso completo.
- public string **UrlApplication**: restituisce l'url della pagina personale dell'utente. Restituisce null se il valore non è presente.
- public string **UrlApplication2**
- public string **InfoApplication**
- public string **Comment**
- public DateTime **AccountExpirationDate**
- public bool **PasswordDontExpires**
- public DateTime **PasswordLastChanged**
- public TimeSpan **PasswordAge**
- public string **BadLoginCount**
- public string **BadPwdCount**
- public int **UserFlags**
- public bool **IsDisabled**
- public bool **IsAccountExpired**
- public bool **IsAccountLocked**
- public bool **IsPasswordExpired**
- public bool **IsDisabledToModify**
- public DateTime **LastLogin**
- public DateTime **LastLogoff**
- public DateTime **LastFailedLogin**
- public string **LoginScript**

Seguono esempi:

```
Console.Write("Dominio utente? ");
string dominio = Console.ReadLine();
Console.Write("Nome utente? ");
string username = Console.ReadLine();
AdsiUserHelper user = new AdsiUserHelper(dominio, username);

Console.WriteLine("Nome: {0} ", user.FirstName);
Console.WriteLine("Cognome: {0} ", user.LastName);
Console.WriteLine("Nome completo: {0} ", user.FullName);
Console.WriteLine("Matricola: {0} ", user.EmployeeID);
Console.WriteLine("Email: {0} ", user.EmailLDAP);
Console.WriteLine("Password Age: {0} ", user.PasswordAge);
Console.WriteLine("Gruppi:");
```

```
foreach(DictionaryEntry nomeGruppo in user.ManagedGroups)
    Console.WriteLine("- " + nomeGruppo.Value);

Console.WriteLine("Users:");
foreach(DictionaryEntry nomeUser in user.ManagedUsers)
    Console.WriteLine("- " + nomeUser.Value);

Console.WriteLine("Computer:");
foreach(DictionaryEntry nomeComputer in user.Computer)
    Console.WriteLine("- " + nomeComputer.Value);

Console.WriteLine("OrganizationalUnit:");
foreach(DictionaryEntry nomeOrganizationalUnit in user.OrganizationalUnit)
    Console.WriteLine("- " + nomeOrganizationalUnit.Value);

Console.WriteLine("GroupsEXTRARER:");
foreach(DictionaryEntry nomeGroupsEXTRARER in user.GroupsEXTRARER)
    Console.WriteLine("- " + nomeGroupsEXTRARER.Value);
```

Quindi è possibile anche avere la scheda di un utente conoscendo solo la matricola (come dipendente regionale)

7.3 AdsiGroupHelper

Questa classe permette di avere informazioni sui gruppi del dominio RERSDM (regionali) ed EXTRARER(extra-regione).

Per instanziare un oggetto di tipo AdsiGroupHelper è possibile utilizzare i 3 costruttori:

- public **AdsiGroupHelper**()
- public **AdsiGroupHelper**(string group)
- public **AdsiGroupHelper**(string domainName, string group)

Di seguito vengono elencate le proprietà disponibili:

- public string **Description**: restituisce la descrizione del gruppo.
- public long **GroupType**: restituisce il tipo di gruppo.
- public string **ManagedBy**: restituisce l'utente referente (per RERSDM)-
- public string **ManagedByExtrarer**: restituisce l'utente referente (per EXTRARER).
- public string **WWWHomePage**: restituisce URL applicazione o UNC share associata.
- public string **Url**: restituisce URL applicazione o UNC share associata (alternativo).
- public SortedList **UsersOrdinati**: restituisce una lista di utenti ordinati per nome.

7.4 AdsiComputerHelper

Questa classe permette di avere informazioni sui computer del dominio RERSDM (regionali).

Per instanziare un oggetto di tipo AdsiComputerHelper è possibile utilizzare i 2 costruttori:

- public **AdsiComputerHelper**()
- public **AdsiComputerHelper**(string computer)

Di seguito vengono elencate le proprietà disponibili:

- public string **Inventario**
- public string **DNSHostName**
- public string **Description**
- public string **ManagedBy**
- public string **OperatingSystem**
- public string **OperatingSystemVersion**
- public string **OperatingSystemServicePack**

- public string **StreetAddress**
- public string **Citta**: (collocazione – solo Server)
- public string **Stanza**: (collocazione – solo Server)
- public string **TelephoneNumber**: Telefono più vicino (collocazione – solo Server)

7.5 AdsiOrganizationalUnitHelper

Questa classe permette di avere informazioni sulle unità funzionali del dominio RERSDM (regionali).

Per instanziare un oggetto di tipo AdsiOrganizationalUnitHelper è possibile utilizzare i 2 costruttori:

- public **AdsiOrganizationalUnitHelper**()
- public **AdsiOrganizationalUnitHelper** (string organizationalUnit)

Di seguito vengono elencate le proprietà disponibili:

- public string **Description**: restituisce la descrizione.
- public string **ManagedBy**: restituisce il referente.
- public string **CodiceHost**: restituisce il codice della struttura sull'host.
- public string **Indirizzo**
- public string **Citta**
- public string **CAP**
- public string **SiglaProvincia**
- public string **DisplayName**: restituisce il nome visualizzato.

8 Altro

In RER.Tools sono anche definite le seguenti classi i cui servizi possono risultare utili.

8.1 RER.Tools.Sql

Questa classe ha 2 metodi statici *CreateLikeClause* e *MakeSafe*:

CreateLikeClause

```
static string CreateLikeClause(  
string userInput,  
string dbFieldName,  
LikeClauseOptions mode,  
out int numberOfTerms  
)
```

oppure

```
static string CreateLikeClause(  
string userInput,  
string dbFieldName,  
LikeClauseOptions mode  
)
```

Questo metodo restituisce la condizione "where" che serve per cercare una o più parole in un campo testuale di una tabella (dbFieldName). In pratica si prende l'input dell'utente (userInput) e lo si scorre per trovare tutte le "parole" che lo compongono (eventualmente raggruppando in una parola sola quelle comprese tra doppi apici [""]) e per ognuna si crea una condizione "LIKE". Tutte queste condizioni "LIKE" vengono raggruppate insieme in "AND" o in "OR" a seconda del parametro "mode"

(AllTerms = AND, AnyTerm = OR).

userInput: l'input inserito dall'utente

dbFieldName: campo su cui fare la ricerca

mode: AllTerms=condizioni messe in AND, AnyTerm=condizioni messe in OR

numberOfTerms: restituisce quanti termini sono stati creati

valore restituito: la stringa contenente la condizione SQL che realizza la ricerca, accodarla allo statement che si sta preparando. E'una stringa sicura relativamente ai problemi di SQL Injection (si utilizza RER.Tools.Sql.MakeSafe, precedentemente citata e sotto descritta).

Esempio:

```
SqlCommand cmd = new SqlCommand();
cmd.CommandText = "SELECT ... FROM ... WHERE ...";
string temp =
    SQL.CreateLikeClause("prova parole chiave", "colonna", SQL.LikeClauseOptions.AnyTerm);
if (temp != string.Empty)
    cmd.CommandText += " AND " + temp;
```

In questo caso la condizione restituita sarebbe:

(colonna LIKE '%prova%' OR colonna LIKE '%parole%' OR colonna LIKE '%chiave%')

Se invece lo user input fosse stato [prova "parole chiave"] la condizione sarebbe stata:

(colonna LIKE '%prova%' OR colonna LIKE '%parole chiave%')

ovvero le parole racchiuse tra doppi apici sono considerate come una parola sola. Come al solito, per includere un doppio apice all'interno di un raggruppamento l'utente deve immetterlo raddoppiato. Per esempio: [prova "di un ""testo"" raggruppato"] crea la seguente condizione where:

(colonna LIKE '%prova%' OR colonna LIKE '%di un "testo" raggruppato%')

MakeSafe(string)

Crea una versione "Sql Injection Safe" di una stringa (raddoppia l'apice singolo) da usare tutte le volte che si crea dinamicamente uno statement SQL e, specificamente, quando si scrive qualcosa del genere:

```
string mysql = "" + RER.Tools.Sql.MakeSafe(myVar) + "";
```

8.2 RER.Tools.StringWriterWithEncoding

E' una semplice wrapper della classe StringWriter che permette di indicare l'encoding (che per lo StringWriter di sistema è sempre UTF16). Ciò risulta utile per produrre file XML tramite XmlTextWriter per poi fisicizzarli sul file system. Esempio:

```
private string CommandLineArguments2XML()
{
    string[] arguments = Environment.GetCommandLineArgs();

    StringWriterWithEncoding xml = new StringWriterWithEncoding(Encoding.UTF8);
    XmlTextWriter writer = new XmlTextWriter(xml);
    writer.Formatting = Formatting.Indented;
    writer.WriteStartDocument();
    writer.WriteStartElement("CommandLineArguments");
    for (int i = 1; i < arguments.Length; i++)
    {
```

```
        writer.WriteStartElement("Argument");
        writer.WriteAttributeString("position", i.ToString());
        writer.WriteCData(arguments[i]);
        writer.WriteEndElement();
    }
    writer.WriteEndElement();
    writer.WriteEndDocument();
    writer.Close();
    return xml.ToString();
}
```

8.3 RER.Tools.Security.ImpersonateUser

Questa classe serve per impersonare un utente di cui si conoscono le credenziali. È un wrapper per la chiamate di sistema LogonUserA di advapi32.dll. Contiene semplicemente i seguenti due metodi:

bool ImpersonateValidUser(string userName, string domain, string password)

Cambia il contesto di sicurezza del thread corrente con quello dell'utente associato alle credenziali passate come parametri. Restituisce true se le credenziali sono corrette e l'*impersonation* ha avuto luogo. Altrimenti restituisce false.

void UndoImpersonation()

Da chiamare dopo avere eseguito l'*impersonation* per ritornare al contesto di sicurezza precedente

Esempio

```
//using System.Security.Principal;
Security.ImpersonateUser impersonationUser = new Security.ImpersonateUser();
if (impersonationUser.ImpersonateValidUser("Pinco_P", "RERSDM", "blablabla"))
{
    Console.WriteLine("OK!");
    Console.WriteLine("Current user: {0}", WindowsIdentity.GetCurrent().Name);
    Console.WriteLine("Undoing impersonation...");
    impersonationUser.UndoImpersonation();
    Console.WriteLine("Current user: {0}", WindowsIdentity.GetCurrent().Name);
}
}
```

8.4 RER.Toos.UrlNormativa

E' una classe che ha il compito di creare gli URL per accedere ai testi dei varia normativa a partire da un numero, da un anno, e un tipo ente. L'uso è molto semplice e completamente "statico" (nel senso che non occorre istanziare nessuna classe): vi serve calcolare l'URL per vedere (per esempio) la legge regionale 45 del 2004? Il metodo che vi restituisce l'URL è:

```
miolink.NavigateUrl = RER.Tools.UrlNormativa.LeggeRegionale.CreaLink(2004, 45,
TipoEnte.Giunta)
```

Se anziché il testo di una legge regionale vi serve quello ad una delibera (diciamo la 232 del 2005 della Giunta):

```
miolink.NavigateUrl = RER.Tools.UrlNormativa.DeliberaGiuntaRegionale.CreaLink(2005, 232,
TipoEnte.Giunta)
```

La classe raggruppa una serie di "tipi di normativa", al momento:

LeggeRegionale

DeliberaConsiglioRegionale

DeliberaGiuntaRegionale

DeliberaGiuntaRegionaleDaIntranet (su internet le delibere se vedono solo dopo che sono pubblicate, su intranet appena approvate, per questo ci sono due link distinti)

DeterminazioneDelDirigente
DeterminazioneDelPresidente
DeterminazioneDellAssessore
BollettinoUfficialeRegionale

I Tipo.Ente ammessi sono

- Giunta,
- Agrea,
- IBACN,
- INTERCENTER,
- ProtezioneCivile

Se si desidera richiamare documenti della Giunta è possibile utilizzare il metodo di overload

```
miolink.NavigateUrl = RER.Tools.UrlNormativa.DeliberaGiuntaRegionale.CreaLink(2011, 232);
```

8.5 Creazione di documenti PDF lato server

La Regione Emilia-Romagna ha acquistato la licenza di 2 componenti per la creazione dei documenti PDF:

- IBEX PDF Creator (v. 4.5.0.3): per la generazione via XSL-FO
- XMLPDF (v. 4.9.0): per la generazione tramite dei template XML (più semplice di XSL-FO, ma meno potente)

Per i dettagli si rimanda al sito del produttore dei componenti <http://www.xmlpdf.com>

Tutte le volte che si crea un oggetto xmlpdf.PDFDocument, indicare il file della licenza nel seguente modo:

```
ibex4.FODocument foDocument = new FODocument();  
ibex4.licensing.Generator.LicenseFileLocation =  
    RER.Tools.Configuration.IbexPdfCreatorLicenseFileLocation;
```

Tutte le volte che si crea un oggetto xmlpdf.PDFDocument, indicare il file della licenza nel seguente modo:

```
xmlpdf.PDFDocument doc = new xmlpdf.PDFDocument();  
xmlpdf.licensing.Generator.LicenseFileLocation =  
    RER.Tools.Configuration.XmlPdfLicenseFileLocation;
```

8.6 Generazione di reportistica lato server

La Regione Emilia-Romagna ha adottato come strumento di reportistica della filiera Microsoft Reporting services.

9 Installazione e configurazione di RER.Tools

Assieme a questo documento è possibile richiedere i seguenti file:

- RER.Tools.dll
- RER.Tools.ApplicationLogger.dll
- RER.Tools.config
- ApplicationLoggerDBSetup.sql

Gli assembly che compongono il namespace RER.Tools.* sono 2:

- RER.Tools.dll

- RER.Tools.ApplicationLogger.dll

Sono assembly con *strongname*, quindi è possibile (nonché consigliabile) installarli nella GAC (Global Assembly Cache).

A questi assembly sono associate alcune sezioni di configurazione. Esattamente come è consigliabile installare gli assembly nella GAC è analogamente consigliabile aggiungere tali sezioni direttamente nel *machine.config*.

L'intera sezione di configurazione è contenuta nel file RER.Tools.config. Naturalmente se si decide di aggiungere tali configurazioni nel *machine.config* occorre distribuirle coerentemente con quanto già definito nel proprio *machine.config* (ciò vale fondamentalmente per la sezione `<sectionGroup name="RER">` che andrà aggiunta alla esistente elemento `<configSections>` del *machine.config*).

Tali sezioni di configurazione richiedono l'immissione di alcune informazioni personalizzate. Ci sono commenti autoesplicativi, comunque i punti in cui intervenire sono indicati dalla presenza della stringa **!TODO!** e in particolare occorre:

- indicare il nome del server SMTP
- indicare la stringa di connessione per il DB dell'ApplicationLogger (vedere paragrafo 9.1 più sotto)
- indicare la/le *email* a cui inviare le notifiche dell'ApplicationLogger

La sezione di configurazione più importante di tutte è `<SqlServerInstanceMappings>`. Essa serve al SqlConnectionBroker per decidere a quale istanza di Sql Server richiedere una connessione. Di default è presente un solo *mapping*:

```
<Mapping defaultDataSource="(local)" />
```

che suppone che il DB server sia sulla stessa macchina in cui risiede l'applicazione. Sostituire a "(local)" il nome della propria istanza di SqlServer se, in locale, non sia installato il DB server. L'utilizzo di più elementi `<Mapping>` permette la semplificazione del deployment delle applicazioni nel caso si abbia una infrastruttura hardware più articolata (DB server di sviluppo e produzione, Web Farms, ...). In tal caso fare riferimento ai commenti presenti nel file RER.Tools.config oppure ai tecnici regionali.

9.1 DB per l'ApplicationLogger

Il componente RER.Tools.ApplicationLogger *logga* gli eventi da esso gestiti in un DB, tra i file allegati è presente anche ApplicationLoggerDBSetup.sql che contiene lo script SQL necessario alla creazione del DB.

Identificare il DB Server in qui si vuole installare questo DB, in esso creare:

- Un nuovo database vuoto di nome "ApplicationLogger"
- Un nuovo login di nome "usrApplicationLogger"
- Lanciare lo script ApplicationLoggerDBSetup.sql
- Modificare di conseguenza la stringa di connessione nella sezione di configurazione RER\GlobalSettings\ApplicationLoggerConnStr.

Allegato 4: Strumenti di supporto e linee guida per sviluppo applicazioni Java EE

1	Introduzione	1
2	Dettaglio specifiche Java EE6 / Java EE5.....	1
2.1	2
3	Scelta del JDK	4
4	Best practices	4
5	Ambienti di sviluppo.....	5
6	Utilizzo di stored procedure	5
7	Configurazione JBoss EAP 6 in RER	6
7.1	Introduzione.....	6
7.2	Configurazione in RER.....	7
7.3	Classloading e moduli	7
7.4	Percorsi e filesystem	8
7.5	Differenze fra Standalone e Domain	8
7.6	Profili.....	8
8	Nexus.....	9
8.1	Struttura	9
8.2	Sicurezza.....	9
8.2.1	Privilegi	9
8.2.2	Ruoli.....	9
8.2.3	Utenti	10
9	Dati tecnici richiesti per il deploy delle applicazioni.....	10
9.1	Indicazioni da seguire.....	10
9.2	Scheda tecnica da compilare e allegare al ticket per il deploy	11
9.3	Caratteristiche del Deploy Automatizzato.....	12

1 Introduzione

Scopo di questo documento è quello di fornire alcune regole e suggerimenti di base da seguire per minimizzare l'entità delle attività di migrazione di applicazioni JEE nel caso di porting da un Application Server ad un altro e chiarire alcuni aspetti fondanti dello standard jee.

Questo documento prende in considerazione, per necessità di sintesi, due Application Server: Jboss v5 EAP e JBoss EAP 6.

2 Dettaglio specifiche Java EE6 / Java EE5

Si prendono qui in considerazione le seguenti versioni degli Application Server:

- JBoss Application Server v5.x.x EAP

JBoss EAP 6/JBoss Application Server v5.x.x EAP è certificato Java EE 5, mentre JBoss EAP 6 è certificato Java EE 6.

Da un punto di vista tecnologico il passaggio da J2ee1.4 a Jee5 ha rappresentato un “salto generazionale” circa le modalità di sviluppo Java Enterprise, dal momento che il processo di sviluppo è stato enormemente semplificato dall'uso massivo delle “annotazioni”.

Riportiamo di seguito le specifiche JEE 5 e JEE 6. Osserviamo che in JEE 6 si sono introdotti i cosiddetti profili, intesi come particolari configurazioni delle specifiche indicate per particolari classi di applicazioni.

Specifiche Java EE 5

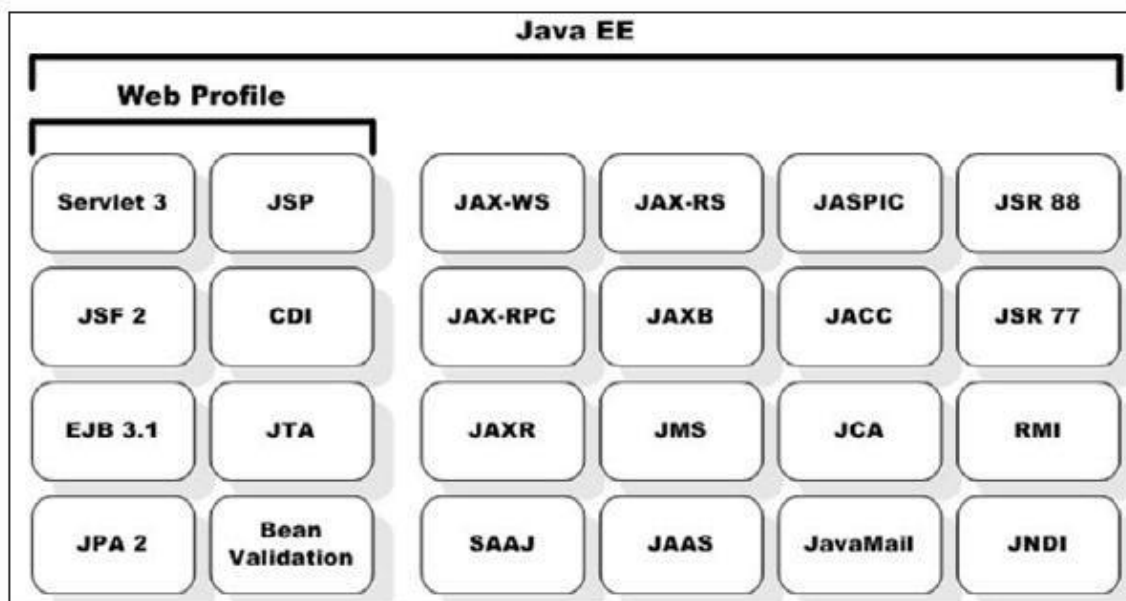
Tecnologia	Versione	JSR
Web Services Technologies:		
Web Services	1.2	JSR109
Java API for XML-Based Web Services (JAX-WS)	2.0	JSR224
Java Architecture for XML Binding (JAXB)	2.0	JSR222
Web Service Metadata for the Java Platform	2.0	JSR181
Java API for XML-Based RPC (JAX-RPC)	1.1	JSR101
Java API for XML Registries (JAXR)	1.0	JSR93
SOAP with Attachments API for Java (SAAJ)	1.3	JSR67
Streaming API for XML (StAX)	1.0	JSR173
Web Application Technologies:		
Java Servlet	2.5	JSR154
JavaServer Faces (JSF)	1.2	JSR252
JavaServer Pages (JSP)	2.1	JSR245
JavaServer Pages Standard Tag Library (JSTL)	1.2	JSR52
Debugging Support for Other Languages	1.0	JSR45
Enterprise Application Technologies:		
Enterprise JavaBeans (EJB)	3.0	JSR220
Java Persistence API (JPA)	1.0	JSR220
Java EE Connector Architecture	1.5	JSR112
Common Annotations for the Java Platform	1.0	JSR250
Java Message Service API (JMS)	1.1	JSR914
Java Transaction API (JTA)	1.1	JSR907
JavaMail API	1.4	JSR919
JavaBeans Activation Framework (JAF)	1.1	JSR925
Management and Security Technologies:		
Java Authorization Service Provider Contract for Containers (JACC)	1.1	JSR115
J2EE Application Deployment	1.2	JSR88
J2EE Management	1.1	JSR77

2.1

Specifiche Java EE 6

Tecnologia	Versione	JSR	Inclusa nel profilo web
Web Services Technologies:			
Java API for RESTful Web Services (JAX-RS)	1.1	JSR311	
Web Services	1.3	JSR109	
Java API for XML-Based Web Services (JAX-WS)	2.2	JSR224	
Java Architecture for XML Binding (JAXB)	2.2	JSR222	
Web Services Metadata for the Java Platform	2.1	JSR181	
Java API for XML-based RPC (JAX-RPC)	1.1	JSR101	
Java APIs for XML Messaging (JAXM)	1.3	JSR67	
Java API for XML Registries (JAXR)	1.0	JSR93	
Web Application Technologies:			
Java Servlet	3.0	JSR315	SI
JavaServer Faces (JSF)	2.0	JSR314	SI
JavaServer Pages (JSP)	2.2	JSR245	SI
Expression Language (EL)	2.2	JSR245	SI
JavaServer Pages Standard Tag Library (JSTL)	1.2	JSR52	SI
Debugging Support for Other Languages	1.0	JSR45	SI
Enterprise Application Technologies:			
Enterprise JavaBeans (EJB)	3.1	JSR318	SI versione Lite
Java Persistence API (JPA)	2.0	JSR317	SI
Contexts and Dependency Injection for Java	1.0	JSR299	SI
Dependency Injection for Java	1.0	JSR330	SI
Bean Validation	1.0	JSR303	SI
Managed Beans	1.0	JSR316	SI
Interceptors	1.1	JSR318	SI
Java EE Connector Architecture	1.6	JSR322	
Common Annotations for the Java Platform	1.1	JSR250	SI
Java Message Service API (JMS)	1.1	JSR914	
Java Transaction API (JTA)	1.1	JSR907	SI
JavaMail API	1.4	JSR919	
Management and Security Technologies:			
Java Authentication Service Provider Interface for Containers (JASPIC)	1.0	JSR196	
Java Authorization Service Provider Contract for Containers (JACC)	1.4	JSR115	
Java EE Application Deployment	1.2	JSR88	
J2EE Management	1.1	JSR77	

Riassumendo graficamente le tecnologie incluse nel profilo web:



3 Scelta del JDK

In generale è sempre preferibile utilizzare, dove possibile, la versione più aggiornata del JDK per evitare possibili ricadute in fase di porting verso versioni più aggiornate dell'Application Server che abbiano come prerequisito l'utilizzo di un JDK più aggiornato.

Per quanto riguarda JEE 5 si richiede almeno JDK 1.6, anche se è fortemente consigliato per JBoss 5 usare JDK 1.7

Le specifiche JEE 6 indicano sia il JDK 1.6 che il JDK 1.7 come ambiente di riferimento. Anche in questo caso è preferibile usare la versione più aggiornata del JDK.

4 Best practices

Per minimizzare gli sforzi da effettuare quando si vuole migrare un'applicazione da un Application Server ad un altro è buona norma seguire le seguenti regole:

Evitare di utilizzare librerie proprietarie dell'Application Server (ad es. per effettuare chiamate allo scopo di reperire la connessione nativa dal data source) e quindi limitare i riferimenti a classi ed interfacce delle API JEE escludendo dipendenze da classi implementative dello specifico container.

Adottare le API specificate nelle tabelle relative alle tecnologie JEE 5 o JEE 6 in maniera consistente rispetto alla versione JEE supportata dall'Application Server. E' evidente che la violazione di questo accorgimento, con utilizzo combinato di versioni non afferenti alla stessa specifica JEE, può creare difficoltà nel porting poiché può dar luogo a comportamenti dissimili tra differenti Application Server.

Possono verificarsi problemi legati alla diversa gestione dei class loaders in differenti Application Server. Sia JBoss che Websphere forniscono la possibilità di configurazione di differenti politiche di

classloading; pertanto il porting può comportare interventi sulla configurazione del classloading dell'applicazione.

Possono anche verificarsi problemi legate alle diverse librerie installate nei server a livello di runtime (ad esempio in entrambi i server sono presenti le librerie di Xerces, ma con versioni leggermente diverse). Anche questo tipo di problemi sono solubili intervenendo sulla configurazione della politica di classloading.

In ogni caso, anche seguendo le suddette regole, il porting non è immediato in quanto alcune risorse sono comunque non portabili: una parte dei deployment descriptor delle applicazioni non rientrano nello standard (es:jboss-web.xml) ed hanno formati specifici dei singoli Application Server e quindi non sono portabili e richiedono un adattamento od una riscrittura.

5 Ambienti di sviluppo

Negli ambienti Eclipse, sono presenti dei validatori che permettono di effettuare una serie di controlli già in fase di sviluppo. Ecco un esempio dei validatori presenti in Eclipse 3.3:

Application Client Validator
Classpath Dependency Validator
Connector Validator
DTD Validator
EAR Validator
EJB Validator
HTML Syntax Validator
JPA Validator
JSF Application Configuration Validator
JSP Content Validator
JSP Semantics Validator (JSF)
JSP Syntax Validator
ModuleCore Validator
War Validator
WSDL Validator
WS-I Message Validator
XML Schema Validator
XML Validator

Si consiglia di attivare questi validatori in modo da effettuare automaticamente i relativi controlli.

6 Utilizzo di stored procedure

Si ritiene opportuno in questo contesto dare anche alcune indicazioni sull'utilizzo delle stored procedure nello sviluppo delle applicazioni.

Vi sono ragioni a supporto dell'utilizzo delle stored procedure:

- ✓ Elaborazioni massive: quando i dati da elaborare sono molti l'uso delle stored può rivelarsi conveniente dal punto di vista della velocità di elaborazione, in quanto viene minimizzato l'overhead di rete necessario per la trasmissione dei dati dal database al nodo in cui i dati vengono elaborati.

Ci sono anche ragioni per non utilizzarle:

- ✓ Non portabilità del codice su diversi database: il codice delle stored di solito non è portabile tra diversi database, costringendo alla riscrittura delle stesse nel momento in cui si voglia migrare il database.
- ✓ Minore scalabilità dell'applicazione: se il database è l'elemento in cui vengono effettuate tutte le elaborazioni, diventa complesso distribuire il carico con impatto sulla scalabilità. Va anche tenuto presente che normalmente un database server serve più Application Server.

Il suggerimento è quello di bilanciare le diverse esigenze e adottare le stored solo quando motivi di efficienza dal punto di vista delle prestazioni lo richiedano, in quanto devono essere manipolate quantità ingenti di dati (decine di migliaia di righe ed oltre), evitando possibilmente di implementare completamente la logica applicativa dentro alle stored, lasciando all'applicazione Java solo la responsabilità di gestire il front-end.

7 Configurazione JBoss EAP 6 in RER

7.1 Introduzione

Di seguito si descrivono le particolarità dei server di produzione JBoss EAP 6 e contestualmente si suggeriscono strumenti di supporto che possono essere utili per un più veloce e facile sviluppo.

JBoss EAP 6 permette due modalità di installazione: Standalone e Domain.

Come specificato dalla guida ufficiale [docs.jboss.org] lo Standalone è un processo indipendente, esattamente come funzionavano le versioni precedenti di JBoss.

La modalità domain è una nuova feature di JBoss EAP 6 che permette di gestire diverse installazioni, suddivise su più server, da un unico punto centrale.

Gli elementi principali di questa infrastruttura sono gli Host controller, il Domain controller, i Server group ed i Server.

Host Controller: processo che si occupa di avviare i singoli server ed interagire con il Domain controller.

Domain Controller: un Host controller definito come punto centrale della configurazione per tutto il dominio. Questo processo si occupa di gestire le policy e di farle applicare a tutti gli host controller a lui associati.

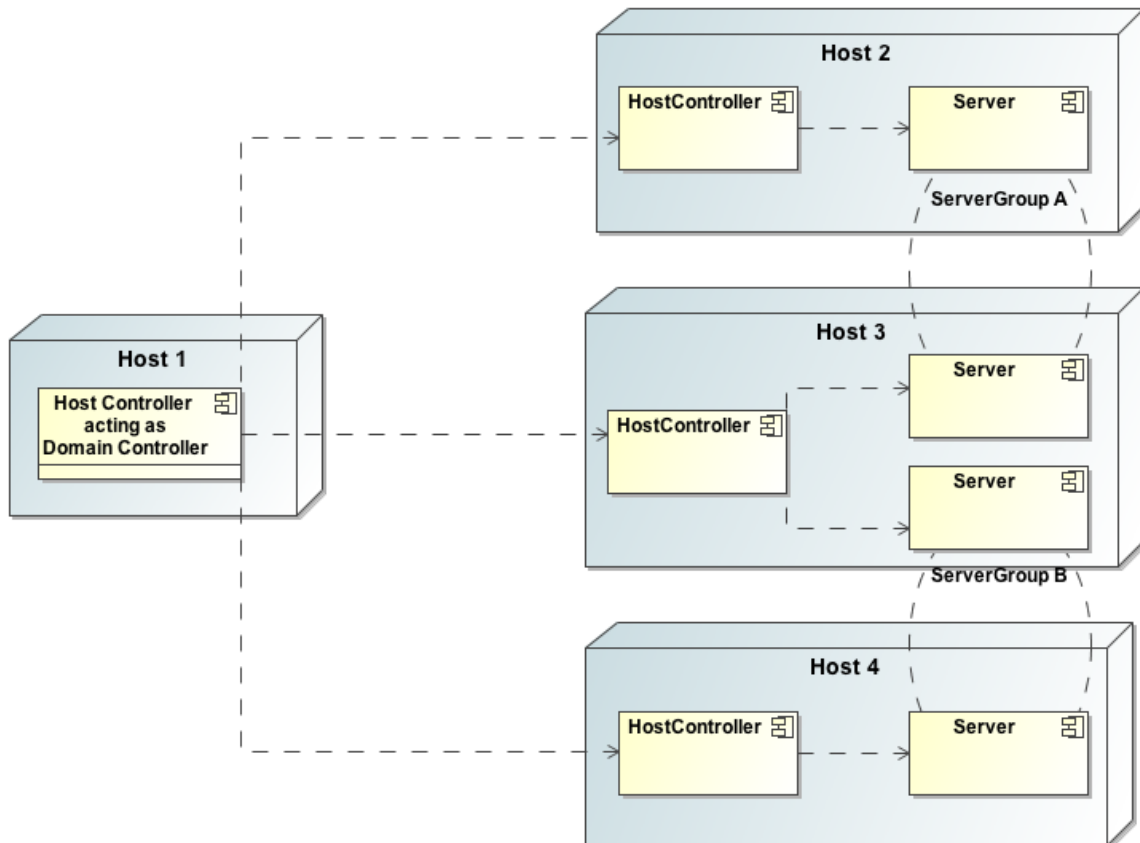
Profile: un profilo è la parte di configurazione specifica che viene poi applicata al server group. Qui sono specificate tutte le informazioni come datasource, messaging, connettori come nella versione standalone.

Server Group: raggruppamento logico di server. Un server group contiene informazioni che vengono condivise dalle istanze che ne fanno parte. Le applicazioni ed i deploy sono definiti in questo livello e vengono replicati in tutte le istanze.

Server: application server sul quale sono deployate le applicazioni. è un processo JVM separato dall'host controller.

7.2 Configurazione in RER

La modalità scelta per l'installazione e la configurazione degli ambienti in Regione è la modalità Domain. Questo per semplificare la gestione delle installazioni e velocizzare le operazioni di deploy e di manutenzione ordinaria.



Questa modalità permette di centralizzare le configurazioni in un unico punto senza doverle replicare su ogni singolo application server.

7.3 Classloading e moduli

Ci sono differenze fondamentali dalle vecchie installazioni di JBoss.

Il classloader dove sono state inserite le priorità per il caricamento delle classi. Nel link è possibile leggere la documentazione estratta dalla guida dello sviluppatore.

È prevista la possibilità di aggiungere moduli oltre a quelli standard presenti nell'installazione JBoss, purché questi non contrastino o si sovrappongano a moduli esistenti. Ad esempio, nelle installazioni di base effettuate in RER sono presenti due moduli aggiuntivi che sono oracle ed oracle6, rispettivamente corrispondenti al driver JDBC per oracle ojdbc14 ed al driver JDBC ojdbc6. Questi moduli sono condivisi fra tutte le istanze JBoss installate sul server. Le librerie specifiche per

l'applicativo devono essere caricate all'interno del pacchetto applicativo stesso come specificato nel link al paragrafo precedente.

7.4 Percorsi e filesystem

Il VFS (virtual file system) è utilizzato per migliorare l'accesso alle risorse presenti sul filesystem. Nelle vecchie versioni di JBoss era possibile accedere al filesystem richiamando direttamente la risorsa attraverso il path, utilizzando il VFS sarà possibile accedere ai file utilizzando le API di JBoss.

Per rendere portabili su installazioni differenti gli applicativi è necessario utilizzare le variabili messe a disposizione da JBoss (vedere docs.jboss.org) ed evitare ove possibile l'utilizzo di path assoluti. L'utilizzo delle variabili facilita la pratica di mantenere tutti i file e cartelle esterni al pacchetto applicativo all'interno del path dedicato a JBoss. È quindi da evitare, a meno di esigenze esplicite, di utilizzare path non standard ed esterni all'installazione JBoss. Da considerare inoltre che il filesystem di riferimento è ext4.

7.5 Differenze fra Standalone e Domain

Da documentazione di JBoss non vi sono differenze fra la versione standalone e la versione domain. A parità di configurazione, ogni applicativo funzionante sulla versione standalone può essere portato nella versione domain.

7.6 Profili

Il profilo è una differenziazione su come è impostata la configurazione fra domain e standalone. Ogni profilo contiene al suo interno le informazioni necessarie per la creazione dell'istanza JBoss, come datasource, connettori, code e messaging. I profili di base di JBoss sono 4: default, full, ha e full-ha.

In base alle funzionalità di Jboss usate dall'applicazione (code JMS, clustering ecc.) sarà scelto il profilo con il minor numero di features per ridurre l'impronta dell'application server e i possibili problemi derivanti da componenti attivati e non utilizzati.

Le funzionalità avanzate di Jboss utilizzate dall'applicazione andranno indicate nella scheda per la richiesta di deploy nuova applicazione.

In RER ad ogni istanza, o cluster di istanze, viene assegnato un proprio profilo personalizzato creato da una copia di uno dei quattro di default nel quale sono configurati i datasource relativi alle applicazioni deployate, le eventuali code jms, il cluster di messaging se presente (via hornetq) ed i connettori http e/o https.

Per una gestione centralizzata degli artefatti creati dagli sviluppatori si è deciso di utilizzare Nexus.

8 Nexus

Nexus è un repository manager, organizza e facilita la condivisione di librerie e componenti software tra sviluppatori dello stesso team o fra diversi team di sviluppo.

8.1 Struttura

La gestione dei repository è stata pensata nel seguente modo:

Gli accessi in lettura possono essere sia anonimi che protetti da autenticazione, mentre l'accesso in scrittura ai repository richiede sempre l'autenticazione via username e password. L'accesso anonimo alla lettura è la modalità standard, la protezione in questo caso viene utilizzata se i dati presenti nel repository sono sensibili (es. un jar contenente le credenziali di accesso ad un database).

Ci sono due tipi differenti di sicurezza dei repository, uno ad accesso anonimo e uno ad accesso protetto.

I repository dello stesso gruppo di sviluppo vengono uniti in un gruppo "logico" su nexus, ad esempio:

siir-snapshot e **siir-release** sono uniti nel gruppo **siir** ed accessibili da un unico url

I repository utilizzati sono di tipo proxy o hosted. I **proxy** sono configurati come ponte verso repository esterni e fanno da caching. Gli **hosted** sono locali e contengono i componenti software (librerie, pacchetti, ecc.) creati dai gruppi di sviluppo.

La differenziazione tra **release** e **snapshot** è quella generica degli artefatti maven. *Riassumendo:* gli snapshot sono versioni in evoluzione ancora in fase di sviluppo, mentre le release sono versioni stabili che non subiranno mutazioni in futuro.

8.2 Sicurezza

8.2.1 Privilegi

I repository hanno cinque tipi di **privilegi**, due di lettura (view e read) e tre di scrittura (create, update, delete).

View: permette di visualizzare il repository o di fare list di quelli presenti

Read: permette di leggere il contenuto di un repository

Create: permette di creare gli oggetti all'interno del repository

Update: permette di aggiornare gli oggetti già presenti nel repository

Delete: permette di eliminare oggetti dal repository

Alla creazione di un nuovo repository viene in automatico generato solo il permesso di view. Gli altri vanno aggiunti manualmente.

8.2.2 Ruoli

I **privilegi** vengono raccolti in ruoli i quali verranno associati agli **utenti**.

Nell'installazione regionale abbiamo definito un ruolo per l'accesso anonimo: *anonymous-repository-viewer*. A questo ruolo vengono associati tutti i privilegi view e read dei repository ad accesso anonimo.

Un altro ruolo creato è il *basic-repo-admin* che fornisce i privilegi di base per la gestione di un repository, a questo non è associato nessun repository in particolare, i privilegi legati ad esso diventano effettivi solamente se l'utente ha anche i permessi di scrittura sul repository.

Per dare la possibilità di scrittura sul repository bisogna generare un ruolo, di default chiamato *<nome_repository>-admin*, al quale vengono associati i privilegi di scrittura sul repository.

Per poter leggere dal repository bisogna generare un ruolo, di default chiamato *<nome_repository>-read*, al quale vengono associati i privilegi di lettura dal repository.

Il ruolo *Nexus Administration Role* è il ruolo di amministrazione dell'istanza di Nexus, viene utilizzato per la gestione e la creazione dei repository e degli utenti con annessi i privilegi è un super-user.

8.2.3 Utenti

Gli **utenti** sono gestiti tramite LDAP. Gli account che vengono abilitati utilizzeranno le credenziali regionali per poter accedere ai repository.

Il nome utente è case sensitive quindi deve avere la prima lettera del cognome e la prima del nome in maiuscolo (es. Rossi_M)

9 Dati tecnici richiesti per il deploy delle applicazioni

9.1 Indicazioni da seguire

Per una migliore collaborazione e per una gestione più rapida delle applicazioni sono state stabilite alcune linee guida da seguire:

Il nome del pacchetto dovrà sempre essere uguale al nome dell'applicazione. L'applicazione che risponde al nome "esempio" avrà nome del pacchetto "esempio.war".

I log saranno gestiti attraverso il sistema di logging del container, vanno quindi fornite le classi o handler per il log con il livello da associargli. L'applicazione dovrà scrivere in un file di log dedicato, non nel server log né sulla console del container.

Il "JNDI name" sarà formato da java:jboss/datasources/NomeApplicazione o NomeDatabase se usato da più applicazioni.

L'HEAP delle applicazioni è settato di default a 512Mb, se si necessita di ampliarlo è necessario specificarlo e motivare la necessità.

Il PermSize è settato di default a 256m, se si necessita di ampliarlo è necessario specificarlo e motivare la necessità

9.2 Scheda tecnica da compilare e allegare al ticket per il deploy

Informazioni generali sull'applicazione (compilazione a carico del servizio committente)	
Servizio Committente	
Interfaccia Web / Webservice	
Tipologia e numero di utenze	
Nome del DB	
Documentazione/specifiche utili per la predisposizione dell'ambiente (compreso Allegato 14)	
Eseguita richiesta di verifica preliminare alla presa in carico	Si / No
Espressione visto di riscontro di congruenza tecnica	Si / No

Dati specifici dell'applicazione (compilazione a carico del servizio committente)	
Esposizione dell'applicazione su nuovo URL o su URL esistente	Indicare l'url desiderato, se già esistente, o se ne va creato uno nuovo.
Contesto dell'applicazione	
Numero di istanze di application server richieste	(una o più istanze bilanciate)
Applicazione distribuita	(Specificare se l'applicazione è distribuita o meno)
Utilizzo di code JMS	(Specificare se l'applicazione necessita di code JMS)
Utilizzo della Cache	(Specificare se l'applicazione utilizza il caching di Jboss)
Livello di logging	(TRACE, INFO, DEBUG, ecc)
Categorie di logging	(it.regione, it.emr, ecc)
http e/o https	
Versione di Application Server (Jboss) e JDK	(Se non specificato sarà usata l'ultima release disponibile di Jboss EAP 6)
Necessità dell'esposizione dei log	(l'esposizione è via web)
Necessità di interazione con altre applicazioni	Lista applicazioni e modalità di interazione
Necessità di un HEAP maggiore	(Default 512Mb)
Necessità di un PERMSIZE maggiore	(max=256m)
Necessità di ulteriore spazio disco locale	(Specificare uno spazio stimato)
Necessità di una share esterna	(Specificare uno spazio stimato)

Necessità di uno o più file di configurazioni esterni al pacchetto applicativo

Tempistiche e vincoli del Servizio committente (compilazione a carico del servizio committente)	
Consegna in <u>test</u> per verifiche utenti entro il :	gg/mm/aaaa
Consegna in <u>produzione</u> entro il :	gg/mm/aaaa
Tipologia di vincoli normativi	
Tipi di criticità	
Note	

9.3 Caratteristiche del Deploy Automatizzato

I gruppi di sviluppo che ritengono utile automatizzare la procedura di deploy, possono utilizzare, per il solo ambiente di test, il deploy automatizzato messo a disposizione dal SIIR. Questa procedura è attiva esclusivamente per le applicazioni installate su Jboss EAP 5 e Jboss EAP 6.

L'automazione dei deploy nell'ambiente della regione emilia romagna e' stata implementata con l'aiusilio di:

- uno script python che si occupa dell'autenticazione e dell'automazione del deploy e del riavvio delle istanze jboss
- share samba dove posizionare il pacchetto da deployare
- lo schema cmdbuild dal quale reperire le informazioni su applicativi ed istanze.
- un database di appoggio dove immettere le abilitazioni di deploy degli applicativi

Basato su python 2.7, lo script di autodeploy si occupa di leggere i file scritti in determinate directory ed effettuare il deploy od il riavvio delle istanze.

Come funziona?

L'utente che deve effettuare il deploy copia il pacchetto sulla share samba dedicata. Lo script si accorge del nuovo file, legge il path dei deploy per determinare se e' un pacchetto di test o produzione, legge l'utente che ha scritto il file e determina, in base ai dati su db, se questo e' abilitato ad effettuare il deploy. Effettua il deploy via scp per jboss 5, via commandline di jboss per versioni superiori. Se il deploy e' andato a buon fine il pacchetto viene inserito nella cartella old/YYYYMMDD (AnnoMeseGiorno).

Lo status dell'operazione viene descritto con la creazione di files sulla stessa directory del war da deployare. il nome del file e' nomepacchetto.STATUS. STATUS puo' essere uno dei seguenti: deploying, deployed, error (in caso di errore generico), usernotenabled se l'utente non e' abilitato, .timeout in caso di timeout dell'operazione di deploy. Questi file sono eliminabili dall'utente

stesso in quanto servono esclusivamente per comunicare lo stato dell'operazione a chi effettua il deploy

È sufficiente richiedere l'abilitazione degli utenti per le applicazioni di propria competenza e copiare l'applicazione nella share samba designata. L'applicazione verrà aggiornata automaticamente. Questa procedura permette inoltre il riavvio delle istanze.

Per quanto riguarda la gestione degli utenti da abilitare ai vari war di deploy e' presente lo script `user_mgmt.py`.

Questo permette la visualizzazione, cancellazione ed aggiunta sia di applicativi che di utenti abilitati agli stessi sul database relativo.

E' previsto l'import massivo tramite file csv. Il file deve avere la seguente struttura:

<code>nome_war,ambiente[test/prod],account</code>

Fare attenzione che ogni informazione è CASE SENSITIVE.

Allegato 4a: procedure di aggiornamento dei servizi applicativi

1	Introduzione	1
2	procedure di aggiornamento applicazioni SAP	4
3	procedure di aggiornamento applicazioni BO	5
4	procedure di aggiornamento base dati	5
4.1	Workflow di rilascio	6
5	procedure di aggiornamento applicazioni filiera C	6
5.1	Workflow di rilascio	7
6	procedure di aggiornamento applicazioni filiera A	7
6.1	Workflow di rilascio: container Tomcat	7
6.2	Workflow di rilascio: container Jboss AS 7, Jboss 5 e Jboss 4 - TEST	8
6.3	Workflow di rilascio: container Jboss EAP 6 - TEST	9
6.4	Workflow di rilascio: container Jboss EAP 6, Jboss AS 7, Jboss 5 e Jboss 4 - Produzione	9
7	procedure di aggiornamento applicazioni filiera B	10
7.1	Workflow di rilascio: delega ad Area applicativa SIIR	10
7.2	Workflow di rilascio: gestito da Area Sistemi SIIR	11
8	procedure di aggiornamento applicazioni GIS	12
8.1	Workflow di rilascio: delega ad Area applicativa	12
8.2	Workflow di rilascio: Servizi GIS – Servizi Mappa ed Immagine	13
8.3	Workflow di rilascio: Customizzazione Back-end GIS – Tool Geoprocessing	13

1 Introduzione

Scopo di questo documento è in particolare quello di descrivere le attività di aggiornamento delle applicazioni Custom realizzate nell'ambito delle filiere tecnologiche descritte negli allegati 1 ed 1a. Tali attività rientrano nei processi SIIR-SYS-App-02 e SIIR-SYS-App-03 descritti nel paragrafo 12 delle Linee Guida.

Il processo SIIR-SYS-App-01, relativo alla presa in carico ed avvio di un nuovo servizio, si configura come un'attività progettuale che non è obiettivo del presente documento.

Le condizioni per l'attivazione del processo SIIR-SYS-App-02 prevedono che l'area applicativa abbia:

- definito in dettaglio e documentato le nuove configurazioni nel caso in cui si tratta di attivare nuove configurazioni del sistema
- conclusa la realizzazione della nuova release della componente SW del servizio applicativo e quindi pronta per essere rilasciata in ambiente di test, collaudo (se previsto) e produzione

Le condizioni per l'attivazione del processo SIIR-SYS-App-03 prevedono che l'area applicativa abbia definito il servizio applicativo non più in linea con il business dell'Amministrazione e pronto per la dismissione.

Nei paragrafi 2 e 3 si farà una breve digressione sulle modalità di aggiornamento dei servizi applicativi SAP e BO che costituiscono una particolarità rispetto alle filiere Custom poiché il rilascio viene gestito in piena autonomia dalle aree applicative.

Lo strumento informatico per la gestione delle richieste è RT (<https://rt.regione.emilia-romagna.it/rt/>) che con le configurazioni implementate prevede un Workflow specialistico dedicato alla collaborazione diretta tra i gruppi specialistici di secondo livello (comprese le aree applicative del SIIR e delle strutture regionali con competenze informatiche verticali) senza transitare dal Service Desk.

Su tale sistema è stato definito ed implementato un meccanismo di classificazione delle richieste basato su 3 Livelli: **servizio di Business** (es. *Hosting*), **macrofunzione** (es. *Middleware/Piattaforme applicative – Manutenzione/Aggiornamento*), **richiesta di servizio/incidente** (es. *Aggiornamento applicazione (deploy)*).

Per ogni singola area applicativa (compresi i fornitori) è stato definito un gruppo su RT e sono state date le abilitazioni all'utilizzo dei Workflow, in particolare per quanto riguarda l'aggiornamento dei servizi applicativi, a quello denominato "Change Area Sistemi".

La medesima aggregazione in gruppi RT è stata fatta per le aree tecniche del SIIR (Area Infrastruttura) che, tra le altre attività di natura sistemistica, forniscono supporto alla implementazione e gestione dei servizi applicativi sui sistemi di propria competenza. Ovviamente anche tali gruppi sono stati definiti su RT ed abilitati al medesimo Workflow.

Pertanto l'area applicativa si configura come un "cliente" e l'area sistemi del SIIR come il primo assegnatario della richiesta ed immediatamente dopo come coordinatore degli interventi indirizzando alle varie aree tecniche del SIIR le singole attività per competenza.

Di seguito si propone un elenco sintetico e non esaustivo delle attività normalmente svolte da tali aree tecniche nell'ambito dei processi su menzionati.

Area	Gruppo	Descrizione	Attività svolte nella gestione Serv. Applicativo
AREA SISTEMI	Amministratori Citrix - S435	Gestori piattaforma Citrix	Aggiornamento / installazione applicazione client su Citrix e gestione abilitazioni
	Amministratori CMDB - S435	Gestori piattaforma Cmdbuild	Implementazione di nuove classi su cmdbuild ed aggiornamento asset materiali ed immateriali gestiti dall'Area Sistemi configurabili come attività nell'ambito del processo di "Service Asset and Configuration Management"
	Amministratori SAP - S435	Gestori Landscape SAP	Gestione degli utenti e delle abilitazioni (ruoli ed autorizzazioni, gestione del supporto OSS di SAP, gestione del Monitoraggio)
	Amministratori	Gestori RDBMS Oracle, Sql	Backup/restore, creazione DB –

	Database - S435	Server, PostgreSQL	schemi, gestione privilegi, installazioni lato server e client, patching, performance tuning, monitoraggio, supporto alle aree di sviluppo in fase di deploy
	Amministratori Hardware - S435	Gestione della infrastruttura tecnologica server e storage (fisica e virtuale)	Capacity Planning, creazione, gestione macchine virtuali, installazione ed update di sistema operativi (Windows, Distribuzioni linux), gestione delle risorse storage, vCpu, Ram, monitoraggio e performance tuning
	Amministratori Server Linux - S435	Gestori delle piattaforme linux dal software di base al middleware alla gestione delle applicazioni in esercizio	Gestione piattaforme applicative (middleware) Linux (installazione, configurazione, aggiornamento, monitoraggio), Gestione applicativa (fileiera A e C) e degli strumenti di ausilio alla gestione applicativa (deploy, autodeploy, mount, esposizione log, Redmine ed SVN), performance tuning
	Amministratori Server Microsoft - S435	Gestori delle piattaforme Microsoft, in particolare dell'ambiente .NET e file server applicativi, nonché del sistema di bilanciamento del traffico realizzato con prodotto LBL	Gestione piattaforme applicative (middleware) Microsoft (configurazione, aggiornamento, monitoraggio), Gestione sistemi di bilanciamento applicativo (LBL), dei sistemi di Monitoraggio realtime (Zabbix) e reportistica relativa (SpagoBI)
	Amministratori Infrastruttura GIS	Gestori del Infrastruttura Geografica (Esri) Regionale e dei Client e Servizi annessi	Gestione piattaforme applicative GIS Esri (configurazione, aggiornamento, monitoraggio), definizione servizi GIS, dati e loro pubblicazione sui sistemi preposti
AREA DOMINIO	Amministratori NT – S435 Amministratori Extrarer – S435	Gestori del sistema di autenticazione Microsoft ed altri servizi di Dominio (Posta, Instant messaging, Sharepoint)	Gestione utenze di dominio (creazione, modifica, proroga, sblocco, reset), dei gruppi AD anche per la aree applicative, gestione certificati SSL interni, DNS interno (ente.regione.emr.it), gestione autorizzazioni su AD e su risorse condivise, monitoraggio e performance tuning
	Amministratori IDM - S435	Gestori del sistema IAM	Gestione target e connettori su IDM, configurazione esposizione applicazioni su AM e Federa, monitoraggio, performance tuning, supporto alle aree applicative per le specifiche di integrazione AM e Federa
	Amministratori Mail - S435	Gestione servizi di Posta ed SMTP	Monitoraggio log traffico snmp, supporto alle aree applicative per l'eventuale intergrazione con i servizi di posta/SMTP
AREA RETI	Area Reti Telematiche – S435	Gestori della rete locale, geografica e Datacenter; gestione del DNS pubblico ed indirizzamento IP	Gestione richieste DHCP, DNS pubblico, indirizzi ip, monitoraggio, performance tuning

AREA SICUREZZA	Area Sicurezza - S435	Gestione della sicurezza logia: firewall, vpn, proxy, IDS/IPS	Modifica configurazione proxy/firewall/VPN a seguito di attivazione/aggiornamento/terminazione di un servizio applicativo
AREA CLIENT		Gestione PDL	Supporto alla verifica del corretto funzionamento e configurazione del SW client eventualmente necessario per l'applicazione (es. JVM, applet java), valutazione potenziamento risorse PC.
SERVICE DESK		Supporto di I livello all'Utenza finale	Gestione delle problematiche di I livello sulle PDL, escalation ai II livelli

Le attività di aggiornamento dei servizi applicativi terminano normalmente con:

- l'aggiornamento dell'ambiente di monitoraggio (es. quando si aggiunge/modifica un contesto web o se cambiano le regole di esposizione dell'applicazione o si aggiunge un DB o un'istanza di application server);
- l'aggiornamento dei CI (Configuration Item) su CMDB (es. quando si aggiunge/modifica un contesto web o se cambiano le regole di esposizione dell'applicazione o si aggiunge un DB o un'istanza di application server);
- rapporto di aggiornamento del servizio applicativo che di norma si sostanzia nella risposta all'area applicativa in fase di risoluzione del ticket RT a cui può aggiungersi, in funzione della complessità dell'intervento, un documento operativo da inserire nel KMDB.

Le aree applicative pur configurandosi come "Clienti" si assumono i seguenti oneri:

- Supportare le aree tecniche del SIIR nell'esecuzione delle attività richieste (es. aggiunta di informazioni ulteriori rilevate come necessarie, analisi dei log in caso di anomalie in fase di aggiornamento);
- Eseguire azioni correttive sia sul codice che sulle configurazioni dell'applicazione (anche sul DB) al fine di superare le eventuali problematiche di aggiornamento;
- Verificare il corretto completamento dell'attività richiesta fornendo un feedback al gruppo risolutore del ticket;
- Nel caso in cui le modifiche applicative, per applicazioni utilizzate dall'utenza regionale, possono determinare un impatto sulla fruizione da parte dell'utente finale, comunicare al Service Desk le informazioni necessarie per gestire al meglio il supporto.

2 procedure di aggiornamento applicazioni SAP

L'ambiente SAP è costituito da un ambiente di sviluppo, da un ambiente di test e da un ambiente di produzione. Gli sviluppi vengono effettuati nell'ambiente di sviluppo e testati in ambiente di test, con deploy a cura dell'area applicativa dedicata (HR, eRecruiting, BW, CRM, R3, BPM, BPC). Il deploy in produzione avviene sempre a cura dell'area applicativa.

Il sistema dei trasporti delle CR vengono fatti in autonomia dalle aree applicative SAP dall'ambiente di Sviluppo all'ambiente di Test.

Il trasporto del CR dal test alla produzione viene fatto sempre dall'area applicativa ma di concerto con l'area sistemistica, che provvederà ad un fermo di sistema (ovviamente previa comunicazione agli utenti finali).

L'area sistemistica SAP interviene solo a fronte di problematiche emerse in fase di deployment e non risolvibili dall'area applicativa.

3 procedure di aggiornamento applicazioni BO

Nel caso dei programmi di contabilità, l'intento è quello di un allineamento continuo con SAP. Questo significa che l'area applicativa dedicata alla business intelligence segue a stretto contatto gli sviluppi che avvengono su SAP, in modo da poter predisporre in breve tempo i corrispettivi oggetti di BI.

L'ambiente BO è costituito da un ambiente di test e da un ambiente di produzione. Gli sviluppi verificati nel loro funzionamento in ambiente di test vengono aggiornati in produzione con deploy a cura dell'area applicativa (su RT sono registrati come "Specialisti BO-BPC ...").

L'area sistemistica interviene sui sistemi BO solo per manutenzione del sistema operativo o per analisi problematiche ma sempre attinenti il solo sistema operativo.

4 procedure di aggiornamento base dati

E' necessario innanzitutto individuare la tipologia di rilascio sulla base dati.

Una prima classificazione avviene in funzione dell'impatto sull'applicazione:

1. rilascio DB da effettuarsi ad applicazione aperta
2. rilascio da effettuarsi ad applicazione chiusa (rilascio DB a cui non corrisponde un rilascio applicativo)
3. rilascio DB corrispondente ad un rilascio applicativo: è necessario coordinare lo spegnimento dell'applicazione e considerare le interrelazioni

Una seconda classificazione dei rilasci avviene in funzione della tipologia di impatto sulla base dati; tale impatto determina anche la metodologia di backup da mettere in atto per un eventuale rollback dell'aggiornamento:

- 1) rilascio con impatti minimi sulla base dati per i quali non si reputa necessario predisporre alcun tipo di backup
- 2) rilascio con impatto di media entità: è opportuno/necessario predisporre misure quali: scripting di oggetti, export/dump di tabelle o interi schemi
- 3) rilascio con impatto rilevante: è necessario effettuare backup/dump aggiuntivi dell'intero DB oltre a prendere le precauzioni di cui al punto 2).

E' evidente che la classificazione non può essere rigida, considerato che ad es. rilasci concettualmente di tipologia 2) potrebbero essere ascrivibili alla categoria 3) in funzione del quantitativo di dati coinvolti.

La classificazione del tipo di rilascio viene effettuata dal gruppo di sviluppo nei casi più semplici, altrimenti viene concordata col gruppo sistemistico insieme con le strategie di backup da mettere in campo per un eventuale rollback.

Il rilascio sulla base dati consta almeno di due componenti: set di script ed istruzioni di rilascio. Queste informazioni dovranno essere messe a disposizione preferibilmente in una share dedicata all'applicazione, altrimenti allegate al ticket. Oltre alle informazioni minime citate potrà essere necessario che siano fornite dal gruppo di sviluppo altri dati ausiliari, es. file di dump da importare o istruzioni dettagliate di rollback.

Gli script dovranno essere forniti in un formato compatibile con i tool di rilascio concordati, in sequenze facilmente riconoscibili, distinguendo con estrema cura classi di istruzioni diverse (DML e DDL), definendo esattamente le politiche delle transazioni (se e quando bisogna effettuare un COMMIT), evitando assolutamente di inserire COMMIT negli script che potrebbero compromettere la possibilità di effettuare un rollback dell'aggiornamento (rollback qui inteso in senso estensivo e non nell'accezione precipua dello RDBMS).

4.1 Workflow di rilascio

L'area applicativa apre il ticket sul sistema RT:

- a) ai DBA (nome del gruppo assegnatario "*Amministratori Database - S435*") nel caso 1. della classificazione riguardante l'impatto sull'applicazione;
- b) ai sistemisti delle piattaforme applicative nei restanti casi 2. e 3.

Nel caso a) i DBA procedono in modo indipendente al rilascio.

Nel caso b) i sistemisti delle piattaforme applicative aprono un ticket, figlio del ticket aperto dal gruppo di sviluppo, ai DBA scambiando le opportune informazioni di coordinamento.

I DBA effettuano il rilascio chiudendo il ticket figlio e ripassando il controllo del workflow ai sistemisti delle piattaforme applicative.

A rilascio effettuato il gruppo di sviluppo dovrà attestare il buon esito dell'aggiornamento ed in caso contrario saranno attivate le azioni correttive (compreso l'eventuale rollback).

5 procedure di aggiornamento applicazioni filiera C

Le applicazioni in filiera C, "LAMP" (PHP su Apache con database MySQL), di TEST e PRODUZIONE sono aggiornate manualmente dall'area Sistemi del SIIR. I sorgenti di alcune applicazioni sono "versionati" nei sistemi di VCS (Subversion e Git) della regione rendendo possibile l'aggiornamento automatico in TEST e facilitando l'aggiornamento in PRODUZIONE.

Il rilascio dell'applicazione consta almeno di due componenti: pacchetto di installazione ed istruzioni di rilascio. Queste informazioni possono essere messe a disposizione in una share dedicata all'applicazione o allegate al ticket. Oltre alle informazioni minime citate potrà essere necessario che siano fornite dall'area applicativa altre informazioni ausiliari, es.: fermo applicativo in attesa di esecuzione script su database, orari, script batch da schedulare, istruzioni dettagliate di rollback.

5.1 Workflow di rilascio

L'area applicativa apre il ticket sul sistema RT:

- richiede l'aggiornamento al gruppo Linux Administrator (nome del gruppo assegnatario "Amministratori Server Linux – S435");
- Se i sorgenti sono "versionati" sui sistemi di VCS della regione l'aggiornamento viene eseguito con un *check-out* del relativo repository;
- Se i sorgenti non sono "versionati" sui sistemi della regione l'area applicativa fornisce i files da aggiornare (su share dedicata o allegati al ticket) al gruppo *Amministratori Server Linux*;
- L'aggiornamento viene eseguito e viene monitorato il log del Web Server.
- viene verificata la corretta risposta della pagina iniziale dell'applicazione;
- Se l'aggiornamento fallisce con evidenti errori nel log di Apache si segnala all'area applicativa e si attendono istruzioni.

Per i Workflow sopra descritti, se sono necessarie operazioni che richiedono interventi anche da parte di altre aree tecniche del SIIR, i Linux Administrator aprono uno o più ticket, figli dei ticket di cui sopra, ai gruppi RT afferenti a tali aree fornendo le opportune informazioni. Terminata ogni singola attività, i gruppi destinatari il ticket e i Linux Administrator procedono con l'aggiornamento dell'applicazione seguendo le operazioni descritte ai punti precedenti.

A rilascio effettuato, se non si individuano errori nei log, l'area applicativa dovrà attestare il buon esito dell'aggiornamento ed in caso contrario saranno attivate le azioni correttive (compreso l'eventuale rollback).

6 procedure di aggiornamento applicazioni filiera A

Le applicazioni in filiera A, J2EE (installate sui container Jboss e Tomcat), di Test e di Produzione sono aggiornate dall'Area Sistemi del SIIR utilizzando diverse metodologie in funzione dei Container e delle versioni degli stessi. Di seguito si descrivono tali metodologie.

Il rilascio dell'applicazione consta almeno di due componenti: file `<.war>` o `<.ear>` ed istruzioni di rilascio. Queste informazioni dovranno essere messe a disposizione in una share dedicata all'applicazione. Oltre alle informazioni minime citate potrà essere necessario che siano fornite dall'area applicativa altre informazioni ausiliari, es.: fermo applicativo in attesa di esecuzione script su database, orari, script batch da schedulare, istruzioni dettagliate di rollback.

N.B. Non si accettano rilasci che prevedano la sostituzione puntuale di files all'interno della webapp già deployata.

6.1 Workflow di rilascio: container Tomcat

Gli aggiornamenti delle applicazioni installate su tale container in TEST e PRODUZIONE sono eseguiti in modalità manuale.

L'area applicativa apre il ticket sul sistema RT:

- richiede l'aggiornamento al gruppo Linux Administrator (nome del gruppo assegnatario "Amministratori Server Linux – S435");
- vengono applicate eventuali configurazioni specifiche per l'ambiente;
- viene spento il container;
- viene eseguita una copia di backup della versione corrente dell'applicazione;
- viene copiato il nuovo pacchetto applicativo all'interno del container;
- viene fatta pulizia delle cartelle temporanee;
- viene avviato il Container e controllati i log compresi i log specifici dell'applicazione (se vi sono);
- viene verificata la corretta risposta della pagina iniziale dell'applicazione;
- se il deploy fallisce si segnala all'area applicativa e si attendono istruzioni.

6.2 Workflow di rilascio: container Jboss AS 7, Jboss 5 e Jboss 4 - TEST

Gli aggiornamenti delle applicazioni installate su tali container per il solo ambiente di TEST sono gestiti con un processo automatico chiamato "autodeploy". Il processo automatico ricava le informazioni necessarie al deploy dal catalogo delle applicazioni presente sul CMDB, inoltre verifica se l'utente che ha copiato il pacchetto applicativo (su share dedicata) ha i diritti per installare l'applicazione, tracciando l'operazione richiesta in un file di log specifico.

La procedura seguita dall'area applicativa è la seguente:

- copia il pacchetto nella relativa share dedicata sul fileserver *deployjava* (.ente.regione.emr.it);
- il processo di autodeploy ricava l'application server partendo dal nome del pacchetto ed eseguendo una ricerca sul CMDB.
- Autodeploy esegue il deploy del pacchetto applicativo restituendo l'esito dell'operazione all'utente.

L'area applicativa apre il ticket sul sistema RT solo ne caso in cui il processo di autodeploy restituisce un errore:

- richiede la verifica al gruppo Linux Administrator (nome del gruppo assegnatario "Amministratori Server Linux – S435");
- viene verificato il file di log del autodeploy;
- vengono effettuate le operazioni manuali di rollback ed eseguite le azioni correttive.
- Risolta l'anomalia il gruppo di sviluppo dovrà attestare il buon esito dell'aggiornamento.

Per questa tipologia di deploy, se sono necessarie operazioni sul database dell'applicazione, l'area applicativa apre il ticket direttamente ai DBA (come descritto nel paragrafo 2).

6.3 Workflow di rilascio: container Jboss EAP 6 - TEST

Gli aggiornamenti delle applicazioni installate su tale container per il solo ambiente di TEST sono gestiti con un processo manuale da parte dell'Area Sistemi del SIIR.

E' in corso, ma non ancora attivata, la configurazione della console web di amministrazione per profili di autorizzazione al fine di consentire la delega dei deploy all'area applicativa.

La procedura seguita è la seguente:

- l'area applicativa consegna il pacchetto (file <.war> o <.ear>) nella share dedicata sul fileserver *rilascijava* (.ente.regione.emr.it);
- l'area applicativa richiede l'aggiornamento al gruppo Linux Administrator (nome del gruppo assegnatario "Amministratori Server Linux – S435");
- il deploy viene eseguito e se richiesto vengono riavviate le istanze e/o pulite le directories temporanee;
- il log del container viene monitorato per verificare la presenza di eventuali errori.
- viene verificata la corretta risposta della pagina iniziale dell'applicazione;
- se il deploy fallisce si segnala all'area applicativa e si attendono istruzioni.

6.4 Workflow di rilascio: container Jboss EAP 6, Jboss AS 7, Jboss 5 e Jboss 4 - Produzione

li aggiornamenti delle applicazioni installate su tali container per l'ambiente di Produzione sono gestiti con un processo manuale da parte dell'Area Sistemi del SIIR.

La procedura seguita è la seguente:

- l'area applicativa consegna il pacchetto (file <.war> o <.ear>) nella share dedicata sul fileserver *rilascijava* (.ente.regione.emr.it);
- l'area applicativa richiede l'aggiornamento al gruppo Linux Administrator (nome del gruppo assegnatario "Amministratori Server Linux – S435");
- Il deploy viene eseguito e se richiesto vengono riavviate le istanze e/o pulite le directories temporanee.
- Il log viene monitorato per verificare la presenza di eventuali errori.
- viene verificata la corretta risposta della pagina iniziale dell'applicazione;
- se il deploy fallisce si segnala all'area applicativa e si attendono istruzioni.

Per i Workflow sopra descritti (ad eccezione del Workflow 4.2), se sono necessarie operazioni che richiedono interventi anche da parte di altre aree tecniche del SIIR, i Linux Administrator aprono uno o più ticket, figli dei ticket di cui sopra, ai gruppi RT afferenti a tali aree fornendo le opportune informazioni. Terminata ogni singola attività, i gruppi destinatari il ticket e i Linux Administrator procedono con l'aggiornamento dell'applicazione seguendo le operazioni descritte ai punti precedenti.

A rilascio effettuato, se non si individuano errori nei log, l'area applicativa dovrà attestare il buon esito dell'aggiornamento ed in caso contrario saranno attivate le azioni correttive (compreso l'eventuale rollback).

7 procedure di aggiornamento applicazioni filiera B

Le applicazioni in filiera B (Microsoft), .NET (installate su IIS), di Test e di Produzione sono aggiornate utilizzando diverse metodologie in funzione delle aree applicative richiedenti. Pertanto gli aggiornamenti possono essere fatti direttamente dalle aree applicative (vedremo di seguito in quali casi) o mediate dall'Area Sistemi del SIIR.

A differenza degli ambienti di runtime delle applicazioni in filiera A, tutte le applicazioni della filiera B sono consolidate su un'unica piattaforma distinta tra ambiente di Test e di Produzione. In particolare, le configurazioni degli application server sono centralizzate su un file server remoto ed esposte tramite share di rete:

- \\fileserver\webcfg\$\TEST, per l'ambiente di Test
- \\fileserver\webcfg\$\PROD, per l'ambiente di Produzione

a cui hanno accesso solo gli Amministratori di sistema. I dati (i contenuti e quindi le applicazioni stesse) sono invece centralizzati sulla share:

- \\fileserver\webcontent\$\TEST, per l'ambiente di Test
- \\fileserver\webcontent\$\PROD, per l'ambiente di Produzione

e gli accessi sono gestiti centralmente tramite gruppi Active Directory.

Gli ambienti .NET si suddividono in due aree dal punto di vista della gestione del servizio applicativo:

1. **(delega) - Ambienti con contenuti gestiti da area applicativa .NET del SIIR:**
 - l'aggiornamento a minore e medio impatto sull'applicazione e sulla base dati è totalmente in carico a tale area sia per l'ambiente di test che per l'ambiente di produzione;
 - l'aggiornamento a medio ed alto impatto sull'applicazione e sulla base dati è coordinato da tale area sia per l'ambiente di Test che di Produzione ma prevede interventi dell'Area Sistemi del SIIR per azioni specifiche che possono ad esempio riguardare le strategie di backup da mettere in campo per un eventuale rollback.
2. **(gestito) - Ambienti con contenuti gestiti dall'Area Sistemi del SIIR:** tutte le attività di aggiornamento sull'applicazione e sulla base dati vengono eseguite da tale Area. Le aree applicative si configurano come meri richiedenti.

7.1 Workflow di rilascio: delega ad Area applicativa SIIR

Questo ambito è relativo a tutte le applicazioni in cui il referente del servizio applicativo appartiene all'area applicativa del SIIR. Per questo tipo di applicazioni è stata creata una struttura sul file server del tipo <nome servizio>_SSIIR e a queste share è stato assegnato il permesso di R/W agli appartenenti a tale area (configurata su Active Directory come un gruppo specifico).

In questo caso l'Area Sistemi interviene, con apertura di ticket da parte dell'area applicativa, solo a fronte di problematiche che si dovessero presentare in fase di aggiornamento.

7.2 Workflow di rilascio: gestito da Area Sistemi SIIR

Questo ambito è relativo a tutte le applicazioni in cui il referente di progetto non appartiene all'area applicativa del SIIR ma tipicamente appartiene ad altre direzioni/strutture regionali che hanno autonomia tecnica e di risorse per gestire progetti di sviluppo applicativo.

Pertanto è l'Area Sistemi del SIIR che esegue le attività di aggiornamento sull'applicazione e sulla base dati configurandosi un vero e proprio servizio di *Hosting*.

Per le applicazioni che rientrano in questo ambito è stata creata una struttura del tipo:

- <nome servizio>_<nomedirezione> per le aree applicative che lavorano presso gli uffici dell'Ente Regione. Negli ambienti di TEST è stato assegnato il permesso di R/W agli appartenenti ad ogni singola area (configurata su Active Directory come un gruppo specifico). Non è consentito l'accesso ai contenuti degli ambienti di produzione.
- <nome servizio>_SSIIR_esterni oppure <nome servizio> per le aree applicative esterne (fornitori esterni e aree applicative non operative presso gli uffici dell'Ente Regione). In questo caso tali aree non hanno nessun accesso (né sugli ambienti di TEST né sugli ambienti di produzione). Per ogni singola area è stato predisposto uno spazio dedicato ai rilasci sul servizio FTPS regionale.

La procedura seguita è la seguente:

- l'area applicativa che NON lavora presso gli uffici dell'Ente Regione predispone il pacchetto applicativo ed effettua un upload sul proprio spazio FTPS;
- l'area applicativa che lavora presso gli uffici dell'Ente Regione predispone il pacchetto applicativo ed effettua un upload sulla share dedicata.
- l'area applicativa richiede l'aggiornamento al gruppo Microsoft Administrator (nome del gruppo assegnatario "Amministratori Server Microsoft – S435") aprendo un ticket RT;
- l'aggiornamento viene eseguito seguendo le istruzioni indicate nel ticket;
- il log del Web Server viene monitorato per verificare la presenza di eventuali errori;
- viene verificata la corretta risposta della pagina iniziale dell'applicazione;
- se l'aggiornamento fallisce si segnala all'area applicativa e si attendono istruzioni.

La richiesta di aggiornamento dell'applicazione deve contenere i seguenti elementi:

- se pianificato, orario in cui effettuare l'attività
- PATH di rilascio (dove è contenuto il pacchetto applicativo da installare)
- PATH di destinazione (dove deve essere deployato il pacchetto)
- URL (indicazione del link con cui viene consultato l'applicativo)
- Istruzioni per il rilascio (note di dettaglio per pilotare le configurazioni custom applicative, tipicamente riguarda il web.config dell'applicazione)
- Altro: es. indicazione se è necessario fermare applicativo in attesa di esecuzione script su database, script batch da schedulare, istruzioni dettagliate di rollback.

Per questo Workflow, se sono necessarie operazioni che richiedono interventi anche da parte di altre aree tecniche del SIIR, i Microsoft Administrator aprono uno o più ticket, figli dei ticket di cui sopra, ai gruppi RT afferenti a tali aree fornendo le opportune informazioni. Terminata ogni singola attività, i gruppi destinatari il ticket e i Microsoft Administrator procedono con l'aggiornamento dell'applicazione seguendo le operazioni descritte ai punti precedenti.

A rilascio effettuato, se non si individuano errori nei log, l'area applicativa dovrà attestare il buon esito dell'aggiornamento ed in caso contrario saranno attivate le azioni correttive (compreso l'eventuale rollback).

8 procedure di aggiornamento applicazioni GIS

Le applicazioni dell'area GIS, di Test e di Produzione sono aggiornate utilizzando diverse metodologie in funzione delle aree applicative richiedenti. Pertanto gli aggiornamenti possono essere fatti direttamente dalle aree applicative (fornitori esterni supporto GIS, Servizio Statistica Informazione Geografica e Servizio Geologico, Sismico dei Suoli) o mediate dall'Area Sistemi del SIIR.

Il rilascio dell'applicazione in ambito GIS consta di un certo numero di componenti si va dal rilascio di file <.war> o <.ear> ed istruzioni di rilascio, la predisposizione di apposite mount su sistemi linux e l'eventuale esposizione dei log, dalla definizione di utenti e relativi schemi su ambiente oracle, dal caricamento di dati in queste utenze attraverso client specialistici Esri, dalla creazione e configurazione di servizi specifici sulle macchine dell'infrastruttura quali map service, image service, cache, tool di geoprocessing o servizi in standard OGC.

Gli ambienti GIS si suddividono in due aree dal punto di vista della gestione dei dati del servizio applicativo GIS:

1. **(delega) - Ambienti con contenuti gestiti da area applicativa (fornitori esterni supporto GIS, Servizio Statistica Informazione Geografica e Servizio Geologico, Sismico dei Suoli):**
 - l'aggiornamento a minore e medio impatto sull'applicazione e base dati GIS è totalmente in carico a tale area sia per l'ambiente di test che per l'ambiente di produzione (ad esclusione dei deploy applicativi e delle attività citate in seguito);
 - l'aggiornamento a medio ed alto impatto sull'applicazione e sulla base dati è coordinato da tale area sia per l'ambiente di Test che di Produzione ma prevede interventi dell'Area Sistemi del SIIR per azioni specifiche che possono ad esempio riguardare le strategie di backup da mettere in campo per un eventuale rollback.
2. **(gestito) - Ambienti con contenuti gestiti dall'Area Sistemi del SIIR:** tutte le attività di aggiornamento sull'applicazione e sulla base dati vengono eseguite da tale Area. Le aree applicative si configurano come meri richiedenti.

8.1 Workflow di rilascio: delega ad Area applicativa

Questo ambito è relativo al punto 1 di cui sopra. Per questo tipo di applicazioni è stata creata una organizzazione sui Server GIS e database alle quali è stato concesso l'accesso Amministrativo alle

Console di Gestione e con Software specialistici ESRI agli appartenenti a tale area (configurata su Active Directory con gruppi specifici).

In questo caso l'Area Sistemi interviene, con apertura di ticket da parte dell'area applicativa, solo a fronte di problematiche che si dovessero presentare in fase di aggiornamento.

8.2 Workflow di rilascio: Servizi GIS – Servizi Mappa ed Immagine

Gli aggiornamenti sui servizi GIS vengono eseguiti in modalità manuale o attraverso software specialistici Esri.

L'area applicativa apre il ticket sul sistema RT:

- l'area applicativa che NON lavora presso gli uffici dell'Ente Regione predispone i pacchetto dati ed effettua un upload sul proprio spazio FTPS;
- l'area applicativa che lavora presso gli uffici dell'Ente Regione predispone i dati ed indica ove essi sono resi disponibili;
- richiede al gruppo Amministratori Infrastruttura GIS le seguenti possibili attività:
 - creazione/aggiornamento di dati e servizi GIS in ambiente Esri e la pubblicazione sui back-end applicativi GIS;
 - copia/inserimento di dati GIS o la verifica delle configurazioni ad essi attribuite su Server dell'Infrastruttura GIS;
 - creazione sui servizi GIS caricati ed esposti di eventuali capabilities accessorie (es. cache o servizi in standard OGC) e che queste vengano esposte su internet/intranet;
- viene verificata la corretta risposta del Servizio GIS pubblicato;
- se l'aggiornamento non soddisfa i prerequisiti iniziali si segnala all'area applicativa e si attendono istruzioni.

La richiesta di aggiornamento del Servizio GIS deve contenere i seguenti elementi:

- PATH di rilascio (dove sono contenuti i dati ed il pacchetto GIS da installare)
- PATH di destinazione (dove deve essere deployato il pacchetto)
- URL (indicazione del link con cui viene consultato il Servizio GIS)
- Istruzioni per il rilascio (note di dettaglio)

8.3 Workflow di rilascio: Customizzazione Back-end GIS – Tool Geoprocessing

Gli aggiornamenti di componenti sulle macchine GIS vengono eseguiti in modalità manuale sulle macchine che assolvono a funzione di server GIS.

L'area applicativa apre il ticket sul sistema RT:

- l'area applicativa che NON lavora presso gli uffici dell'Ente Regione predispone librerie o file ed effettua un upload sul proprio spazio FTPS;
- l'area applicativa che lavora presso gli uffici dell'Ente Regione predispone librerie o file ed effettua un upload sulla share dedicata;

- richiede al gruppo Amministratori Infrastruttura GIS le seguenti possibili attività:
 - copia di file resi disponibili nelle directory applicative dei server gis (eventualmente sostituendo i precedenti)
 - registrazione/deregistrazione di dll sia per le componenti desktop che server installate sulle postazioni server GIS
 - creazione/aggiornamento di connessioni GIS ai DB e percorsi dati di competenza e la loro configurazione sulle postazioni server GIS utilizzando software specialistici Esri
 - creazione/aggiornamento di connessioni amministrative relative ai Server GIS ra GIS e la loro configurazione sulle postazioni server GIS utilizzando software specialistici Esri
 - creazione/aggiornamento servizi GIS in ambiente Esri e la pubblicazione sui Back-End applicativi GIS;
- viene verificata la corretta esecuzione dei Servizi GIS configurati
- se l'aggiornamento non soddisfa i prerequisiti iniziali si segnala all'area applicativa e si attendono istruzioni.

La richiesta di aggiornamento del Back-End GIS deve contenere i seguenti elementi:

- PATH di rilascio (dove è contenuto il pacchetto da installare)
- PATH di destinazione (dove deve essere deployato il pacchetto)
- configurazioni (indicazione delle configurazioni da attribuire al servizio)
- Istruzioni per il rilascio (note di dettaglio)

Per i Workflow 6.2 e 6.3, se sono necessarie operazioni che richiedono interventi anche da parte di altre aree tecniche del SIIR, gli Amministratori Infrastruttura GIS aprono uno o più ticket, figli dei ticket di cui sopra, ai gruppi RT afferenti a tali aree fornendo le opportune informazioni. Terminata ogni singola attività, i gruppi destinatari il ticket e gli Amministratori Infrastruttura GIS procedono con l'aggiornamento dell'applicazione seguendo le operazioni descritte ai punti precedenti.

A rilascio effettuato, se non si individuano errori nei log, l'area applicativa dovrà attestare il buon esito dell'aggiornamento ed in caso contrario saranno attivate le azioni correttive (compreso l'eventuale rollback).

Allegato 5: Clausola “accessibilità” per contratti e capitolati tecnici

Quando si scrive un contratto o un capitolato tecnico per l'**acquisizione di un prodotto o servizio web** (sito, applicazione o CD-ROM/DVD) è necessario inserire una clausola che preveda il rispetto dei requisiti di accessibilità.

Il contenuto di tale clausola deve essere simile a questo:

Accessibilità

La realizzazione/modifica/fornitura del sito/applicazione/prodotto/servizio oggetto del contratto dovrà risultare accessibile secondo la Legge 9 gennaio 2004, n. 4 "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici", e successive integrazioni e variazioni, e in particolare rispettare i requisiti e la metodologia indicati nell'allegato A del DM 20/3/2013 (reperibile in Gazzetta Ufficiale <http://www.gazzettaufficiale.it/eli/id/2013/09/16/13A07492/sq>) .

Il rispetto dei requisiti di accessibilità verrà verificato dal cliente all'atto della consegna da parte del fornitore, e sarà poi accertato dal Servizio SIIR attraverso le verifiche preliminari al rilascio in produzione, prima della messa online del sito e delle applicazioni o di loro modifiche sostanziali. L'Amministrazione inoltre si riserva in qualunque momento, su propria iniziativa o su segnalazione di terzi, di effettuare verifiche di accessibilità ed usabilità sui servizi web oggetto del presente contratto resi dal fornitore, il quale dovrà provvedere, senza ulteriori oneri per l'Amministrazione, alla messa a norma di quanto eventualmente riscontrato difforme a seguito di tali verifiche.

Anche quando si scrive un contratto o un capitolato tecnico per l'**acquisizione di beni/servizi che riguardano sistemi operativi, applicazioni o prodotti a scaffale** è necessario inserire una clausola che preveda il rispetto dei requisiti di accessibilità.

Il contenuto di tale clausola deve essere simile a questo:

Accessibilità

*Il prodotto/Servizio oggetto del contratto dovrà rispondere ai criteri di accessibilità stabiliti dalla Legge 9 Gennaio 2004, n. 4, "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici" e successive integrazioni e variazioni, in particolare dal Decreto Ministeriale 8 agosto 2005 - **Allegato D**.*

Il rispetto dei requisiti di accessibilità verrà verificato dal cliente sulla base di quanto dichiarato a tal proposito dal fornitore, e sarà poi accertato dal Servizio SIIR attraverso le verifiche preliminari alla presa in carico.

Allegato 6: Lista dei requisiti di accessibilità

1	Premessa	2
2	Requisiti da verificare	3
2.1	Requisiti da verificare (sottoinsieme base)	3
2.2	Requisiti da verificare (a campione)	5

1 Premessa

Ogni sito¹, CD-Rom, applicazione basata su tecnologie internet² realizzato da o per conto della Regione Emilia-Romagna deve rispettare i requisiti tecnici sull'accessibilità previsti dalla Legge n. 4/2004.

I requisiti tecnici che guidano le verifiche di accessibilità, previsti dalla legge n. 4/2004 e contenuti nell'allegato A del DM 8 luglio 2005, sono stati rivisti nel 2013 e fanno riferimento alle WCAG2 e ai loro criteri di successo³.

Per semplificare le procedure di verifica dell'accessibilità effettuate dalla Regione nell'ambito della *governance* dei sistemi IT, è stato individuato un sottoinsieme base di requisiti che saranno verificati su ogni prodotto acquistato o realizzato per nome e conto della Regione.

La Regione richiede comunque il rispetto di tutti i requisiti previsti dalla normativa e si riserva l'opportunità di verificare a campione i requisiti non inseriti nel sottoinsieme base.

Come **supporto alla verifica manuale** la Regione mette a disposizione un software automatico che vi invitiamo ad usare.

<http://www.validatore.it>

¹ http://www.pubbliaccesso.gov.it/normative/legge_20040109_n4.htm Legge 4/2004 Art. 4 comma 2

² <http://www.pubbliaccesso.gov.it/normative/DM080705.htm#testo> D.M. 8/7/2005 Art. 2 comma

³ www.gazzettaufficiale.it/eli/id/2013/09/16/13A07492/sg Nuovi requisiti e punti di controllo per l'accessibilità Web

2 Requisiti da verificare

2.1 Requisiti da verificare (sottoinsieme base)

Colori – Comprensibile in B/N

Le istruzioni per comprendere ed operare sul contenuto non si devono basare solo su caratteristiche sensoriali, come forma, dimensione, orientamento, posizione. In particolare il colore non deve essere l'unico mezzo per veicolare informazioni come ad esempio un'azione, la richiesta di una risposta ad un'azione.

Riferimenti: Requisiti 3.3, 4.1; WCAG 1.3.3, 1.4.1

Rende sicuramente non soddisfatto il requisito:

- ▶ Identificare il contenuto solo dalla forma o dal colore (F14)
- ▶ Usare unicamente simboli grafici per veicolare informazioni (F26)
- ▶ Alternative testuali che non includono informazioni date dalla differenza di colore di un'immagine (F13)
- ▶ Link che sono solamente di un colore diverso dal testo (F73)
- ▶ Campi dei moduli obbligatori evidenziati solo da una differenza di colore (F81)

Colori – Contrasto corretto

Il testo e lo sfondo, anche nelle immagini, devono rispettare l'algoritmo dei colori ed avere quindi un rapporto nel contrasto di 4.5:1 tranne: per i logo, il testo grande (rapporto 3:1) e testo volutamente reso poco visibile (es. azioni inattive).

N.B. La verifica si ottiene facilmente per mezzo del "Colour Contrast Analyser version 2" usando l'algoritmo **Luminosità**

Riferimenti: Requisiti 4.3; WCAG 1.4.3

Rende sicuramente non soddisfatto il requisito:

- ▶ Usare immagini di sfondo che non hanno sufficiente contrasto col testo in primo piano (F83)

Link e controlli – Utilizzabili

Informazioni, struttura e relazioni tra gli elementi della pagina devono essere definiti tramite il codice di marcatura e non solo attraverso la presentazione. Inoltre tutti i componenti dell'interfaccia (es. link, campi, menù, bottoni, ecc.) si devono poter utilizzare tramite tastiera analogamente a quanto si riesce a fare col mouse.

N.B. Fare attenzione in particolare ai titoli (Hn) ed alle etichette esplicite (label-for) per tutti i campi. Verificare che si possa entrare ed uscire dai controlli usando la sola tastiera.

Riferimenti: Requisiti 3.1, 5.1, 5.2, 11.2; WCAG 1.3.1, 2.1.1, 2.1.2, 3.3.2

Rende sicuramente non soddisfatto il requisito:

- ▶ Informazioni insufficienti nel DOM per indicare le relazioni uno a uno degli elementi (es. Tra etichette <label> e campi <input>) (F17)
- ▶ Usare gli spazi per simulare le colonne di una tabella (F34)
- ▶ Usare gli script per simulare i link (F42)
- ▶ Usare il markup in modo non conforme alle specifiche (F43)
- ▶ Usare solo eventi legati a specifici dispositivi di input (mouse, touch, gestures ecc.)(F54)
- ▶ Usare gli script per spostare il focus da un elemento, quando questo lo riceve (F55)
- ▶ Combinare uno o più elementi in modo tale che con la semplice tabulazione non si riesca a superarli (F10)

Multimedia – Alternative

Tutti gli elementi non testuali (immagini, video, audio) quando hanno un significato o una funzione devono avere un'alternativa testuale equivalente.

N.B. Fare attenzione soprattutto ai controlli (es. bottoni, CAPTCHA, ecc.)

Riferimenti: Requisiti 1.1; WCAG 1.1.1

Rende sicuramente non soddisfatto il requisito:

- ▶ Usare alternative che non sono tali (es., il nome del file) (F30)
- ▶ Non aggiornare l'alternativo quando cambia l'oggetto non di testo (F20)
- ▶ Usare il CSS per includere immagini importanti (es. il nome del sito) (F3)
- ▶ Non inserire alternative vuote (`alt=""`) per elementi che devono essere ignorati (F39)
- ▶ Non mettere alternative su elementi di input fatti da immagini (F65)
- ▶ Non indicare nell'alternativo informazioni veicolate magari tramite il solo cambio di colore nell'immagine (F13)

Multimedia – Flash (> 3 al sec.)

Le pagine Web non devono contenere nulla che lampeggi per più di tre volte al secondo.

Riferimenti: Requisiti 7.2; WCAG 2.3.2

Multimedia – No audio (se + 3 secondi)

Se un contenuto audio all'interno di una pagina Web è eseguito automaticamente per più di tre secondi, allora deve essere fornita una funzionalità per metterlo in pausa o interromperlo, oppure deve essere fornita una modalità per il controllo del volume del contenuto audio che sia indipendente dal controllo predefinito del sistema.

Riferimenti: Requisiti 4.2; WCAG 1.4.2

Script - Direttamente accessibili

Preferite i componenti standard e non modificate (rendendolo "invisibile") il focus sugli elementi delle pagine. Se si utilizzano componenti non standard, o si modifica il comportamento degli elementi verificare che valore, ruolo e stato degli elementi siano sempre resi disponibili all'utente, in particolare alle tecnologie assistive.

N.B. Portate il focus sugli elementi che devono riceverlo (es. messaggi di errore dopo un input errato) perché non tutti gli utenti possono vedere o usare il mouse

Riferimenti: Requisiti 8.7, 12.2; WCAG 2.4.7, 4.1.2

Rende sicuramente non soddisfatto il requisito:

- ▶ Usare gli script per spostare il focus da un elemento, quando questo lo riceve (F55)
- ▶ Cambiare lo stile agli elementi ed ai loro bordi in modo che non sia più percepibile (F78) l'indicazione del focus
- ▶ Usare componenti "personalizzati" che non hanno API per l'accessibilità o le usano in modo incompleto (F15)

Testo - Adattabilità

Il testo si deve poter ingrandire del 200% senza perdita di contenuto o funzionalità (es. senza sovrapposizioni che lo rendono incomprensibile)

Riferimenti: Requisiti 4.4; WCAG 1.4.4

Rende sicuramente non soddisfatto il requisito:

- ▶ Quando si ridimensiona il testo al 200% il testo, le immagini o i controlli sono troncati, tagliati o nascosti (F69)

- ▶ Quando si ridimensiona il testo, i controlli dei form non si ridimensionano (F80)

Tempo – Regolabile

Per ogni limite di tempo nel contenuto, che non sia essenziale per l'attività, o per ciò che non deve essere in tempo reale, deve essere possibile almeno una di queste cose: rimuovere il limite, regolare la scadenza, estenderla prima del termine con un'azione semplice.

N.B. Mantenere le scadenze delle sessioni sufficientemente lunghe e segnalare anche tramite istruzioni un sistema per estenderle

Riferimenti: Requisiti 6.1, 6.2; WCAG 2.2.2

Rende sicuramente non soddisfatto il requisito:

- ▶ Includere contenuto che "scorre" quando lo scorrimento non è essenziale per l'attività, senza inserire meccanismi per fermare e far ripartire lo scorrimento (F16)
- ▶ Usare l'elemento "blink" (F47)
- ▶ Usare text-decoration:blink senza un meccanismo per arrestarlo entro 5 secondi (F4)
- ▶ Usare script che causano lampeggiamenti senza prevedere meccanismi che li (F50) arrestino entro i primi 5 secondi
- ▶ Usare un object o applet, come Java o Flash, che ha del contenuto che lampeggia senza un meccanismo per metterlo in pausa se dura oltre 5 secondi.(F7)

2.2 Requisiti da verificare (a campione)

Elemento	Requisito	Rev.	WCAG 2.0	Ok ?
HTML	Codice valido	12.1	4.1.1	
	Definire lingua	9.1, 9.2	3.1.1, 3.1.2	
	Titolo pagina	8.2	2.4.2	
	Skiplink	8.1	2.4.1	
	Link home/briciole	8.5	2.4.5	
	Sequenza significativa	3.2	1.3.2	
	Ordine focus	8.3	2.4.3	
CSS	Codice valido	12.1	4.1.1	
IMMAGINI	Non al posto del testo	4.5	1.4.5	
	Lampeggiamenti	7.1	2.3.2	
LINK	Significativi (nel contesto)	8.4	2.4.4	
	Coerenti	10.4	3.2.4	
Menù	Costante	10.3	3.2.3	

Elemento	Requisito	Rev.	WCAG 2.0	Ok ?
	Titolo <Hn> prima	8.6	2.4.6	
FORM	Parsing	12.1, 8.6	4.1.1, 2.4.6	
MULTIMEDIA	Solo audio solo video	2.1	1.2.1	
	Sottotitoli (registrazioni)	2.2	1.2.2	
	Trascrizioni e descrizioni	2.3	1.2.3, 1.2.5	
	Sottotitoli (diretta)	2.4	1.2.4	
SCRIPT	Identificazione errori	11.1	3.3.1	
	Suggerimento errori	11.3	3.3.3	
	Prevenzione errori	11.4	3.3.4	
	Prevedibili (input, focus)	10.1, 10.2	3.2.1, 3.2.2	

Allegato 7: Liste di controllo per le misure minime di sicurezza

Misure minime da osservare per tutti i trattamenti	Note di compilazione e risposte attese	Implementazione	Note
Esiste una procedura di autenticazione che permette l'identificazione univoca dell'utente attraverso opportune credenziali di autenticazione	Obbligatorio per dati in perimetro d.lgs 196/2003		
È utilizzata una parola chiave (password), quando prevista dal sistema di autenticazione, composta da almeno otto caratteri	Obbligatorio per dati in perimetro d.lgs 196/2003		
Esiste la possibilità di modifica della parola chiave, quando prevista dal sistema di autenticazione, da parte dell'utente al primo utilizzo e, successivamente, almeno ogni sei mesi	Obbligatorio per dati in perimetro d.lgs 196/2003		
Esistono meccanismi di disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica	Obbligatorio per dati in perimetro d.lgs 196/2003		
I codici di identificazione già impiegati non sono riutilizzati nel tempo assegnandoli ad altri utenti	Obbligatorio per dati in perimetro d.lgs 196/2003		
Esistono meccanismi di autorizzazione per la separazione dei privilegi degli incaricati in base a diversi profili autorizzativi	Obbligatorio per dati in perimetro d.lgs 196/2003		
Esistono meccanismi di protezione dei dati contro le minacce di intrusione e dell'azione di programmi malevoli (es. cifratura delle password, impiego di firewall o di software antivirus, hardening dei sistemi, ecc ...)	Obbligatorio per dati in perimetro d.lgs 196/2003		
I programmi sono aggiornati periodicamente per prevenire le vulnerabilità e correggerne difetti (es. patch di sistema, aggiornamenti antivirus, ecc ...)	Obbligatorio per dati in perimetro d.lgs 196/2003		
Esistono meccanismi di backup e ripristino, con salvataggio dei dati effettuato con frequenza almeno settimanale	Obbligatorio per dati in perimetro d.lgs 196/2003		

Misure minime ulteriori da osservare nel caso di trattamenti di dati sensibili e/o giudiziari	Note di compilazione e risposte attese	Implementazione	Note
Esiste la possibilità di modifica della parola chiave quando prevista dal sistema di autenticazione, da parte dell'utente al primo utilizzo e, successivamente, almeno ogni tre mesi	Obbligatorio per dati in perimetro d.lgs 196/2003		
Esistono meccanismi di ripristino dei dati che permettono la ricostruzione degli stessi, in caso di danneggiamento, in tempi non superiori ai sette giorni	Obbligatorio per dati in perimetro d.lgs 196/2003		
Sono utilizzate tecniche di cifratura o codici identificativi, tali da rendere temporaneamente inintelligibili i dati sensibili e/o giudiziari anche a chi è autorizzato ad accedervi e da permettere l'identificazione degli interessati solo in caso di necessità	Obbligatorio per dati in perimetro d.lgs 196/2003		

Allegato 8: Clausole “Sicurezza e riservatezza” e “Designazione a responsabile esterno dei trattamenti di dati personali” per contratti e capitolati tecnici

Quando si scrive un contratto o un capitolato tecnico per l'acquisizione di prodotti o servizi IT è necessario inserire due clausole: una clausola relativa alla sicurezza e riservatezza e una clausola che preveda la conformità a quanto previsto dal D.Lgs. 196/2003 “Codice in materia di protezione dei dati personali”, in particolare designando il soggetto quale responsabile esterno dei trattamenti di dati personali richiesti per l'esecuzione del contratto. Il contenuto di tali clausole deve essere analogo ai seguenti fac simili:

A) Sicurezza e riservatezza

1. Il Fornitore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e comunque a conoscenza, anche tramite l'esecuzione del contratto, di non divulgarli in alcun modo e in qualsiasi forma, di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione del Contratto e di non farne oggetto di comunicazione o trasmissione senza l'espressa autorizzazione dell'Amministrazione.
2. L'obbligo di cui al precedente comma sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione del Contratto.
3. L'obbligo di cui ai commi 1 e 2 non concerne i dati che siano o divengano di pubblico dominio.
4. Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché di subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di segretezza di cui ai punti 1, 2 e 3 e risponde nei confronti della Committente per eventuali violazioni dell'obbligo di riservatezza commesse dai suddetti soggetti.
5. Il Fornitore non deve utilizzare servizi di cloud pubblici ove memorizzare i dati e le informazioni trattate nell'espletamento dell'incarico affidato, anche per garantirne la sicurezza e la riservatezza.
6. In caso di inosservanza degli obblighi descritti nei punti da 1 a 5, l'Amministrazione ha facoltà di dichiarare risolto di diritto il Contratto, fermo restando che il Fornitore sarà tenuto a risarcire tutti i danni che ne dovessero derivare.
7. Il Fornitore potrà citare i termini essenziali del Contratto nei casi in cui fosse condizione necessaria per la partecipazione del Fornitore stesso a gare e appalti, previa comunicazione alla Amministrazione delle modalità e dei contenuti di detta citazione.
8. Sarà possibile ogni operazione di auditing da parte della Amministrazione attinente le procedure adottate dal Contraente in materia di riservatezza e degli altri obblighi assunti dal presente contratto.
9. Il Fornitore non potrà conservare copia di dati e programmi della Amministrazione, né alcuna documentazione inerente ad essi dopo la scadenza del Contratto e dovrà, su richiesta, ritrasmetterli all'Amministrazione.
10. Tutte le attività che richiedono sviluppo di software nell'ambito dei servizi oggetto della fornitura dovranno, in particolare, soddisfare le indicazioni fornite nel Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna”, (determinazione n. 4137 del 2014 ed eventuali integrazioni o successive modificazioni) e nel “Disciplinare tecnico per utenti sull'utilizzo dei sistemi

informativi nella Giunta e nell'Assemblea Legislativa" (determinazione n. 14852/2011 ed eventuali integrazioni o successive modificazioni). I suddetti disciplinari sono scaricabili dalla sezione Privacy del sito istituzionale della Regione Emilia-Romagna (<http://www.regione.emilia-romagna.it>).

11. I dati tecnici relativi alle attività della Amministrazione, che dovranno essere portati a conoscenza del Fornitore al fine di realizzare i servizi oggetto della presente fornitura, non saranno considerati come riservati a meno di una espressa indicazione formulata per iscritto.
12. Il rispetto dei requisiti di sicurezza verrà verificato dalla Struttura all'atto della consegna da parte del Fornitore e sarà poi accertato dal Servizio Sistema Informativo-Informatico Regionale della Direzione Generale Organizzazione, Personale, Servizi Informativi e Telematica attraverso le verifiche preliminari al rilascio in produzione, prima della messa on line delle applicazioni o di loro modifiche sostanziali.

B) Designazione a responsabile esterno dei trattamenti di dati personali"

La persona fisica/giuridica/ente/associazione, ai sensi e per gli effetti dell'art. 29 del D.Lgs. n. 196/2003, e con le modalità definite nell'Appendice 5 della deliberazione di Giunta regionale n. 2416 del 2008, è designata responsabile esterno del/i trattamento/i dei dati personali, di cui la Regione Emilia-Romagna è titolare, che di seguito sono/è specificati/o:

- trattamento 1
- trattamento 2
-
- trattamento n

e di quei trattamenti che in futuro verranno affidati nell'ambito di questo stesso incarico per iscritto.

Si sottolinea che i compiti e le funzioni conseguenti a tale individuazione sono indicati nel D.Lgs. n. 196/2003, nell'Appendice 5 della deliberazione di Giunta regionale n. 2416 del 2008, Paragrafi 4 e 4.11. I compiti sono di seguito riportati:

- a) adempiere all'incarico attribuito adottando idonee e preventive misure di sicurezza, con particolare riferimento a quanto stabilito dal D.Lgs. n. 196/2003, dall'Allegato B del D.Lgs. n. 196/2003, dalla D.G.R. n. 1264/2005 e dai Disciplinari tecnici adottati e richiamati, in tutto o in parte, nello specifico incaricoⁱⁱ;
- b) predisporre, qualora l'incarico comprenda la raccolta di dati personali, l'informativa di cui all'art. 13 del D.Lgs. 196/2003 e verificare che siano adottate le modalità operative necessarie perché la stessa sia effettivamente portata a conoscenza degli interessati;
- c) dare direttamente riscontro oralmente, anche tramite propri incaricati, alle richieste verbali dell'interessato di cui ai commi 1 e 2 dell'art. 7 del D.Lgs. 196/2003, con le modalità individuate dal Discipinare tecnico in materia di esercizio del diritto di accesso dell'interessato ai propri dati personali (Determina n. 2650/2007);
- d) trasmettere, con la massima tempestività, le istanze dell'interessato per l'esercizio dei diritti di cui agli artt. 7 e ss. del D.Lgs. 196/2003 che necessitino di riscontro scritto al responsabile del trattamento di cui al Paragrafo 3 dell'Appendice 5 della deliberazione di Giunta regionale n. 2416 del 2008, per consentire allo stesso di dare riscontro all'interessato nei termini stabiliti dal D.Lgs. 196/2003; trasmettere tali istanze per conoscenza anche al Coordinatore del diritto di accesso dell'interessato ai propri dati personali, con le modalità individuate dal Discipinare

tecnico per l'esercizio dei diritti di accesso dell'interessato ai propri dati personali (Determina n. 2650/2007);

- e) fornire al responsabile del trattamento, di cui al Paragrafo 3 dell'Appendice 5 della deliberazione di Giunta regionale n. 2416 del 2008, la massima assistenza, necessaria per soddisfare tali richieste, nell'ambito dell'incarico affidatogli;
- f) individuare gli incaricati del trattamento dei dati personali e fornire agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata secondo quanto tale individuazione deve essere effettuata secondo quanto stabilito al Paragrafo 7 dell'Appendice 5 della deliberazione di Giunta regionale n. 2416 del 2008 e quindi, in particolare, le istruzioni devono quanto meno contenere l'espreso richiamo alla D.G.R. n. 1264/2005 e ai Disciplinari tecnici trasversali e/o di settore già adottati dal soggetto regionale competente;
- g) consentire al Titolare, dandogli piena collaborazione, verifiche periodiche, tramite i Responsabili dei trattamenti di cui al Paragrafo 3 dell'Appendice 5 della deliberazione di Giunta regionale n. 2416/2008 del o il Responsabile della sicurezza di cui al Paragrafo 5 dell'Appendice 5 della deliberazione di Giunta regionale n. 2416 del 2008;

SE L'INCARICO COMPORTA L'AFFIDAMENTO DI SERVIZI DI AMMINISTRAZIONE DI SISTEMA IN INSOURCING E' NECESSARIO INSERIRE IL COMPITO DI CUI ALLA LETTERA H)

- h) di fornire al Titolare, nel caso di servizi di amministrazione di sistema forniti in insourcing, l'elenco con gli estremi identificativi delle persone fisiche che espletano, nell'ambito dell'incarico affidato con il suindicato atto/contratto/buono economico, funzioni di amministratori di sistema unitamente all'attestazione delle conoscenze, dell'esperienza, della capacità e dell'affidabilità degli stessi soggetti, i quali devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Si sottolinea che tale valutazione è propedeutica alla formale designazione ad amministratore/i di sistema da parte del Titolare il quale, in attuazione di quanto prescritto alla lettera f) del paragrafo 2 del Provvedimento del 28/11/2008 del Garante per la protezione dei dati personali relativo agli amministratori di sistema, provvederà alla registrazione degli accessi logici ai sistemi da parte degli amministratori di sistema designati;

SE L'INCARICO COMPORTA L'AFFIDAMENTO DI SERVIZI DI AMMINISTRAZIONE DI SISTEMA IN OUTSOURCING E' NECESSARIO INSERIRE I COMPITI DI CUI ALLA LETTERA I) E J)

- i) di conservare, nel caso di servizi di amministrazione di sistema affidati in outsourcing, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;
- j) il Titolare attribuisce al Responsabile esterno del servizio di amministrazione di sistema affidato in outsourcing, limitatamente alle attività degli amministratori di sistema dello stesso dipendente, il compito di dare attuazione alla prescrizione di cui al punto 2 lettera e) "Verifica delle attività" del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";

SE L'INCARICO IMPONE L'ADOZIONE DI MISURE MINIME DI SICUREZZA E' NECESSARIO INSERIRE IL COMPITO DI CUI ALLA LETTERA K)

- k) attestare, qualora l'incarico affidato ricomprenda l'adozione di misure minime di sicurezza, la conformità degli interventi alle disposizioni di cui alla misura 25 dell'Allegato B del D.Lgs. n. 196/2003 e trasmettere tale attestazione al Responsabile di cui dell'Appendice 5 della deliberazione di Giunta regionale n. 2416 del 2008 e al Responsabile della sicurezza di cui al Paragrafo 5 dell'Appendice 5 della deliberazione di Giunta regionale n. 2416 del 2008;³

Oltre ai suddetti compiti, considerata la natura specifica dell'incarico, si richiede anche di:

- l)
- (indicare eventuali integrazioni che derivano dalla natura specifica dell'incarico)

Relativamente al compito di cui alla lettera g), le relative verifiche consistono:

- A) nell'invio di specifici report a cadenza temporale e/o a richiesta (specificare cadenza temporale: ad esempio semestrale), in cui il responsabile esterno deve fornire le seguenti informazioni (di seguito riportate a titolo esemplificativo e da adattare allo specifico incarico):
- l'attestazione di aver adottato tutte le misure minime di sicurezza di cui agli artt. 33 e ss. e all'Allegato B) del Codice per la protezione dei dati personali
 - l'attestazione di aver implementato tutte le misure idonee di cui all'art. 31 del Codice, ai sensi e per gli effetti del combinato disposto dell'15 del Codice per la protezione dei dati personali e dell'art. 2050 c.c.adozione degli atti di individuazione degli incaricati, specificando in particolare le istruzioni fornite agli incaricati stessi;
 - predisposizione dell'informativa (nel caso in cui il trattamento consista in una raccolta di dati personali), con specifica delle modalità operative con cui la stessa è stata portata a conoscenza degli interessati (ad esempio: consegna di copia dell'informativa e raccolta della firma per presa visione);

SE L'INCARICO COMPORTA L'AFFIDAMENTO DI SERVIZI DI AMMINISTRAZIONE DI SISTEMA IN OUTSOURCING E TRA I COMPITI SONO STATI INDICATI QUELLI DI CUI ALLE LETTERE i) E j) POSSONO ESSERE RICHIESTI I SEGUENTI REPORT

- di aver effettuato la designazione ad amministratori di sistema dei soggetti preposti a tali funzioni nell'ambito dei servizi di amministrazione di sistema forniti in outsourcing e di aver previamente attestato le conoscenze, l'esperienza, la capacità e l'affidabilità degli stessi soggetti, i quali devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
- di aver adempiuto alla prescrizione di cui al punto 2 lettera e) "Verifica delle attività" del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"
e/o

- B) in verifiche in loco, comunicate con un preavviso di almeno 15 giorni.

Tutti i testi dei principali riferimenti normativi relativi alle Deliberazioni di Giunta Regionale sono pubblicati all'indirizzo <http://www.regione.emilia-romagna.it/privacy.htm>.

I Disciplinari tecnici menzionati sono allegati al presente contratto/convenzione/verbale di aggiudicazione/provvedimento di nomina o pubblicati all'indirizzo <http://www.regione.emilia-romagna.it/privacy.htm>.

ⁱ La designazione deve essere comunicata al Coordinatore del diritto di accesso dell'interessato ai propri dati personali

"I compiti e le funzioni elencati, nel caso di effettive e motivate esigenze derivanti dalla particolarità dell'incarico affidato, possono essere in parte adattati alla natura dell'incarico stesso. Gli adattamenti non devono peraltro comportare una diminuzione di responsabilità, ma soltanto, ad esempio, un maggior dettaglio ovvero una diversità terminologica nell'elenco dei compiti e delle funzioni.

ⁱⁱ Per quanto riguarda i Disciplinari tecnici, occorre riportare solo i Disciplinari tecnici che riguardano lo specifico incarico. Ad esempio, il Disciplinare tecnico sulla sicurezza delle applicazioni deve essere richiamato nel caso in cui si affidi un incarico di servizio di sviluppo di applicazioni. I riferimenti ai Disciplinari tecnici sono reperibili su Internos, sezione "Privacy", voce "Normativa".

³ Questo compito deve essere inserito soltanto nei casi in cui l'incarico affidato ricomprenda l'adozione di misure minime di sicurezza. Successivamente deve essere verificato che l'attestazione stessa sia stata inviata anche al Responsabile della Sicurezza e, in caso negativo, si deve sollecitarne l'invio.

Allegato 9: Specifiche tecniche per l'utilizzo del sistema di autenticazione centralizzata

1	Considerazioni generali	2
2	Gestione degli utenti di un'applicazione con il sistema di Identity Management (IdM)	2
3	Accesso alle web application.....	3
3.1	Requisiti di progettazione delle interfacce	3
3.2	Formato parametri	3
3.3	Vincoli	3
3.3.1	Identificazione e Autenticazione dell'utente.....	3
3.3.2	Autorizzazione dell'utente.....	4
3.3.3	Uso di Cookie.....	4
3.3.4	Convenzioni sui nomi dei domini	4
3.3.5	Convenzioni sui nomi delle web application	4
3.3.6	Regole d'instradamento del Reverse Proxy	4
3.3.7	Accessibilità dell'applicazione tramite proxy.....	5
3.3.8	Sicurezza	6
3.3.9	Gestione del logout applicativo.....	6
3.3.10	Definizione delle regole di autorizzazione	6
4	Modulo di raccolta informazioni	7
5	Esempi di utilizzo degli attributi dell'http Header	7

1 Considerazioni generali

Questo documento ha lo scopo di descrivere l'integrazione delle applicazioni ospitate sulle infrastrutture della Regione Emilia-Romagna con il sistema centralizzato di Identity & Access management (IAM), al fine di implementare l'autenticazione.

Il sistema di IAM è finalizzato alla gestione razionale, scalabile ed omogenea delle utenze del Sistema Informativo della Regione ottemperando al tempo stesso alle normative ed ai requisiti di legge in tema di sicurezza informatica e di protezione dei dati personali.

Il sistema di IAM è composto dalle seguenti componenti:

- un servizio di Directory per la gestione centralizzata delle utenze interne ed esterne, sul quale poggiano le funzioni di "profilatura" e "autenticazione" di sistemi e applicazioni integrati nello IAM;
- una soluzione di Identity Management, che, interfacciandosi a diversi repository utente, consente la gestione dell'intero ciclo di vita delle identità su specifici sistemi e applicazioni, la sincronizzazione delle password degli utenti e la delega ai referenti alla gestione delle loro utenze; consente inoltre l'automatizzazione del processo di provisioning degli account, integrato con i processi organizzativi mediante l'utilizzo di workflow;
- una soluzione di Access Management che permette l'accesso in Single Sign On alle applicazioni web integrate, liberando le applicazioni stesse dalla gestione dell'autenticazione.

2 Gestione degli utenti di un'applicazione con il sistema di Identity Management (IdM)

L'applicazione deve delegare al sistema di Identity la gestione degli utenti. L'identity ha bisogno di oggetti chiamati "connettori" che gli permettano di interagire con il repository degli utenti utilizzato dall'applicazione (es. una tabella utenti su un db). In linea generale esistono due tipologie di connettori:

- connettori standard,
- connettori custom.

I primi sono connettori già implementati dal produttore. In questo caso non è necessaria alcuna fase di sviluppo e si può passare alla fase di integrazione. Per informazioni circa i connettori standard si può richiedere ad idmadmin@regione.emilia-romagna.it.

Nel secondo caso, è invece necessario sviluppare dei metodi **network-enable** (API, Store Procedures, Web Services) che devono essere esposti per l'integrazione con il sistema di IdM.

Tali metodi sono normalmente un sottoinsieme dei seguenti, in funzione delle necessità:

- `createUser`, crea un account sul target
- `deleteUser`, cancella un account sul target
- `getUser`, restituisce la vista di un utente sul target
- `getAccountIterator`, restituisce un iteratore sull'accountID degli utenti sul target
- `update`, aggiorna i dati di un utente sul target (compresa la password)
- `enable`, abilita l'utente sul target
- `disable`, disabilita l'utente sul target
- `listProfile`, effettua la lista di tutti i profili del target
- `test`, testa il funzionamento del servizio

Per ognuno dei metodi precedenti dovranno inoltre essere definiti i parametri di input e di output in base al target da integrare (alcuni target potranno avere dei parametri differenti).

Particolare attenzione va al campo password, nel caso in cui nel target che si vuole integrare essa sia gestita.

Qualora infatti si debba gestire la password sul target, deve essere indicato al gruppo di IdM l'algoritmo di cifratura utilizzato.

3 Accesso alle web application

Per poter accedere ad una Web Application protetta da un sistema di Web SSO, l'utente deve prima aver effettuato il Logon al sistema di autenticazione. Effettuato il Logon Primario, l'utente può accedere alle Web Application esposte.

Ad ogni richiesta di accesso vengono ripetuti i seguenti passi:

1. la richiesta viene intercettata dal Reverse Proxy
2. l'Agent del Reverse Proxy verifica la presenza di una sessione autenticata per l'utente. Per il mantenimento della sessione viene utilizzato un cookie volatile sul client. Nel caso non esista una sessione associata alla richiesta, l'utente viene diretto verso il modulo di autenticazione del sistema di Web SSO centralizzato
3. il sistema di Web SSO autentica l'utente e restituisce le informazioni all'Agent che a sua volta trasmette le informazioni necessarie alla web application dell'aderente utilizzando l'header http.

3.1 Requisiti di progettazione delle interfacce

Il passaggio dei parametri tra il reverse proxy e l'applicazione avviene sfruttando i meccanismi standard del Web e cioè gli header del protocollo HTTP, quindi la Web Application deve essere in grado di gestire gli header HTTP.

Nel caso in cui l'applicazione voglia filtrare ulteriormente gli accessi può prelevare gli attributi dell'utente dall'header ed effettuare la profilazione applicativa.

3.2 Formato parametri

I parametri passati nell'header HTTP alla web application esposta servono ad identificare ed a caratterizzare l'originatore della richiesta.

Il parametro necessariamente presente nell'header HTTP dovrà essere il seguente:

Parametro	Significato
USERNAME	Identificativo utente (identifica l'originatore della richiesta).
DOMAIN	Identificativo dominio (RERSDM – EXTRARER)
FIRSTNAME	Identificativo del Nome dell'utente
LASTNAME	Identificativo del Cognome dell'utente
MATRICOLA	Identificativo Matricola dell'utente (solo in caso di utenti regionali)

Potranno essere aggiunti ulteriori parametri da passare nell'header. Questi parametri sono prelevati dagli attributi dell'utente.

I parametri elencati saranno presenti nell'header HTTP di ogni richiesta. La modalità di accesso alle variabili dell'header sono legate al linguaggio utilizzato per la creazione e la gestione delle pagine web. Al termine del presente documento sono riportati esempi di accesso a queste variabili in JSP, PERL, ASP.NET, ASP.

3.3 Vincoli

Sono riportati di seguito i vincoli a cui le Web Application devono attenersi per poter essere protette dal sistema di Web SSO.

3.3.1 Identificazione e Autenticazione dell'utente

La web application esposta non deve richiedere il login agli utenti che accedono, in quanto il processo di identificazione e autenticazione viene già effettuato nella fase di Logon Primario che l'utente effettua sul sistema di Web SSO. In particolare, l'applicazione non deve richiedere l'immissione esplicita da

parte dell'utente di un username e di una password, ma può utilizzare le informazioni di identificazione dell'utente contenute nell'header HTTP di ogni richiesta

3.3.2 Autorizzazione dell'utente

Il processo di autorizzazione all'accesso da parte dell'utente alla web application esposta è effettuato dal Reverse Proxy, che abilita o impedisce l'accesso a singole Applicazioni in base a policy prestabilite. E' facoltà dell'applicazione di estendere il processo di autorizzazione svolto dal Reverse-Proxy, utilizzando le informazioni contenute nell'header HTTP di ogni richiesta per realizzare nuove regole di autorizzazione.

3.3.3 Uso di Cookie

Il meccanismo di Logon e le verifiche effettuate dal Reverse Proxy si basano sullo scambio di *cookie* con la Postazione di Lavoro dell'utente che necessariamente deve permettere l'utilizzo di *cookie*.

3.3.4 Convenzioni sui nomi dei domini

Una web application esposta dalla RER potrà essere accessibile, sia da Internet che dalla rete interna, mediante una URL così strutturata:

`https://applicazioni.regione.emilia-romagna.it/<percorso-applicazione>/`

dove *<percorso-applicazione>* è il *path* (al limite costituito da un singolo nome) scelto per identificare la web application (è ammesso il passaggio di parametri nella URL).

3.3.5 Convenzioni sui nomi delle web application

Qualora un servizio esponga più di una web application, gli URL corrispondenti si differenziano solo relativamente alla componente *<percorso applicazione>*.

Esempio:

`https://<dominio>/<percorso applicazione -1>/`

`https://<dominio>/<percorso applicazione -2>/`

`https://<dominio>/<percorso applicazione -3>/`

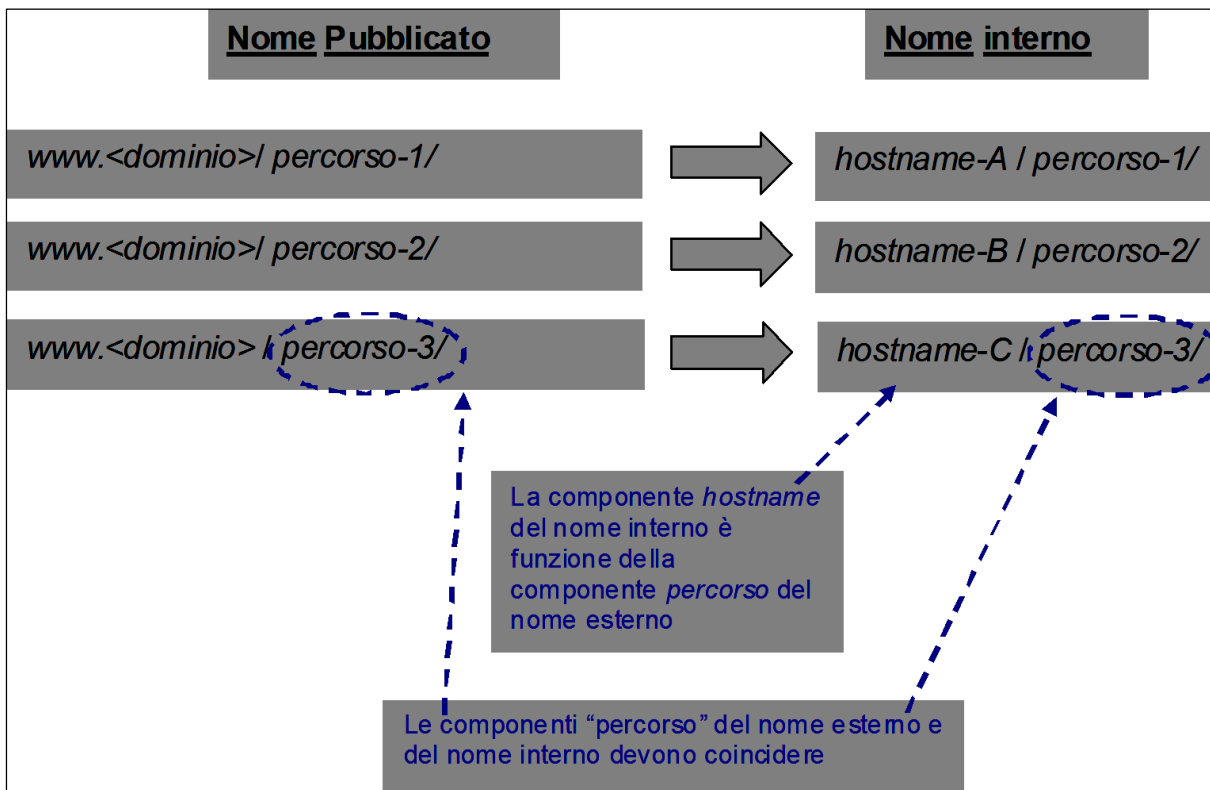
3.3.6 Regole d'instradamento del Reverse Proxy

La convenzione sui nomi degli URL si riferisce all'esposizione delle web application, ovvero al modo in cui tali applicazioni sono esposte tramite Reverse Proxy e non implica che la medesima convenzione debba necessariamente essere adottata internamente all'applicativo.

Internamente all'applicativo, le web application possono risiedere su uno o più host. La corrispondenza tra il "nome esterno" e il "nome interno" dell'applicazione viene effettuata dal Reverse Proxy tramite le *regole di instradamento*. Tali regole consentono di collocare le proprie web application sui server della rete interna, svincolandosi dall'*hostname* con cui sono visibili.

Nell'instradamento, il path dell'applicazione (cioè la porzione dell'URL che viene dopo l'*hostname*) del "nome esterno" deve coincidere con il path del "nome interno".

La figura seguente rappresenta le regole suddette:



E' ammesso il passaggio di parametri nell'URL, se previsto dalla web application, mentre non è ammesso utilizzare i parametri per identificare la web application esposta.

Esempio di utilizzo di URL non è ammesso:

https:// www.<dominio>/entrypoint?applicazione=applicazione1

3.3.7 Accessibilità dell'applicazione tramite proxy

Si descrivono di seguito i vincoli che la web application dell'Aderente deve rispettare per poter essere esposta attraverso il Reverse Proxy (requisiti di *proxability*).

La web application da esporre non deve contenere riferimenti assoluti alle proprie risorse, ma solo puntamenti relativi.

In altri termini le eventuali risorse referenziate all'interno dell'applicazione (quali., ad esempio, immagini o link ad altre pagine) devono essere indirizzate tramite **URL relativi**, ovvero URL in cui viene esplicitata solamente la componente *path* senza le componenti *protocollo* ed *hostname*. Oltre agli URL anche i **PATH devono essere relativi**, ovvero non devono iniziare con il carattere "I".

Ad esempio:

URL ASSOLUTI (NON UTILIZZABILI)	URL RELATIVI (DA UTILIZZARE)
<code>http(s)://hostname/logo.gif</code>	<code>logo.gif</code>
<code>http(s)://hostname/subdir1/index.html</code>	<code>subdir1/index.html</code>
	NOTA : <u>non</u> è possibile utilizzare URL relativi del tipo <code>/subdir1/index.html</code> , i quali, pur essendo URL relativi (non vengono infatti indicati protocollo ed hostname), sono comunque <u>PATH</u> assoluti.

Inoltre, ogni singola Web Application deve prevedere un unico punto di ingresso da cui si diramano i diversi sottoservizi.

Non sono quindi consentiti collegamenti a sottoservizi non appartenenti all'albero che ha come radice la URL di ingresso della Web Application: ad esempio, supponendo che l'URL di "ingresso" della Web Application sia `http(s)://hostnameX/directoryY`, non è consentito il collegamento a pagine che non risiedano sotto il path *directoryY* quali `http(s)://hostnameX/directoryZ/pageJ.jsp` (sempre che

l'applicazione che ha come "ingresso" della WebApplication l'URL [http\(s\)://hostnameX/directoryZ](http(s)://hostnameX/directoryZ) non sia stata esposta a sua volta).

3.3.8 Sicurezza

Ogni applicazione dovrà accettare solo le richieste pervenute dal reverse proxy. Il controllo dovrà essere effettuato mediante un meccanismo di autenticazione con certificato client. Il certificato pubblico del reverse proxy verrà installato sui server sulle quali è installata l'applicazione e l'applicazione, l'application server o il web server dovranno essere configurati in modo da concedere l'accesso all'applicazione solo se il certificato client viene riconosciuto essere quello del reverse proxy. Nel caso questo non fosse possibile occorrerà verificare, a livello applicativo e, ove possibile, a livello sistemistico (con un firewall o sul web server) che le richieste provengano dall'ip del reverse proxy. L'applicazione dovrà riconoscere l'utente, tramite i parametri passati nell'http Header, solo nel caso la richiesta gli venga inoltrata dal *reverse proxy*, in tutti gli altri casi l'applicazione non dovrà permettere l'accesso all'utente.

3.3.9 Gestione del logout applicativo

Nel caso in cui l'applicazione abbia creato una sessione al momento dell'autenticazione dell'utente, il logout dall'applicazione deve invalidare la sessione applicativa.

In ogni caso l'utente deve essere reindirizzato alla lista delle applicazioni al seguente link relativo:

- /index.php

3.3.10 Definizione delle regole di autorizzazione

La regola implicita di autorizzazione degli accessi a una web application esposta sul dominio RER prevede la negazione di ogni accesso. Pertanto, ogni abilitazione deve essere espressamente dichiarata al sottosistema di controllo accessi tramite la formulazione di opportune regole.

Ogni singola regola prevede la specifica di:

1. il nome della risorsa oggetto della regola di abilitazione, dove per 'risorsa' si intende una web application o una sua porzione (sottoalbero o singola pagina);
2. l'elenco dei gruppi applicativi (nell'ambito di quelli definiti dalla RER) abilitati ad accedere alla risorsa di cui al punto precedente;
3. le operazioni ammesse (get e post).

Il nome della risorsa (*Resource Name*) è espresso mediante una *regular expression* che può contenere *wildcards*.

Esempi di nomi risorsa:

<code>https:// www.<dominio>/applicazione1/*</code>	Tutta l'applicazione: 'applicazione1'
<code>https://www.<dominio>/applicazione1/home.htm</code>	La sola pagina 'home.htm' dell'applicazione 'applicazione1'
<code>https://www.<dominio>/applicazione1/consult/*</code>	Tutte le risorse all'interno del sottoalbero 'consult' dell'applicazione 'applicazione1'

Ogni volta che un utente accede ad una *web application* esposta sul dominio RER tramite il *Reverse Proxy*, le URL delle pagine chiamate vengono confrontate con queste *regular expression*. In caso di corrispondenza, viene consentito l'accesso solo se il gruppo dell'originatore della richiesta è stato abilitato per la risorsa identificata e se l'operazione (get o post) è ammessa.

Nel caso vi siano applicazioni con redirectione implicita su una pagina di default è necessario aggiungere una nuova regola dedicata. (ad esempio `https:// www.<dominio>/applicazione2`).

4 Modulo di raccolta informazioni

Concordemente con quanto espresso sopra, al fine di impostare le configurazioni del *Reverse Proxy*, le regole di autorizzazione, ecc., è necessario per il sottosistema di *Access Management* conosca un insieme di informazioni che dovranno essere fornite dai responsabili applicativi, che verranno raccolte mediante il modulo riportato di seguito.

Sulla base dei dati in esso raccolti verranno configurati il *reverse proxy* (interno ed esterno) e le regole di autorizzazione centralizzate del sistema di *Access Management*.

DATO	VALORE
Nome applicativo	
Referente tecnico	
Path relativo	
Path assoluto	
Note	

Indicazioni per la compilazione:

- **Nome applicativo:** nome dell'applicativo per esteso (esempio: Vetrina della sostenibilità)
- **Referente tecnico:** riferimenti della persona indicata come referente tecnico per l'integrazione delle web application (esempio: Marco Rossi, telefono 051-999999, mail xxx@xx.xx)
- **Path relativo:** nome breve dell'applicativo, utilizzato per formare l'URL di accesso alla web application sul portale delle applicazioni¹ (esempio: VetrinaSostenibilita)
- **Path assoluto:** URL completo della web application da mappare sull'Access Management (esempio: <https://amservizi.regione.emilia-romagna.it/VetrinaSostenibilita>).
- **Note:** eventuali note

5 Esempi di utilizzo degli attributi dell'http Header

Esempio di JSP:

```
<html>
<head><title>Recupero Username e Dominio </title></head>
<body>
<%
String userid = request.getHeader("username");
String gruppo = request.getHeader("domain");

out.println("<BR> UserID -> " + username);
out.println("<BR> Dominio -> " + domain);

%>
```

¹ <https://applicazioni.regione.emilia-romagna.it>

```
</body>
</html>
```

Esempio di PERL:

```
#!/usr/bin/env perl
#
# Programma di test
#

print "Content-type: text/html\n\n";
print "<html><head><title>Recupero Username e Dominio</title></head>\n";

print "<table border=1 bordercolor=black>";
foreach $e (%ENV)
{
    if ($e eq "HTTP_USERNAME" || $e eq "HTTP_DOMAIN")
    {
        print "<tr>";
        print "<td>$e </td><td>$ENV{$e}</td>";
        print "</tr>";
    }
}
print "</table></body></html>\n";
```

Esempio di ASP.NET:

```
string username = string.Format(@"{0}\{1}",
    Request.Headers["Domain"],
    Request.Headers["Username"]
);

Response.Write(username);
```

Esempio di ASP:

```
username = Request.ServerVariables("HTTP_Domain") & "\" &
    Request.ServerVariables("HTTP_Username")

Response.Write username
```

Allegato 10: Repository dei sorgenti e tracking

1	Introduzione	1
2	Redmine, SVN e GIT	1
2.1	Utenti e Ruoli	1
2.2	Progetti	2
2.3	Gestione Subversion e Git	3
2.4	Ulteriori informazioni.....	3

1 Introduzione

Scopo di questo documento è quello di illustrare il sistema di repository e tracking adottato dalla Regione Emilia-Romagna.

2 Redmine, SVN e GIT

L'utilizzo di Redmine permette di semplificare la gestione quotidiana di un progetto software unificando in un'unica interfaccia diversi strumenti: sistema di versioning, wiki, forum, bug/ticket tracking, calendario, archivio documentale.

Un project manager ha la facoltà di controllare ogni aspetto del progetto, gli utenti assegnati, i ruoli, i permessi di accesso.

La stretta integrazione con sistemi di versioning come subversion e git ha il vantaggio di automatizzare la procedura di creazione e gestione dei repository (ne viene creato uno per ogni progetto) permettendo una corretta separazione e un utilizzo ottimale del sistema, separando la manutenzione del servizio dalla sua gestione e pratica quotidiana.

E' opportuno etichettare i sorgenti modificati in ogni rilascio in modo rendere possibile la ricomposizione dei contenuti completi di ogni rilascio. In tal modo si consente l'applicazione di patch ad una determinata versione del progetto e si riduce la probabilità di regressioni.

2.1 Utenti e Ruoli

In Redmine ad ogni utente viene associato un account le cui azioni sono fortemente dipendenti dal ruolo assegnato.

Un Ruolo è un oggetto nel quale sono specificati i privilegi di accesso per ogni aspetto o modulo di un progetto.

Ad ogni utente possono essere assegnati uno o più ruoli per ogni progetto: ad esempio uno stesso account può avere privilegi di amministratore di un determinato progetto e sviluppatore in un altro.

Quando si rende necessario assegnare gli stessi privilegi a più utenti è possibile definire un gruppo e assegnare i diritti al gruppo. I membri del gruppo acquisiranno in automatico gli stessi diritti: ogni ruolo associato ad un gruppo viene in automatico propagato a tutti gli utenti facenti parte di quel gruppo.

In redmine esistono i seguenti ruoli predefiniti:

- Gestore

- Sviluppatore
- Segnalatore
- Non member
- Anonymous

Gestore: è il ruolo che ha la possibilità di gestire e controllare ogni aspetto di un progetto e dei relativi sottoprogetti.

Sviluppatore: accesso in lettura e scrittura al repository, può creare e modificare le attività, ha accesso in lettura al wiki, calendario, all'archivio file ed ai documenti ma non può modificare le impostazioni del progetto.

Segnalatore: ha accesso in sola lettura al progetto, può segnalare bug.

Non member: ha accesso in lettura ad alcune parti di un progetto **pubblico**, può segnalare bug.

Anonymous: utente non registrato, con permessi analoghi al "non member".

Per utilizzare Redmine e/o se si necessita di creare un nuovo ruolo o un nuovo gruppo, la richiesta va inoltrata tramite il Catalogo dei servizi informatici linkato sul sito Internos nella sezione "[Sapere e fare/funziona così/software computer e applicazioni/Numeri e link utili per utenti della Giunta](#)" o raggiungibile direttamente all'indirizzo <https://rt.regione.emilia-romagna.it/rt/> specificando il nome del nuovo ruolo, il ruolo di base dal quale copiare i permessi (es. Sviluppatore), ed i permessi da modificare (da aggiungere o togliere).

2.2 Progetti

Un progetto in Redmine è un contenitore di informazioni, quali segnalazioni, bug, pagine di wiki, documenti ed un repository (subversion o git nel nostro specifico caso). Un progetto non può essere suddiviso in unità, ma può contenere sottoprogetti. È possibile, quindi, creare uno schema ad albero in cui un progetto principale faccia da contenitore a vari sottoprogetti, pur mantenendo separata ogni parte.

I moduli, tutti abilitati di default, visibili in un progetto sono i seguenti:

- Segnalazioni
- Diagramma di Gantt
- Calendario
- Novità
- Documenti
- Wiki
- Forum
- Files
- Repository
- Impostazioni (solo per chi ne ha i privilegi di accesso.)

Ognuno di questi moduli è configurabile per essere abilitato o disabilitato a livello di progetto, o a livello di Ruolo. Di default ogni modulo, se abilitato, è accessibile in lettura ad ogni utente. Per una lista completa dei permessi vedere le tabelle 4-1 e 4-2.

Segnalazioni: pagina di controllo delle segnalazioni, visualizzazione e modifica del loro stato.

Calendario: mostra in forma di calendario la timeline e le informazioni delle segnalazioni.

Novità: pagina di controllo dove visualizzare, modificare o inserire informazioni legate ad un progetto e visualizzate prima pagina.

Documenti: In Redmine esiste la possibilità di condividere dei files di documentazione, all'esterno del repository associato al progetto.

Wiki: Modulo per la creazione di documentazione stile wiki.

Forum: Modulo per la gestione di forum legati al progetto.

Files: Pagina per la condivisione di files generici.

Repository: browser del repository associato al progetto.

Impostazioni: Pagina per la gestione e configurazione di ogni aspetto del progetto (moduli, membri, versioni ecc.)

2.3 Gestione Subversion e Git

Ad ogni progetto è associabile un repository subversion o git. Di default alla creazione di un nuovo progetto viene generato in automatico un repository vuoto con lo stesso nome del progetto. Se si necessita di importare un repository già esistente bisogna inoltrare la richiesta tramite il Catalogo dei servizi informatici linkato sul sito Internos nella sezione "[Sapere e fare/funziona così/software computer e applicazioni/Numeri e link utili per utenti della Giunta](#)" o raggiungibile direttamente all'indirizzo <https://rt.regione.emilia-romagna.it/rt/>

Non è previsto l'utilizzo di controllo degli accessi ai sottorami del repository, i privilegi di lettura o scrittura vengono impostati a livello globale del progetto, in base al ruolo assegnato all'utente. Come specificato in precedenza, per separare sezioni di un progetto è necessario creare un sottoprogetto ed assegnare ad esso la sezione desiderata del repository originale.

L'url di accesso ad un repository è il seguente:

<https://rersvn.ente.regione.emr.it/svn/IdDelProgetto> (repository subversion)

<https://rersvn.ente.regione.emr.it/git/IdDelProgetto> (repository git)

I permessi di default sono così specificati:

- Gestori: Lettura e scrittura
- Sviluppatori: Lettura e scrittura
- Segnalatori: sola lettura

2.4 Ulteriori informazioni

Indirizzo server Redmine RER: <https://rersvn.ente.regione.emr.it/redmine>

Alcuni collegamenti alla guida di Redmine (in inglese):

Progetti: <http://www.redmine.org/wiki/redmine/RedmineProjects>

Gruppi: <http://www.redmine.org/wiki/redmine/RedmineGroups>

Ruoli e privilegi: <http://www.redmine.org/wiki/redmine/RedmineRoles>

Segnalazioni: <http://www.redmine.org/wiki/redmine/RedmineIssueTrackingSetup>

Custom Fields: <http://www.redmine.org/wiki/redmine/RedmineCustomFields>

Enumerations: <http://www.redmine.org/wiki/redmine/RedmineEnumerations>

Accounts: <http://www.redmine.org/wiki/redmine/RedmineAccounts>

Login: <http://www.redmine.org/wiki/redmine/RedmineLogin>

Registrazione utente: <http://www.redmine.org/wiki/redmine/RedmineRegister>

Panoramica progetti: <http://www.redmine.org/wiki/redmine/RedmineProjectOverview>

Attività progetti: <http://www.redmine.org/wiki/redmine/RedmineProjectActivity>

Segnalazioni: <http://www.redmine.org/wiki/redmine/RedmineIssues>

Lista segnalazioni: <http://www.redmine.org/wiki/redmine/RedmineIssueList>

Change log: <http://www.redmine.org/wiki/redmine/RedmineIssueChangelog>

Panoramica segnalazioni: <http://www.redmine.org/wiki/redmine/RedmineIssueSummary>

Roadmap: <http://www.redmine.org/wiki/redmine/RedmineRoadmap>

Panoramica versioni: <http://www.redmine.org/wiki/redmine/RedmineVersion>

Calendario: <http://www.redmine.org/wiki/redmine/RedmineCalendar>

Grafico Gantt: <http://www.redmine.org/wiki/redmine/RedmineGantt>

Time tracking: <http://www.redmine.org/wiki/redmine/RedmineTimeTracking>

Dettagli timelog: <http://www.redmine.org/wiki/redmine/RedmineTimelogDetails>

Rapporto sul timelog: <http://www.redmine.org/wiki/redmine/RedmineTimelogReport>

Novità: <http://www.redmine.org/wiki/redmine/RedmineNews>

Documenti: <http://www.redmine.org/wiki/redmine/RedmineDocuments>

Files: <http://www.redmine.org/wiki/redmine/RedmineFiles>

Forum: <http://www.redmine.org/wiki/redmine/RedmineForums>

Wiki: <http://www.redmine.org/wiki/redmine/RedmineWikis>

Repository: <http://www.redmine.org/wiki/redmine/RedmineRepository>

Statistiche del repository:
<http://www.redmine.org/wiki/redmine/RedmineRepositoryStatistics>

Impostazioni del progetto: <http://www.redmine.org/wiki/redmine/RedmineProjectSettings>

Formattazione del testo: <http://www.redmine.org/wiki/redmine/RedmineTextFormatting>

Allegato 11: Linee guida sulla grafica condivisa dei siti web

1	Introduzione	1
2	Percorsi e files	1
3	Esempio di utilizzo di templates condivisi.....	4
3.1	Classic ASP	5
3.2	ASP.Net.....	7
3.3	Microsoft MVC	8
4	Stili ed accorgimenti da utilizzare	10
4.1	Titoli e bande orizzontali	10
4.2	Briciole di pane	11
4.3	Menù	12
4.4	Form.....	13
4.5	Risultati di una ricerca e tabelle.....	14
4.6	Dettaglio e elenchi con molte colonne (non intabellati)	14
4.7	Altre possibili forme di un elenco di risultati e dettagli.....	15

1 Introduzione

Questo documento ha lo scopo di dare delle indicazioni tecniche su come le applicazioni web possono condividere la grafica dei siti web Plone realizzati dal Servizio SIIR , infatti per agevolare la navigazione degli utenti all'interno dei siti web regionali e relative applicazioni, è opportuno che le applicazioni destinate alla consultazione web abbiano un aspetto graficamente coerente con quello dei siti da cui vengono consultate. A tale scopo, per ogni sito Plone realizzato dal Servizio SIIR viene predisposto un insieme di files che ne rappresentano la cosiddetta "grafica condivisa". Se si includono dinamicamente questi template, le applicazioni saranno sempre aggiornate anche a fronte di modifiche nella linea grafica dei portali web.

2 Percorsi e files

Tutti i portali condividono con ER i fogli di stile, li ereditano e li modificano. Alcuni stili sono stati aggiunti per sistemare i difetti di IE, anche questi stili andranno importati in opportuni commenti condizionali dentro ai template.

I files si trovano sia in **test**

<http://www.servizitest.regione.emilia-romagna.it/includes/TemplatesER>

che **produzione**, in cartelle condivise.

<http://www.servizi.regione.emilia-romagna.it/includes/TemplatesER>

Sono presenti 3 file asp, di cui uno solo è importante:

- **template_ermes.asp**: il template usato dalle applicazioni asp, utile base per comprendere l'uso dei vari file di testo
- **default.asp**: pagina .asp di esempio e **ErroreSistema.asp** pagina .asp generica di errore sono presenti solo per usi di servizio quali verifica del funzionamento dei collegamenti, ecc.

In particolare sono presenti dei file txt, unico formato importabile in tutti i linguaggi:

- **aperturaBriciole.txt**
- **chiusuraBriciole.txt**
- **testata.txt**
che contiene la parte superiore dentro alla tabella di impaginazione del <body> il motore ed i link alle 3 pagine principali (primo piano, entra in regione, temi)
- **footer.txt**
che contiene la parte inferiore dentro alla tabella di impaginazione del <body> con i link alle pagine generiche (credits, accessibilità, ecc. ecc.)
- **stylesheets.txt**
che richiama il foglio di stile del portale e fogli di stile per IE **[DIVERSO TRA TEST E PRODUZIONE]**
- **stylesheetshtml.txt**
uguale al precedente ma **da usare quando si generano pagine in HTML** e non XHTML
- **styles.css**
il foglio di stile condiviso dalle applicazioni, che contiene alcuni aggiustamenti per le applicazioni. Se incorpora immagini, l'url va richiamato in https per evitare i messaggi di IE

I **files evidenziati** contengono i collegamenti alle pagine e/o immagini del sito. Di norma puntano alla produzione, per evitare 2 versioni tra test e produzione, tranne nel caso di stylesheets.txt che punta al css di sviluppo.

Questa struttura viene replicata anche per i singoli portali.

All'interno della cartella dei template esiste una cartella per ciascun portale:

- ambiente
- autonomie
- imprese
- mobilità
- sociale, ecc.

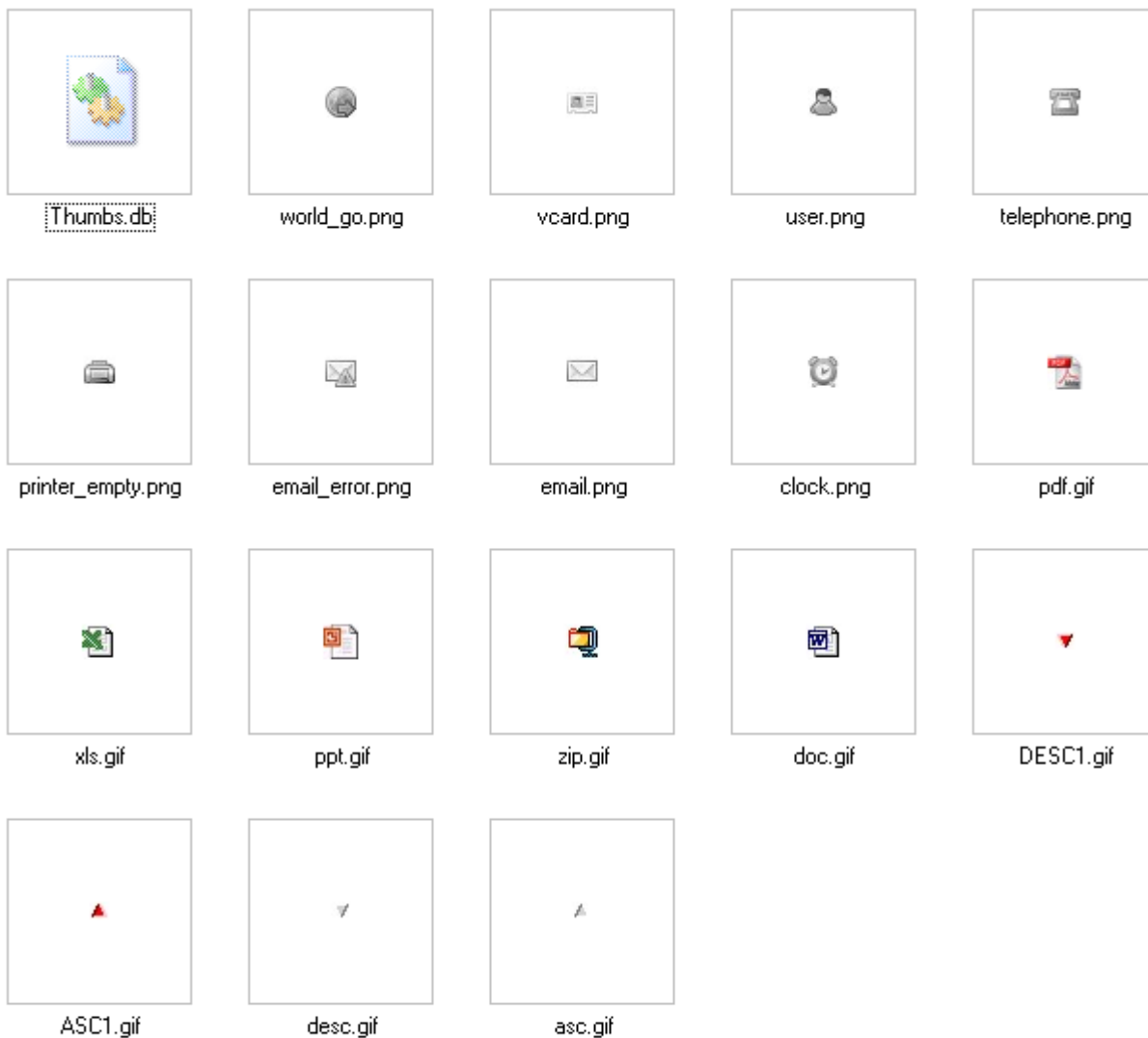
Quindi se l'applicazione deve avere la grafica di ER si useranno i files delle cartella **TemplatesER**.

Negli altri casi vanno usati i file specifici del portale di cui l'applicazione deve ereditare la grafica.

Richiedere al Servizio SIIR il percorso dei template da utilizzare scrivendo una mail alla casella itgovernance@regione.emilia-romagna.it.

Nel caso di nuovo portale è necessario richiedere al SSIIR la creazione dei nuovi templates di riferimento.

Esiste anche una generica cartella di immagini, per icone: **img**



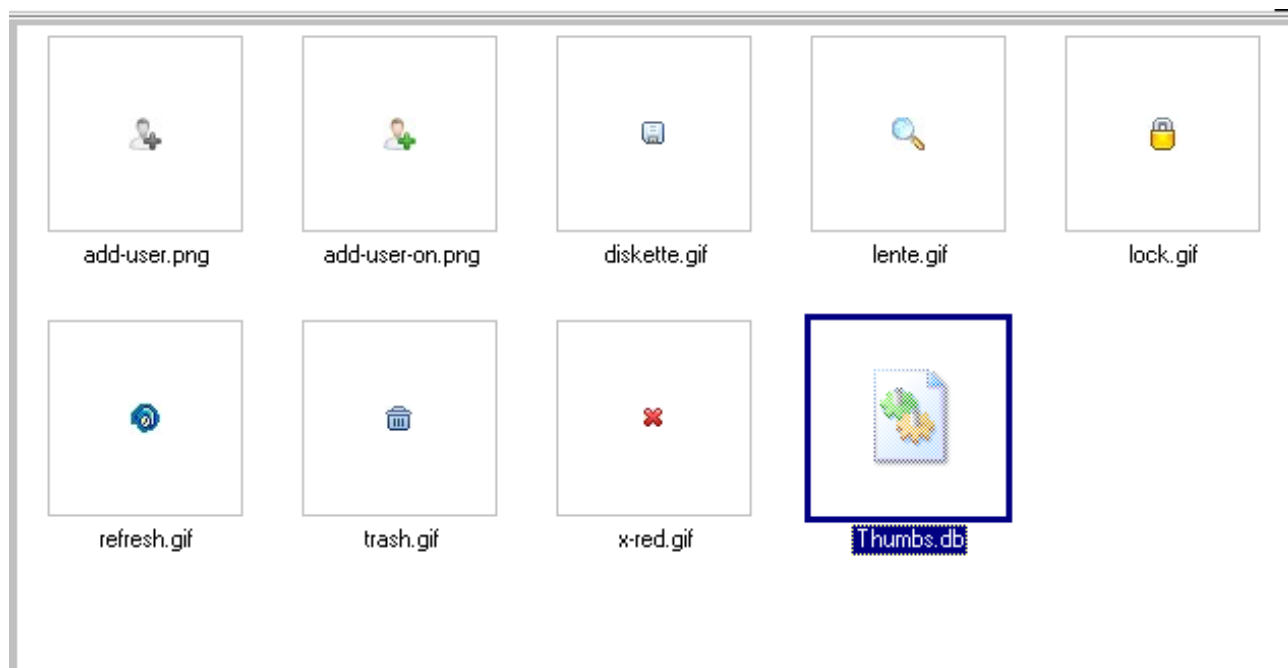
Una per la navigazione: **img/navigation**



In questo caso esistono anche le classi per i bottoni:

- input.first
- input.last
- input.next
- input.previous

E una per le azioni: **img/actions**



Ne può esistere una identica anche nelle cartelle di ciascun portale. Di norma è vuota e al massimo contiene qualche logo.

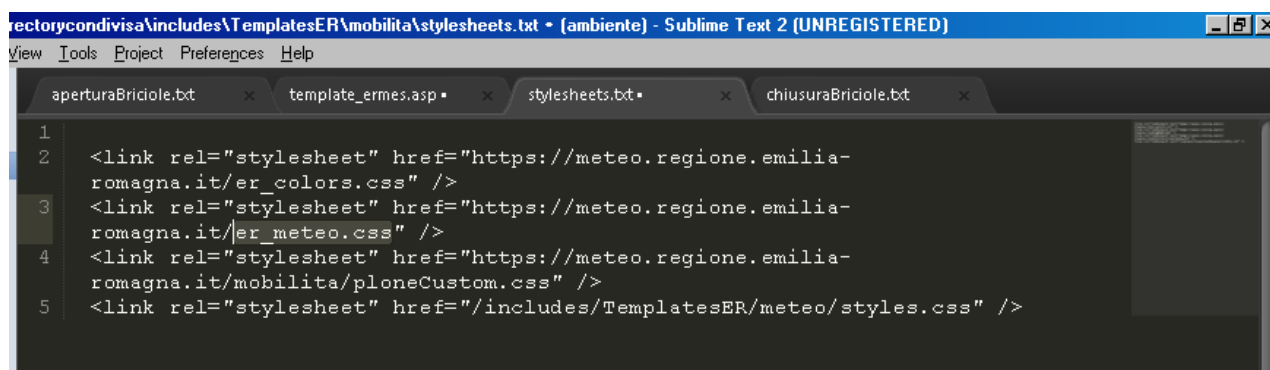
NB

Le immagini utili ad una applicazione di un portale, lo possono essere anche per tutte le applicazioni di tutti i portali, conviene quindi sempre condividerle a livello più alto.

3 Esempio di utilizzo di templates condivisi

L'esempio che segue è il caso di un'applicazione integrata con un portale esemplificativo "Meteo".

1. Sul server sarà presente una "meteo" sotto <http://www.servizitest.regione.emilia-romagna.it/includes/TemplatesER>
2. La cartella conterrà i files:
 - aperturaBriciole.txt
 - chiusuraBriciole.txt
 - footer.tx
 - styles.css
 - stylesheets.txt
 - template_ermes.asp
 - testata.txt
3. Il file **styleshets.txt** punta all'indirizzo di produzione del portale, ovvero "**meteo.regione.emilia-romagna.it**".



```
1
2 <link rel="stylesheet" href="https://meteo.regione.emilia-
romagna.it/er_colors.css" />
3 <link rel="stylesheet" href="https://meteo.regione.emilia-
romagna.it/er_meteo.css" />
4 <link rel="stylesheet" href="https://meteo.regione.emilia-
romagna.it/mobilita/ploneCustom.css" />
5 <link rel="stylesheet" href="/includes/TemplatesER/meteo/styles.css" />
```

4. I link in testata.txt e footer.txt puntano sempre a **meteo.regione.emilia-romagna.it**
5. Esempio di codice di una applicazione che utilizza i templates condivisi

3.1 Classic ASP

Template_ermes.asp contiene già le 3 funzioni necessarie per costruire la pagina:

- **Start_HeadTemplate**
che apre solo l'html
- **End_HeadTemplate (sezione, titolo_pagina, briciole)**
che chiude la testata incorporando i fogli di stile del portale prima e del portale tematico poi, inserisce il titolo, costruisce la banda del titolo del sottosito se presente e infine posizione la briciole

```

21 End Sub
22
23 Sub End_HeadTemplate (sezione, titolo_pagina, briciole)
24 %>
25 <title>
26 <%
27     If titolo_pagina <> "" then
28         response.Write titolo_pagina & " - Regione Emilia-Romagna"
29     Else
30         response.Write "Regione Emilia-Romagna "
31     End if
32 %>
33 </title>
34
35 <!--#include file="../stylesheets.txt"-->
36 <!--#include file="../stylesheets.txt"-->
37
38 <meta name="robots" content="noindex, nofollow" />
39 </head>
40
41 <body>
42 <div id="visual-portal-wrapper">
43 <!--#include file="testata.txt"-->
44 <% if sezione <> "" then %>
45 <div id="contentCarousel">
46 <div class="shadow_wrapper_sx">
47 <div class="shadow_wrapper_dx">
48 <div id="subsiteTitle">
49 <h2><%=sezione %></h2>
50 </div>
51 </div>
52 </div>
53 </div>
54 <% End if %>
55 <div class="shadow_wrapper_sx">
56 <div class="shadow_wrapper_dx">
57 <div id="contentTop">
58 <div class="page-max-width">
59 <div id="portal-breadcrumbs">
60 <a class="path_er" href="http://www.regione.emilia-romagna.it/">ER</a>
61 <span class="breadcrumbSeparator"> | </span>
62 <span dir="ltr">
63 <span><%=briciole %></span>
64 </span>
65 </div>
66 </div>
67 </div>
68 <div class="visualClear" id="clear-space-before-wrapper-table"><!--></div>
69 <!--div class="shadow_wrapper_sx">
70 <div class="shadow_wrapper_dx"-->
71 <table id="portal-columns">
72 <tbody>
73 <tr>
74 <td id="portal-column-content">
75 <div class="contenuti_pagine_interne">
76 <div id="content">
77
78 <!--FINE HEADER-->
79 <%
80 End Sub
81 Sub Crea_FooterTemplate ()

```

- **Crea_FooterTemplate**
che chiude la tabella di impaginazione fino a chiudere l'html, incorporando footer.txt

N.B:

Per quelle applicazioni asp, che hanno l'esigenza di incorporare ad esempio javascript specifici, queste funzioni sono avvolte in altre, analoghe, che le estendono. Es.:

```

Sub End_Head(sezione, titolo, briciole)
    %>
    <script type="text/javascript" src="/includes/validazioni.js"></script>
    <%
End sub

```


3.2 ASP.Net

Si riporta un esempio di una master page ASP.NET

```
<%@ master language="C#" autoeventwireup="true" codebehind="MasterPage.master.cs"
inherits="RER.Meteo.WebUI.MasterPage" %>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="it">
<head id="Head1" runat="server">
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <title>
    <asp:literal id="litTitle" runat="server" />
  </title>
  <!--#include virtual="/includes/TemplatesER/meteo/stylesheets.txt"-->
</head>
<body>
  <div id="visual-portal-wrapper">
    <!--#include virtual="/includes/TemplatesER/meteo/testata.txt"-->
    <div class="shadow_wrapper_sx">
      <div class="shadow_wrapper_dx">
        <form runat="server" id="form1">
          <!--#include
virtual="/includes/TemplatesER/meteo/aperturaBriciole.txt"-->
          <asp:literal id="litBriciole" runat="server" />
          <!--#include
virtual="/includes/TemplatesER/meteo/chiusuraBriciole.txt"-->
          <div class="visualClear" id="clear-space-before-wrapper-table"></div>
          <table id="portal-columns">
            <tbody>
              <tr>
                <td id="portal-column-content">
                  <div id="content">
                    <div class="contenuti_pagine_interne">
                      <h1 class="documentFirstHeading">
                        <asp:literal id="litTitoloPagina"
runat="server" />
                      </h1>
                      <a href="#esitoOperazione" name="anchorEsito"
id="anchorEsito" runat="server" class="skip">
                        salta a esito operazione</a><a
id="esitoOperazione" name="esitoOperazione"></a>
                      <asp:literal id="litEsito" runat="server"
enableviewstate="false" />
                    <div>
                      <asp:contentplaceholder id="cphContenuto"
runat="server"></asp:contentplaceholder>
                    </div>
                  </div>
                </td>
              </tr>
            </tbody>
          </table>
        </form>
      </div>
    </div>
    <!--#include virtual="/includes/TemplatesER/meteo/footer.txt"-->
  </div>
</body>
</html>
```

3.3 Microsoft MVC

Si riporta un esempio di shared layout:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="it">
<head>
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" />
  <title>@ViewBag.Title</title>
  @Html.Partial("InsertCSS")
</head>
<body>
  <div id="visual-portal-wrapper">
    @Html.Partial("testata")
    <!--FINE HEADER-->
    <div class="shadow_wrapper_sx">
      <div class="shadow_wrapper_dx">
        <div id="contentTop">
          @Html.Partial("aperturaBriciole")
          @ViewBag.Briciole
          @Html.Partial("chiusuraBriciole")
        </div>
        <div class="visualClear" id="clear-space-before-wrapper-table">
        </div>
        <table id="portal-columns">
          <tbody>
            <tr>
              <td id="portal-column-content">
                <div class="documentContent">
                  <div class="contenuti_pagine_interne">
                    <div id="content">
                      @RenderBody()
                    </div>
                  </div>
                </div>
              </td>
            </tr>
          </tbody>
        </table>
        <!--/div>
      </div-->
    </div>
    @Html.Partial("footer")
  </div>
</body>
</html>
```

Dove le partial sono pagine .aspx in cui è scritto il codice da includere, si riporta il solo esempio di "testata"

```
<%@ Page Language="C#" Inherits="System.Web.Mvc.ViewPage" %>
<!--#include virtual="/includes/TemplatesER/meteo/testata.txt"-->
```

Java

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%@ taglib uri="http://java.sun.com/jstl/core" prefix="c" %>
<html lang="it">
<head>
  <title>Meteo - Regione Emilia-Romagna</title>
  <meta http-equiv="X-UA-Compatible" content="IE=edge" >
```

```

    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" >
    <c:import url="http://wwwservizi.regione.emilia-
romagna.it/includes/TemplatesER/meteo/stylesheetshtml.txt" />
    <link type="text/css" href="http://wwwservizi.regione.emilia-
romagna.it/includes/templatesER/meteo/css/styles.css" rel="stylesheet"
media="screen" >
</head>
<body>
    <div id="visual-portal-wrapper">
        <c:import url="http://wwwservizi.regione.emilia-
romagna.it/includes/TemplatesER/meteo/testata.txt" />
        <div class="shadow_wrapper_sx">
            <div class="shadow_wrapper_dx">
                <c:import url="http://wwwservizi.regione.emilia-
romagna.it/includes/TemplatesER/meteo/aperturaBriciole.txt" />
                <c:import url="http://wwwservizi.regione.emilia-
romagna.it/includes/TemplatesER/meteo/chiusuraBriciole.txt" />
                <div class="visualClear" id="clear-space-before-wrapper-table"><!-- --></div>
                <table id="portal-columns">
                    <tbody>
                        <tr>
                            <td id="portal-column-content">
                                <div id="content">
                                    <div class="contenuti_pagine_interne">
                                        <form id='form1' name='form1' action='action1' method='post'>
                                            <table id='corpo-pagina' summary="tabella per
l'impaginazione">
                                                <tbody>
                                                    <tr>
                                                        <td>
                                                            <div id='header'>
                                                                <h1><%=title%></h1>
                                                            </div>
                                                            <div style="clear:both;"></div>
                                                            <div id='contenuto' style="margin-left:10px">
                                                                <div class='modulo'>
                                                                    </div>
                                                                </div>
                                                            </td>
                                                        </tr>
                                                    </tbody>
                                                </table>
                                            </form>
                                        </div>
                                    </div>
                                </td>
                            </tr>
                        </tbody>
                    </table>
                </div>
            </div>
        </div>
    <!-- footer -->
    <c:import url="http://wwwservizi.regione.emilia-
romagna.it/includes/TemplatesER/footer.txt"/>
</body>
</html>

```

NB: in filiera Microsoft i templates di utilità sono incorporati con url relativi in quanto la cartella includes/TemplatesER è una cartella virtuale ospitata sotto IIS, in tutti gli alti casi saranno sempre da incorporare con chiamate agli url assoluti **<https://wwwservizi.regione.emilia-romagna.it/includes/TemplatesER/nomesito>**

4 Stili ed accorgimenti da utilizzare

4.1 Titoli e bande orizzontali



Se una applicazione si trova in un sottosito riporta la banda colorata del sottosito (nell'immagine "Unioni di Comuni" è il sottosito).

In questo **caso si deve collegare un ulteriore foglio di stile**, subito prima di `</head>`

```
<link href="https://www.regione.emilia-romagna.it/portal_css/er_base_theme/rer_subsites.css" type="text/css" rel="stylesheet" />
</head>
```

Altre volte le applicazioni sono raggiungibili direttamente dalle home page e non hanno un sottosito che le accoglie: quindi non presentano la barra colorata.

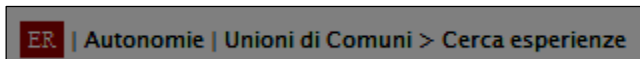
Il titolo delle varie pagine va formattato in questo modo:

```
<h1 class="documentFirstHeading">Risultati ricerca</h1>
```



4.2 **Briciole di pane**

Se una applicazione si trova in un sottosito, le briciole devono essere costruite in questo modo:



da notare i “|” tra portale, portale tematico e sottosito e il “>” tra i vari livelli dell’applicazione.

“ER” è il portale

“Autonomie” è il portale tematico

“Unioni di Comuni” è il sottosito

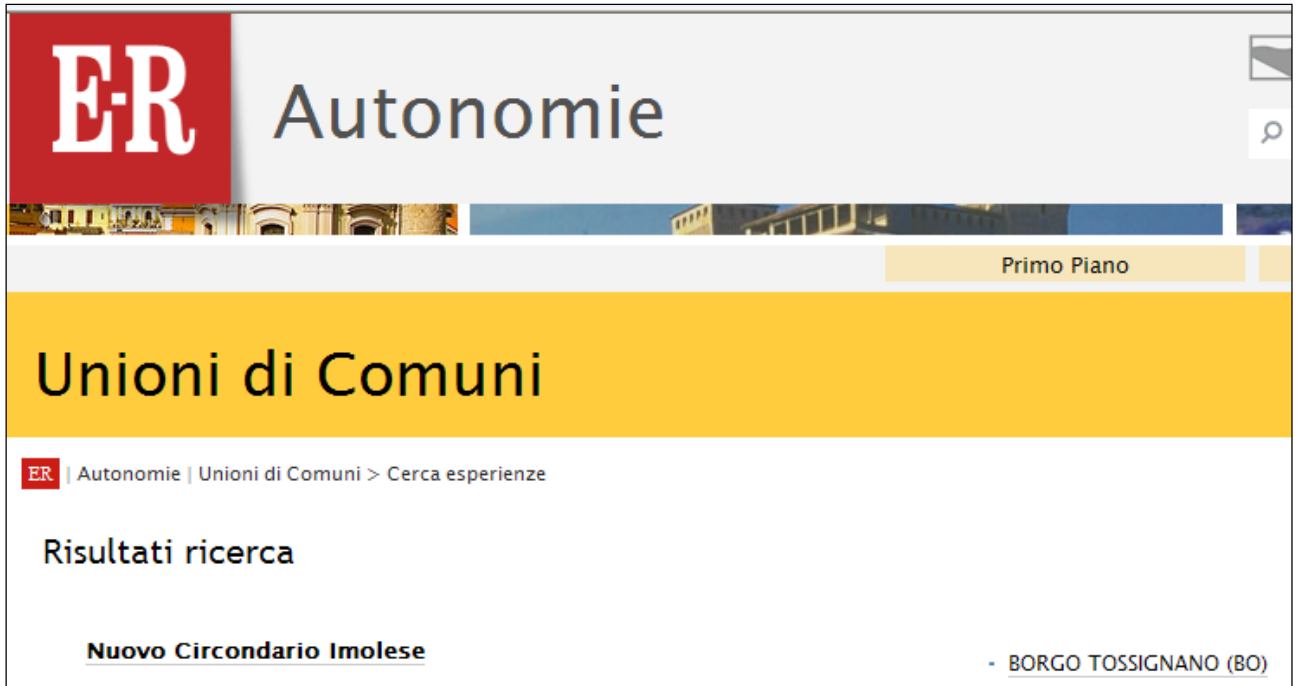
“Cerca esperienze” è il titolo dell’applicazione (che compare nella pagina di 2° livello dell’applicazione)

Le briciole di pane seguono le indicazioni presenti nelle linee guida: non riportano il nome della pagina su cui ci si trova, e sono costituite dai link a pagine che precedono quella attuale

Esempio prima pagina di un’applicazione di un sottosito



Esempio seconda pagina di un’applicazione di un sottosito



4.3 Menù

Se un'applicazione necessita di un menù interno, utilizzare gli stili del portale in cui va inserito:

Il menù è a destra all'interno di una nuova <td>.

Purtroppo per essere certi di ereditare tutti gli stili da Plone, occorre replicarne la struttura anche se è eccessivamente ricca.

```

<td id="portal-column-two">
  <div class="visualPadding">
    <div class="portletWrapper">
      <dl class="portlet portletNavigationTree">
        <dt class="portletHeader">
          <span class="portletTopLeft"></span>
          <a class="tile" href="#">Navigazione</a>
          <span
            class="portletTopRight"></span>
        </dt>
        <dd class="portletItem lastItem">
          <ul class="navTree navTreeLevel0">
            <li class="navTreeItem visualNoMarker">
              <div>
                <a href="#"><span>LINK</span></a>
              </div>
            </li>
          </ul>
          <span class="portletBottomLeft"></span>
          <span class="portletBottomRight"></span>
        </dd>
      </dl>
    </div>
  </div>
  &nbsp;
</td>

```



N.B:

Esistono 2 funzioni ASP, che svolgono questo compito:

- Sub Apri_MenuTemplate() che crea l'html fino a `<ul class="navTree navTreeLevel0">`
- Sub Chiudi_MenuTemplate() che comincia da ``

Se si deve quindi creare un menù sempre presente si può utilizzare, nell'applicazione, un metodo simile a questo:

```
Sub Crea_Menu
Apri_MenuTemplate
%>
<li><a href="http://autonomie.regione.emilia-romagna.it/entra-in-regione/norme-e-
documenti/decentramento-amministrativo">Documentazione</a></li>
<%
Chiudi_MenuTemplate
End Sub
```

4.4 Form

I form contengono quasi sempre uno o più riquadri `<fieldset class="v">` che danno loro lo sfondo grigio.

La classe, oltre allo sfondo fa sì che si possano inserire etichetta e campo in un div, e questo venga allineato correttamente. In questo caso:

```
<div>
<label for="associazione">Associazione:</label>
<input name="associazione" type="text" id="associazione" size="20" />
<span>(&grave; sufficiente parte del nome)</span>
</div>
```

The screenshot shows a web application interface with a dark blue header containing the word 'Associazione'. Below the header, there is a navigation bar with 'E-R' and 'Sociale'. The main content area is titled 'Banca dati delle associazioni' and contains three sections:

- Imposta i criteri di ricerca:** This section contains four input fields: 'Denominazione:' (with a text box and the note '(è sufficiente parte del nome)'), 'Comune:' (with a text box and the note '(è sufficiente parte del nome)'), 'Provincia:' (with a dropdown menu showing a minus sign), and 'Codice fiscale:' (with a text box and the note '(è sufficiente parte del codice fiscale)').
- Seleziona la rilevanza territoriale:** This section contains two checkboxes: 'regionale' and 'locale', both of which are currently unchecked.
- Seleziona una o più tipologie di attività:** This section contains a note '(NB: la selezione sulle tipologie di attività non sarà considerata se si è indicata la denominazione)' and four checkboxes: 'produzione e vendita di beni', 'ristorazione', 'commercio di beni', and 'bar e altre forme di somministrazioni di alimenti e bevande', all of which are currently unchecked.

Tutti i bottoni devono essere grigi, va in rosso solo quello dell'azione predefinita, o più importante.

<input type="submit" name="cerca" value="Cerca" class="cerca" />

4.5 Risultati di una ricerca e tabelle

Contenzioso costituzionale – Titolo V

ER | Autonomie | Contenzioso costituzionale – Titolo V > Ricerca per ricorso

Risultati ricerca per ricorso

Nr. totale record: 1639

Tutta la banca dati ⓘ Avvertenza: Le decisioni c
riportate più volte nel report di risultato sottostan
ono riguardare più ricorsi e, pertanto, possono essere

Export Excel

1 di 55 avanti ▶

Nr. totale record: 1639

Nr. ▼	Giudizio ▼	Atto impugnato ▼	Ricorrente ▼	Resistente ▼
70	Ricorso delle Regioni per legittimità costituzionale	Legge dello Stato	TOSCANA	PRESIDENZA DEL CONSIGLIO DEI MINISTRI
71	Ricorso delle Regioni per legittimità costituzionale	Legge dello Stato	TOSCANA	PRESIDENZA DEL CONSIGLIO DEI MINISTRI

I bottoni per scaricare files o eseguire alcune azioni possono avere un'icona, esistono infatti alcune classi predefinite nel css (se ne occorrono di nuove non crearle ma condividere l'esigenza per trovare una soluzione comune):

- pdf
- xls
- doc
- ppt
- zip



Le righe delle tabelle devono essere alternate con le classi **even** e **odd**, le intestazioni diventano grigie scure se vengono marcate come <th>

4.6 Dettaglio e elenchi con molte colonne (non intabellati)

Quando le colonne di dettaglio sono molte, è consigliabile usare altri sistemi per mostrare i dati: le liste non ordinate o di definizione, precedute da una intestazione, come in questo caso.





ASSOCIAZIONE GELSOMINA - IL CLOWN AL SERVIZIO DELLA PERSONA

attività' ricreativa, attività' varie, attività' a tutela della salute dei minori

 Indirizzo:	VIA FERRARESE 3 40128 BOLOGNA (BOLOGNA)
 Soci:	38
Atto Iscrizione:	Det. n. 124066 del. 26/03/2008 - Amministrazione Provinciale di Bologna

ASSOCIAZIONE MATRE TERRA

attività' a tutela della salute dei minori

 Indirizzo:	VIA DELL'OSSERVANZA 88 40136 BOLOGNA (BOLOGNA)
 Telefono:	051/582024
 Email:	matreterra@virgilio.it
 Soci:	12
Atto Iscrizione:	Det. n. 416497 del. 18/12/2007 - Amministrazione Provinciale di Bologna


In particolare le anagrafiche hanno alcune icone associabili ai campi usati più spesso:

- dl.anagrafica.indirizzo
- dl.anagrafica.telefono
- dl.anagrafica.fax
- dl.anagrafica.persona
- dl.anagrafica.email, .email
- dl.anagrafica.emailcert
- dl.anagrafica.web

4.7 Altre possibili forme di un elenco di risultati e dettagli

Altri aspetti possibili per una<dl> sono:

1. <http://wwwservizi.regione.emilia-romagna.it/ambiente/vetrinasostenibilita/>

 Ambiente | Vetrina della sostenibilità > Ricerca Buone Pratiche

Elenco Buone Pratiche

hai cercato per:
Sezione: - Settore: - Area: - Provincia: - Titolo: - Organizzazione/Ente: - Parola: -

BO001	<u>Agricoltura e territorio</u>	Cooperativa Dulcamara - Ozzano dell'Emilia (BO)
BO003	<u>Dismo dissociatore molecolare</u>	ITEA S.p.A - Zola Predosa (BO)
BO004	<u>Progetto di comunicazione e monitoraggio ambientale</u>	Associazione Amici della terra - Club di Ozzano Emilia ONLUS - Ozzano dell'Emilia (BO)

2. <http://wwwservizi.regione.emilia-romagna.it/sagre/default.asp>

RISULTATI DELLA RICERCA FIERE

22/07/2015 – **FIERA DEI PRODOTTI NATURALI E BIOLOGICI IN LIDO DELLE NAZIONI – COMACCHIO (FE)**

Merci: prodotti dell'apicoltura, erboristeria, cartoleria ecologica, essenze naturali, lavori con fiori secchi, frutti particolari.

Note: *la fiera ha cadenza settimanale dal primo mercoledì di giugno all'ultimo mercoledì di settembre*

22/07/2015 – **SAGRA DI SAN GIACOMO – RO (FE)**

Merci: posteggio assegnato (n.5) settore alimentare – posteggi non assegnati (nn. 6, 7, 8, 9) settore merceologico indistinto

23/07/2015 – **MERCATINO SOTTO LE STELLE – FRASSINORO (MO)**

Merci: artigianato (cucito, ricami, ceramica, bigiotteria), prodotti alimentari tipici, dolciumi, formaggi, abbigliamento, pelletteria.

Note: *coordinamento: pro loco piandelagotti*

Con il relativo dettaglio

SAGRA DI SAN GIACOMO

Dove

capoluogo: p.zza umberto i – p.zza mazzini, **RO (FE)**

Date e orari

20/07/2015 (19:00 – 23:90)

21/07/2015 (19:00 – 23:90)

22/07/2015 (19:00 – 23:90)

23/07/2015 (19:00 – 23:90)

24/07/2015 (19:00 – 23:90)

25/07/2015 (19:00 – 23:90)

Posteggi

5 di cui:

Assegnati in concessione:

- Alimentare 1 (32mq)

Non assegnati in concessione:

3. <http://wwwservizi.regione.emilia-romagna.it/autonomie/gestioni-associate/>

Risultati ricerca

Nuovo Circondario Imolese






- [BORGHI TOSIGNANO \(BO\)](#)
- [CASALFUMANESE \(BO\)](#)
- [CASTEL DEL RIO \(BO\)](#)
- [CASTEL GUELFO DI BOLOGNA \(BO\)](#)
- [CASTEL SAN PIETRO TERME \(BO\)](#)
- [DOZZA \(BO\)](#)
- [FONTANELICE \(BO\)](#)
- [IMOLA \(BO\)](#)
- [MEDICINA \(BO\)](#)
- [MORDANO \(BO\)](#)

Unione Alto Ferrarese


- [BONDENO \(FE\)](#)

Con il relativo dettaglio



Nuovo Circondario Imolese

 Indirizzo	Via Boccaccio 27 40026 IMOLA (BO)
 Telefono	0542-603200
 Fax	0542-34895
 Email	circ@provincia.bologna.it
 Web	http://www.nuovocircondarioimolese.it/

Documenti fondamentali

- Statuto 

Servizi / funzioni trasferiti all'Unione o gestiti in forma associata

- **Funzioni attinenti il settore sociale e socio sanitario**
 - Ufficio di Piano sociale, ISEE, Servizi nidi, servizi agli anziani, servizi ai disabili, servizi al disagio sociale, servizi ai minori
 - Programmazione politiche Sociali
- **Funzioni di polizia municipale e Protezione Civile**
 - Polizia municipale, Protezione civile 
- **Gestione del Personale**
 - Reclutamento, trattamento economico, trattamento giuridico, relazioni sindacali, formazione professionale 
- **Gestione del territorio**
 - Gestione e manutenzione strade
 - Funzione urbanistica

Allegato 12: Scheda tecnica per nuovo servizio da erogare o fruire tramite Porta di Dominio IcarER

Fruizione di un servizio

Dati del Gestore del servizio	
Nome	
Cognome	
Email	
Telefono	
Note	
Soggetto Fruitore	
Nome del Soggetto	<i>Si tratta del Soggetto SPCoop che desidera fruire del servizio</i>
Dati identificativi del servizio	
Nome del Soggetto Erogatore	<i>Si tratta del Soggetto SPCoop che eroga il servizio</i>
Nome del Servizio	<i>Indicare il nome del servizio</i>
Accordo di Servizio *	<i>Se l'accordo di servizio è già configurato indicare Nome, Soggetto Referente e Versione.</i>
Package CNIPA *	<i>Allegare il package 'apc' / 'aps'</i>
Dati di cooperazione *	<i>Indicare il nome del servizio, delle azioni con i relativi profili che compongono l'accordo. In caso di profilo asincrono (simmetrico o asimmetrico) dovranno essere indicati anche il nome del servizio e dell'azione correlata. Opzionalmente, allegare il wsdl</i>
Messaggi di Test	<i>Se esistono, allegare messaggi di test in formato xml. Per ogni messaggio deve essere indicata l'azione e il servizio corrispondente.</i>
Accordo di Servizio *	<i>Se l'accordo di servizio è già configurato indicare Nome, Soggetto Referente e Versione.</i>
Dati della Porta di Dominio che eroga il servizio <i>(da compilare solo se esterna alla Regione Emilia Romagna)</i>	
Endpoint	<i>Url con la quale richiamare la PDD</i>
IP pubblico	<i>Specificare l'IP (o gli IP se fossero più di uno) sui quali la PDD viene contattata</i>
IP di presentazione	<i>Specificare l'IP (o gli IP se fossero più di uno) con i quali la PDD si presenta verso l'esterno.</i>
Identificativo Porta	<i>Es: RegioneEmiliaRomagnaSPCoopIT</i>
Identificativo Parta	<i>Es.: SPC/RegioneEmiliaRomagna</i>

Erogazione di un servizio

Dati del Gestore del servizio	
Nome	
Cognome	
Email	
Telefono	
Note	
Dati del servizio	
Accordo di Servizio *	<i>Se l'accordo di servizio è già configurato indicare Nome, Soggetto Referente e Versione.</i>
Package CNIPA *	<i>Allegare il package 'apc' / 'aps'</i>
Dati di cooperazione *	<i>Indicare il nome del servizio, delle azioni con i relativi profili che compongono l'accordo. In caso di profilo asincrono (simmetrico o asimmetrico) dovranno essere indicati anche il nome del servizio e dell'azione correlata. Opzionalmente, allegare il wsdl</i>
Messaggi di Test	<i>Se esistono, allegare messaggi di test in formato xml. Per ogni messaggio deve essere indicata l'azione e il servizio corrispondente.</i>
Url interno da richiamare	<i>L'url all'interno della rete regionale che eroga il servizio esposto</i>
Autenticazione HTTP	
Credenziali richieste dal Servizio Applicativo Erogatore	<i>Fornire Username e Password</i>
Autenticazione HTTPS	
Credenziali richieste dal Servizio Applicativo Erogatore	<i>Allegare il certificato X509</i>
URI e Credenziali per asincrono asimmetrico	<i>In caso di profilo asincrono asimmetrico devono essere indicati anche i dati di accesso al servizio applicativo che permette di effettuare il polling per comprendere se la risposta asincrona è disponibile: URI interna e modalità di autenticazione con relative credenziali:username e password oppure allegare il certificato</i>

* Le sezioni **Accordo di Servizio**, **Package CNIPA**, **Dati di cooperazione** sono alternative. Compilare solo una delle tre. In presenza dell'Accordo di Servizio compilare solo la sezione **Accordo di Servizio**, in presenza del Package CNIPA compilare solo la sezione **Package CNIPA**. In assenza dei due precedenti compilare la sezione **Dati di cooperazione**.

Riferimenti e bibliografia

<http://www.digitpa.gov.it/reti-della-pa/spc-i-concetti-chiave>
<http://www.digitpa.gov.it/reti-della-pa/documenti-tecnico-operativi>
<http://www.digitpa.gov.it/reti-della-pa/specifiche-requisiti-funzionali-del-spcoop>
<http://www.openspcoop.org>

Allegato 13: Specifiche tecniche per l'utilizzo dei web services di consultazione dei dati di personale e strutture

1	Introduzione	1
1.1	Web services	1
1.2	Descrizione generale	1
1.3	Storicizzazione.....	2
2	Classi principali.....	2
2.1	UnitaFunzionale.....	2
2.2	Persona.....	3
3	Classi "creazionali" e di utilità	5
3.1	UnitaFunzionaleManager.....	5
3.2	Persona Manager	7
4	Gestione delle gerarchie	7
5	Esempi d'uso	8
6	Specifiche per l'accesso al web service	9
6.1	"Schemi" XML	9
6.2	Dettaglio delle funzioni.....	11

1 Introduzione

Questo documento ha lo scopo di descrivere l'utilizzo dei componenti in RER.Tools.Organigramma, namespace contenente le classi che permettono l'accesso ai dati dell'organigramma regionale. Tali dati risiedono attualmente su SAP HR, ma è stata predisposta una replica su SQL Server. Le classi di RER.Tools.Organigramma accedono ai dati presenti su SQL Server.

La configurazione dei parametri d'accesso al DB è eseguita al livello di machine.config dei singoli web server della filiera .NET, pertanto ogni applicazione installata su tali web server può utilizzare tali classi senza fare altro che aggiungere il riferimento alla DLL corrispondente.

1.1 Web services

Una sintesi delle funzioni disponibili tramite la class library RER.Tools.Organigramma è fruibile anche attraverso un web service. Si veda il capitolo 6 ("Specifiche per l'accesso al web service") per i riferimenti e le specifiche.

1.2 Descrizione generale

Le entità che riguardano l'organigramma e su cui è basata la libreria delle classi si possono sintetizzare in:

- Unità funzionali: strutture apicali (direzioni/agenzie/istituti/ecc.), servizi, posizioni di responsabilità, ...
- Persone: i dipendenti regionali o comunque chi ha un rapporto di lavoro con la Regione
- Caratteristiche: si tratta di "attributi" che possono essere associati alle unità funzionali (per esempio, tutte le direzioni generali hanno la caratteristica "DIG", i servizi hanno la caratteristica "SER", ...)

I servizi forniti sono essenzialmente i seguenti:

- dettaglio delle informazioni relative ad una unità funzionale;
- elenco delle unità funzionali che soddisfano certi parametri di ricerca;
- dettaglio delle informazioni relative ad una persona;
- risposte a domande tipo “una persona appartiene a un struttura?”, oppure “c’è un legame di parentela tra due unità funzionali?”, ...

1.3 Storicizzazione

L’organigramma regionale è una struttura che muta nel tempo, perciò qualsiasi estrazione di dati da tale struttura deve sempre essere relativa ad un ben preciso istante. Pertanto tutte le chiamate di metodi hanno sempre come parametro la *data di riferimento*, anche se per comodità sono stati aggiunti gli overload in cui non è necessario passare la data di riferimento che, in questo caso, è fissata con la data corrente.

NB: per motivi “storici” le “date fine” su DB contengono il valore “31/12/2049” per indicare che non c’è una data di fine. Invece, all’interno di questa libreria di classi, tali valori sono stati sostituiti con il valore `DateTime.MaxValue`.

2 Classi principali

Le classi principali implementate sono le seguenti:

- **UnitaFunzionale**: contiene i dati di un unità funzionale
- **Persona**: contiene i dati di una persona

Per quanto riguarda `UnitaFunzionale` e `Persona`, si sono implementate anche le corrispondenti classi **`UnitaFunzionaleCollection`** e **`PersonaCollection`**. Infine esiste anche la classe **`Caratteristica`** e la relativa **`CaratteristicaCollection`**.

2.1 UnitaFunzionale

Di seguito si riporta la definizione della classe (senza implementazione). Si veda anche il capitolo 3 per come creare istanze di questa classe.

```
[Serializable]
public class UnitaFunzionale
{
    public DateTime DataRif;

    public int Livello;
    public string Cod;
    public DateTime DataInizio;
    public DateTime DataFine;
    public string Descrizione;
    public string CodUnitaPadre;
    public int MatricolaResponsabile;
    public string DescrizioneEstesa;

    public static string NullCod;
    public static int NullLivello;

    public PersonaCollection ElencaPersoneAssegnate();
    public UnitaFunzionaleCollection ElencaDiscendentiDiretti();
    public CaratteristicaCollection ElencaCaratteristiche();
    public bool HaLeCaratteristiche(string[] caratteristiche,
```

```

bool richiediTutteLeCaratteristiche);
public bool HaLaCaratteristica(string codCaratteristica);

public bool DiscendeDa(string codUnitaAntenato, int livelloMax);
public bool DiscendeDa(string codUnitaAntenato);

public int CalcolaLivelliParentela(string codUnitaAntenato, int livelloMax);
public int CalcolaLivelliParentela(string codUnitaAntenato);

} // end class UnitaFunzionale

```

Descrizione attributi

I primi attributi rappresentano il dettaglio dei dati dell'unità funzionale. Il campo Livello rappresenta a che livello, nella gerarchia delle unità funzionali si trova quella specifica unità funzionale, in verità questa informazione non è sempre presente, in tal caso sarà indicato. Nel caso non sia presente, l'attributo Livello è valorizzato con il valore dell'attributo statico NullLivello.

Analogamente è stato definito l'attributo statico NullCod, utile in tutti i casi in si vuole indicare il concetto di "nessuna unità funzionale" (per esempio, l'attributo CodUnitaPadre vale NullCod nel caso in cui l'unità funzionale non abbia nessun padre, oppure: se tra i parametri di un metodo di ricerca si può indicare il codice di un'unità funzionale, ma in verità non si vuole fare nessuna scelta, si può utilizzare UnitaFunzionale.NullCod).

Descrizione metodi

Relativamente ai metodi, non c'è molto da dire, i nomi sono "parlanti", solo qualche precisazione:

1. essendo metodi di "istanza" non accettano parametri. Quindi, per esempio, la chiamata al metodo "ElencaPersoneAssegnate" significa implicitamente "elenca le persone assegnate all'unità funzionale in data DataRif".
2. il parametro LivelloMax (dei metodi DiscendeDa e CalcolaLivelliParentela) funziona come un limitatore, ovverosia "DiscendaDa" limita il controllo alle unità funzionali entro Livello Max livelli.
3. CalcolaLivelliParentela calcola la distanza tra l'unità funzionale e un possibile antenato (codUnitaAntenato), se non c'è parentela (oppure è superiore a LivelloMax) il metodo ritorna il valore UnitaFunzionale.NullLivello.

2.2 Persona

Di seguito si riporta la definizione della classe (senza implementazione). Si veda anche il capitolo 3 per come creare istanze di questa classe.


```

[Serializable]
public class Persona
{
    public DateTime DataRif;

    public int Matricola;
    public string Nome;
    public string Cognome;
    public string CodiceFiscale;
    public string Sesso;
    public DateTime DataNascita;
    public string CodCatastoNascita;
    public string Email;
    public string StatoCivile;
    public string CognomeAcquisito;
    public string ResidenzaIndirizzo;
    public string ResidenzaCap;
    public string ResidenzaCodComune;
    public string ResidenzaFrazione;
    public string DomicilioIndirizzo;
    public string DomicilioCap;
    public string DomicilioCodComune;
    public string Domicilio Frazione;
    public string CodUnitaAppartenenza;
    public string CodUnitaResponsabilita;
    public string CodRapportoTipoLavoro;
    public DateTime DataAssunzione;
    public DateTime DataCessazione;

    public static int NullMatricola;
    public static DateTime NullDataNascita;
    public static DateTime NullDataAssunzione;
    public static DateTime NullDataCessazione;

    public bool IsAssegnataAUnitaFunzionale(string codUnita);
    public bool IsResponsabileUnitaFunzionale(string codUnita);
}

```

Descrizione attributi

I nomi degli attributi dovrebbero essere sufficienti a spiegare il contenuto. Si noti solo che sono presenti degli attributi statici che contengono valori “particolari”: quelli con prefisso “Null”. Come per l’unità funzionale, sono stati definiti per gestire i casi di “mancanza di dati”. Per esempio se la persona non ha data di cessazione allora il corrispondente campo avrà come valore Persona.NullDataCessazione. Stesso discorso, ma questa volta riferito all’unità funzionale, per l’attributo CodUnitaResponsabilita, nel caso la persona non sia responsabile di nessuna struttura, allora l’attributo è valorizzato on UnitaFunzionale.NullCod.

Descrizione metodi

Come per l’unità funzionale, relativamente ai metodi, non c’è molto da dire, i nomi sono “parlanti”. Vale sempre la precisazione che, essendo metodi di “istanza”, perciò la chiamata al metodo “IsAssegnataAUnitaFunzionale” significa implicitamente “la persona è assegnata alla struttura (passata come parametro) in data DataRif?”.

3 Classi "creazionali" e di utilità

Finora si è vista la struttura delle classi fondamentali, in verità esse rappresentano la base per costruire le informazioni restituite dai metodi delle seguenti classi che sono puramente "statiche", in quanto implementano solo "servizi": di creazione delle classi basi e ricerca vera a propria nell'organigramma.

Un paio di precisazioni:

1. di ogni metodo, per comodità, sono stati definiti diversi overload che permettono di evitare di indicare certi parametri, i quali assumono quindi dei valori di default, in questo documento è indicato solo la versione "completa";
2. riguardo al parametro *dataRif* (la data riferimento), come già accennato nel paragrafo 1.3, se non indicato si assume la data corrente (tale fatto non sarà ulteriormente precisato nei dettagli dei singoli metodi).

3.1 UnitaFunzionaleManager

```
UnitaFunzionale Crea(  
    string codUnita,  
    DateTime dataRif)
```

Crea un'istanza dell'unità funzionale

```
UnitaFunzionaleCollection Elenca(  
    DateTime dataRif,  
    string[] caratteristiche,  
    bool richiediTutteLeCaratteristiche)
```

Elenca le unità funzionali aventi le caratteristiche specificate (tutte o almeno una a seconda del valore di 'richiediTutteLeCaratteristiche'.

NB: Il valore dell'attributo Livello delle unità funzionali presenti nella collection in questo caso non è valorizzato.

```
UnitaFunzionaleCollection ElencaDiscendentiDiretti(  
    string codUnitaRadice,  
    DateTime dataRif,  
    string[] caratteristiche,  
    bool richiediTutteLeCaratteristiche)
```

Elenca le unità funzionali discendenti direttamente dall'unità funzionale *codUnitaRadice* (le "figlie") aventi le caratteristiche specificate (tutte o almeno una a seconda del valore di 'richiediTutteLeCaratteristiche'

```
UnitaFunzionaleCollection ElencaDiscendentiInProfondita(  
    string codUnitaRadice,  
    DateTime dataRif,  
    string[] caratteristiche,  
    bool richiediTutteLeCaratteristiche)
```

Elenca le unità funzionali discendenti direttamente o indirettamente dall'unità funzionale *codUnitaRadice* aventi le caratteristiche specificate (tutte o almeno una a seconda del valore di 'richiediTutteLeCaratteristiche'

```
UnitaFunzionaleCollection ElencaDiscendenti(  
    string codUnitaRadice,  
    int livelloMax,  
    DateTime dataRif,  
    string[] caratteristiche,  
    bool richiediTutteLeCaratteristiche)
```

Elenca le unità funzionali discendenti fino al livello livelloMax dall'unità funzionale codUnitaRadice aventi le caratteristiche specificate (tutte o almeno una a seconda del valore di 'richiediTutteLeCaratteristiche')

```
PersonaCollection ElencaPersone(  
    string codUnita,  
    DateTime dataRif)
```

Elenca le persone assegnate all'unità funzionale

```
bool DiscendeDa(  
    string codUnita,  
    string codUnitaAntenato,  
    DateTime dataRif,  
    int livelloMax)
```

Calcola se c'è un legame di parentela con non più di 'livelloMax' livelli tra l'unità codUnita e codUnitaAntenato (codUnita deve discendere da codUnitaAntenato). Assegnare UnitaFunzionale.NullLivello a 'livelloMax' per eseguire la ricerca su tutti i livelli possibili

```
bool FigliaDi(  
    string codUnita,  
    string codUnitaPadre,  
    DateTime dataRif)
```

Calcola se un'unità funzionale codUnita discende direttamente da codUnitaPadre

```
int CalcolaLivelliParentela(  
    string codUnita,  
    string codUnitaAntenato,  
    DateTime dataRif,  
    int livelloMax)
```

Calcola la 'distanza', in 'livelli di parentela', tra l'unità funzionale codUnita e un suo antenato (codUnitaAntenato). Assegnare UnitaFunzionale.NullLivello a 'livelloMax' per eseguire la ricerca su tutti i livelli possibili. Se le due unità non sono parenti o la distanza è maggiore di 'livelloMax' restituisce UnitaFunzionale.NullLivello

```
CaratteristicaCollection ElencaCaratteristiche(  
    string codUnita,  
    DateTime dataRif)
```

Elenca le caratteristiche assegnate all'unità funzionale

```
bool HaLeCaratteristiche(  
    string codUnita,  
    DateTime dataRif,  
    string[] caratteristiche,  
    bool richiediTutteLeCaratteristiche)
```

Calcola se l'unità funzionale ha le caratteristiche specificate (tutte o almeno una a seconda del valore

di 'richiediTutteLeCaratteristiche'

```
bool HaLaCaratteristica(  
    string codUnita,  
    DateTime dataRif,  
    string caratteristica)
```

Calcola se l'unità funzionale ha la caratteristica specificata

```
UnitaFunzionale CercaAntenatoConCaratteristica(  
    string codUnita,  
    DateTime dataRif,  
    string caratteristica,  
    int distanzaMax)
```

Restituisce, se esiste, la prima unità funzionale (tra gli antenati, scorrendoli a ritroso, fino a 'distanzaMax' livelli) che ha le caratteristiche specificate (tutte o almeno una a seconda del valore di 'richiediTutteLeCaratteristiche'). Assegnare `UnitaFunzionale.NullLivello` a 'distanzaMax' per eseguire la ricerca fino alla radice. Se non esiste nessuna unità funzionale che ha i requisiti restituisce *null*

3.2 Persona Manager

```
Persona Crea(  
    int matricola,  
    DateTime dataRif)
```

Crea un'istanza della persona

```
bool IsResponsabileUnitaFunzionale(  
    int matricola,  
    string codUnita,  
    DateTime dataRif)
```

Calcola se la persona è il responsabile dell'unità funzionale

```
bool IsAssegnataAUnitaFunzionale(  
    int matricola,  
    string codUnita,  
    DateTime dataRif)
```

Calcola se la persona è assegnata all'unità funzionale

```
IncaricoCollection ElencaIncarichi(  
    int matricola,  
    DateTime dataRif)
```

Elenca tutti gli incarichi di una persona.

4 Gestione delle gerarchie

La classe **UnitaFunzionaleGerarchia** (e la sua controparte **UnitaFunzionaleGerarchiaManager**) contiene i dati di una (porzione) di gerarchia dell'organigramma ed è stata introdotta per gestire efficientemente e efficacemente¹ i risultati di ricerche sulle unità funzionali per cui si vuole un output

¹ Di fatto, la chiamata a questo metodo, esegue un solo accesso al DB, per costruire l'intera gerarchia

“gerarchico” (utile per una navigazione o rappresentazione dei dati tramite un “albero”)
La classe contiene sono un sottoinsieme minimale degli attributi delle unità funzionali:

```
public class UnitaFunzionaleGerarchia
{
    public string Cod;
    public string Descrizione;
    public UnitaFunzionaleGerarchiaCollection Discendenti;
}
```

Per creare una gerarchia utilizzare il seguente metodo statico della classe UnitaFunzionaleGerarchiaManager:

```
UnitaFunzionaleGerarchia Crea(
    string codUnitaRadice,
    int livelloMax,
    DateTime dataRif)
```

Crea la gerarchia completa dei discendenti dell'unità con non più di 'livelloMax' livelli di parentela. Assegnare UnitaFunzionale.NullLivello a 'livelloMax' per creare la gerarchia su tutti i livelli possibili

5 Esempi d'uso

```
foreach(UnitaFunzionale u in UnitaFunzionaleManager.Elenca())
    Console.WriteLine("{0} | {1} | {2} | {3}", u.Cod, u.Descrizione, u.CodUnitaPadre,
u.MatricolaResponsabile);

foreach(UnitaFunzionale u in UnitaFunzionaleManager.Elenca(new DateTime(2006,08,21), "SER"))
    Console.WriteLine("{0} | {1} | {2} | {3}", u.Cod, u.Descrizione, u.CodUnitaPadre,
u.MatricolaResponsabile);

foreach(Persona p in UnitaFunzionaleManager.ElencaPersone("00000315", new
DateTime(2005,12,31)))
    Console.WriteLine("{0} | {1} | {2} | {3}", p.Matricola, p.Cognome, p.Nome, p.CodiceFiscale);

foreach(UnitaFunzionale u in UnitaFunzionaleManager.Elenca(new DateTime(2005,12,31), new
string[] {"ENT", "IST", "DIG"}, false))
    Console.WriteLine("{0} | {1} | {2} | {3}", u.Cod, u.Descrizione, u.CodUnitaPadre,
u.MatricolaResponsabile);

foreach(UnitaFunzionale u in UnitaFunzionaleManager.Elenca(new DateTime(2005,12,31), new
string[] {"DIG", "BUD", "ORG"}, true))
    Console.WriteLine("{0} | {1} | {2} | {3}", u.Cod, u.Descrizione, u.CodUnitaPadre,
u.MatricolaResponsabile);

foreach(UnitaFunzionale u in UnitaFunzionaleManager.Elenca(new DateTime(2005,12,31), new
string[] {"SER"}, true))
    Console.WriteLine("{0} | {1} | {2} | {3}", u.Cod, u.Descrizione, u.CodUnitaPadre,
u.MatricolaResponsabile);

Console.WriteLine(PersonaManager.IsResponsabileUnitaFunzionale(999999, "00000315", new
DateTime(2005,12,31) ));
Console.WriteLine(PersonaManager.IsAssegnataAUnitaFunzionale(999999, "00000315", new
DateTime(2005,12,31) ));
Console.WriteLine(PersonaManager.IsAssegnataAUnitaFunzionale(999999, "00000315", new
DateTime(2005,12,31) ));
```

```

Console.WriteLine(UnitaFunzionaleManager.DiscendeDa("00000315", "D0000022", new
DateTime(2005,12,31), 1 ));
Console.WriteLine(UnitaFunzionaleManager.DiscendeDa("00000315", "D0000022", new
DateTime(2000,12,31) ));

foreach(UnitaFunzionale u in UnitaFunzionaleManager.ElencaDiscendenti("D0000022", 3, "SER"))
    Console.WriteLine("{0} | {1} | {2} | {3}", u.Cod, u.Descrizione, u.CodUnitaPadre,
u.MatricolaResponsabile);

Persona p = PersonaManager.Crea(999999);
Console.WriteLine(p.Cognome + " " + p.IsResponsabileUnitaFunzionale("00000435"));

UnitaFunzionale u = UnitaFunzionaleManager.Crea("00000315", new DateTime(2005,12,31));
Console.WriteLine("***** PERSONA ASSEGNATE: *****");
foreach(Persona p in u.ElencaPersoneAssegnate())
    Console.WriteLine("{0} | {1} | {2} | {3}", p.Matricola, p.Cognome, p.Nome, p.CodiceFiscale);
Console.WriteLine("***** DISCENDENTI DIRETTI: *****");
foreach(UnitaFunzionale u1 in u.ElencaDiscendentiDiretti())
    Console.WriteLine("{0} | {1} | {2} | {3}", u1.Cod, u1.Descrizione, u1.CodUnitaPadre,
u1.MatricolaResponsabile);
Console.WriteLine("***** CARATTERISTICHE: *****");
foreach(Caratteristica c in u.ElencaCaratteristiche())
    Console.WriteLine("{0} | {1}", c.Cod, c.Descrizione);
Console.WriteLine(u.HaLeCaratteristiche(new string[] {"SER", "DPS"}, false));
Console.WriteLine(u.DiscendeDa("D0000022"));
Console.WriteLine(u.CalcolaLivelliParentela("G0000001"));

Console.WriteLine(UnitaFunzionaleManager.CercaAntenatoConCaratteristica("00000315", new
DateTime(2005,12,31), "DIG").Cod);

```

6 Specifiche per l'accesso al web service

L' "end-point" a cui fare riferimento per l'utilizzo del web service è il seguente:

<http://intraservizi.regione.emilia-romagna.it/WebServices/Organigramma/Main.asmx>

Il file WSDL corrispondente è scaricabile dal seguente indirizzo:

<http://intraservizi.regione.emilia-romagna.it/WebServices/Organigramma/Main.asmx?WSDL>

6.1 "Schemi" XML

Le strutture dati utilizzate dal servizio sono prima di tutto schematizzate all'interno del file WSDL, comunque si riportano di seguito, per ulteriore chiarezza, i frammenti XML corrispondenti a tali strutture dati.

Persona

```
<Persona>
  <DataRif></DataRif>
  <Matricola></Matricola>
  <Nome></Nome>
  <Cognome></Cognome>
  <CodiceFiscale></CodiceFiscale>
  <Sesso></Sesso>
  <DataNascita></DataNascita>
  <CodCatastoNascita></CodCatastoNascita>
  <Email></Email>
  <StatoCivile></StatoCivile>
  <CoognoomeAcquisito></CoognoomeAcquisito>
  <ResidenzaIndirizzo></ResidenzaIndirizzo>
  <ResidenzaCap></ResidenzaCap>
  <ResidenzaCodComune></ResidenzaCodComune>
  <ResidenzaFrazione></ResidenzaFrazione>
  <DomicilioCap></DomicilioCap>
  <DomicilioCodComune></DomicilioCodComune>
  <DomicilioFrazione></DomicilioFrazione>
  <CodUnitaAppartenenza></CodUnitaAppartenenza>
  <CodUnitaResponsabilita></CodUnitaResponsabilita>
  <CodRapportoTipoLavoro></CodRapportoTipoLavoro>
  <DataAssunzione></DataAssunzione>
  <DataCessazione></DataCessazione>
  <Livello></Livello>
</Persona>
```

Unità funzionale

```
<UnitaFunzionale>
  <DataRif></DataRif>
  <Livello></Livello>
  <Cod></Cod>
  <DataInizio></DataInizio>
  <DataFine></DataFine>
  <Descrizione></Descrizione>
  <CodUnitaPadre></CodUnitaPadre>
  <MatricolaResponsabile></MatricolaResponsabile>
  <DescrizioneEstesa></DescrizioneEstesa>
</UnitaFunzionale>
```

Unità funzionale gerarchia

```
<UnitaFunzionaleGerarchia>
  <Cod></Cod>
  <Descrizione></Descrizione>
  <Discendenti>
    <UnitaFunzionaleGerarchia>
      <Cod></Cod>
      <Descrizione></Descrizione>
      <Discendenti>
        ...
      </Discendenti>
    </UnitaFunzionaleGerarchia>
    <UnitaFunzionaleGerarchia>
      <Cod></Cod>
      <Descrizione></Descrizione>
      <Discendenti>
        ...
      </Discendenti>
    </UnitaFunzionaleGerarchia>
    <UnitaFunzionaleGerarchia>
      <Cod></Cod>
      <Descrizione></Descrizione>
      <Discendenti>
        ...
      </Discendenti>
    </UnitaFunzionaleGerarchia>
    ...
  </Discendenti>
</UnitaFunzionaleGerarchia>
```

6.2 Dettaglio delle funzioni

Di seguito si riportano le specifiche delle singole operazioni esposte tramite il web service.

Unità Funzionale

```
UnitaFunzionale DettaglioUnitaFunzionale(
  string codUnita,
  DateTime dataRif
)
```

Carica i dati base di una unità funzionale

```
PersonaCollection ElencaPersoneUnitaFunzionale(
  string codUnita,
  DateTime dataRif
)
```

Elenca le persone assegnate all'unità funzionale


```
CaratteristicaCollection ElencaCaratteristicheUnitaFunzionale(  
    string codUnita,  
    DateTime dataRif  
)
```

Elenca le caratteristiche assegnate all'unità funzionale

```
bool UnitaFunzionaleHaLeCaratteristiche(  
    string codUnita,  
    DateTime dataRif,  
    string[] caratteristiche,  
    bool richiediTutteLeCaratteristiche)
```

Calcola se l'unità funzionale ha le caratteristiche specificate (tutte o almeno una a seconda del valore di 'richiediTutteLeCaratteristiche')

```
UnitaFunzionale UnitaFunzionaleCercaAntenatoConCaratteristiche(  
    string codUnita,  
    DateTime dataRif,  
    string[] caratteristiche,  
    bool richiediTutteLeCaratteristiche,  
    int distanzaMax)
```

Restituisce, se esiste, la prima unità funzionale (tra gli antenati, scorrendoli a ritroso, fino a 'distanzaMax' livelli) che ha le caratteristiche specificate (tutte o almeno una a seconda del valore di 'richiediTutteLeCaratteristiche'). Assegnare -1 a 'distanzaMax' per eseguire la ricerca fino alla radice

```
bool UnitaFunzionaleDiscendeDa(  
    string codUnita,  
    string codUnitaAntenato,  
    DateTime dataRif,  
    int livelloMax  
)
```

Calcola se c'è un legame di parentela con non più di 'livelloMax' livelli. Assegnare -1 a 'livelloMax' per eseguire la ricerca su tutti i livelli possibili

```
bool UnitaFunzionaleFigliaDi(  
    string codUnita,  
    string codUnitaPadre,  
    DateTime dataRif  
)
```

Calcola se un'unità funzionale discende direttamente da un'altra

```
int UnitaFunzionaleCalcolaLivelliParentela(  
    string codUnita,  
    string codUnitaAntenato,  
    DateTime dataRif,  
    int livelloMax  
)
```

Calcola la 'distanza', in 'livelli di parentela', tra una unità funzionale e un suo antenato. Assegnare -1 a 'livelloMax' per eseguire la ricerca su tutti i livelli possibili. Se le due unità non sono parenti o la distanza è maggiore di 'livelloMax' restituisce -1

Gerarchia

```
public UnitaFunzionaleGerarchia UnitaFunzionaleCreaGerarchia(  
    string codUnitaRadice,  
    int livelloMax,  
    DateTime dataRif  
)
```

Crea la gerarchia completa dei discendenti dell'unità con non più di 'livelloMax' livelli di parentela. Assegnare -1 a 'livelloMax' per creare la gerarchia su tutti i livelli possibili

Elenchi

```
UnitaFunzionaleCollection ElencaUnitaFunzionali(  
    DateTime dataRif  
)
```

Elenca le unità funzionali

```
UnitaFunzionaleCollection ElencaUnitaFunzionaliAventiCaratteristiche(  
    DateTime dataRif,  
    string[] caratteristiche,  
    bool richiediTutteLeCaratteristiche  
)
```

Elenca le unità funzionali aventi le caratteristiche specificate (tutte o almeno una a seconda del valore di 'richiediTutteLeCaratteristiche')

```
UnitaFunzionaleCollection ElencaDiscendentiDirettiUnitaFunzionale(  
    string codUnitaRadice,  
    DateTime dataRif  
)
```

Elenca le unità funzionali discendenti direttamente dall'unità funzionale (le "figlie")

```
UnitaFunzionaleCollection ElencaDiscendentiDirettiUnitaFunzionaleAventiCaratteristiche(  
    string codUnitaRadice,  
    DateTime dataRif,  
    string[] caratteristiche,  
    bool richiediTutteLeCaratteristiche  
)
```

Elenca le unità funzionali discendenti direttamente dall'unità funzionale (le "figlie") aventi le caratteristiche specificate (tutte o almeno una a seconda del valore di 'richiediTutteLeCaratteristiche')

```
UnitaFunzionaleCollection ElencaDiscendentiUnitaFunzionale(  
    string codUnitaRadice,  
    int livelloMax,  
    DateTime dataRif  
)
```

Elenca le unità funzionali discendenti dell'unità funzionale con non più di 'livelloMax' livelli di parentela. Assegnare -1 a 'livelloMax' per eseguire la ricerca su tutti i livelli possibili

```
UnitaFunzionaleCollection ElencaDiscendentiUnitaFunzionaleAventi-
    Caratteristiche(
        string codUnitaRadice,
        int livelloMax,
        DateTime dataRif,
        string[] caratteristiche,
        bool richiediTutteLeCaratteristiche
    )
```

Elenca le unità funzionali discendenti dell'unità funzionale con non più di 'livelloMax' livelli di parentela, aventi le caratteristiche specificate (tutte o almeno una a seconda del valore di 'richiediTutteLeCaratteristiche'). Assegnare -1 a 'livelloMax' per eseguire la ricerca su tutti i livelli possibili

```
UnitaFunzionaleGerarchia UnitaFunzionaleCreaGerarchia(
    string codUnitaRadice,
    int livelloMax,
    DateTime dataRif
)
```

Crea la gerarchia completa dei discendenti dell'unità con non più di 'livelloMax' livelli di parentela. Assegnare -1 a 'livelloMax' per eseguire la ricerca su tutti i livelli possibili

Persona

```
Persona DettaglioPersona(
    int matricola,
    DateTime dataRif
)
```

Carica i dati base di una persona

```
bool PersonaIsResponsabileUnitaFunzionale(
    int matricola,
    string codUnita,
    DateTime dataRif
)
```

Calcola se la persona è il responsabile dell'unità funzionale

```
bool PersonaIsAssegnataAUnitaFunzionale(
    int matricola,
    string codUnita,
    DateTime dataRif
)
```

Calcola se la persona è assegnata all'unità funzionale

```
IncaricoCollection ElencaIncarichi(
    int matricola,
    DateTime dataRif)
```

Elenca tutti gli incarichi di una persona.

Allegato 14: Schede tecniche: applicativa e sistemi

SCHEMA TECNICA APPLICAZIONE <nome applicazione>

Dati generali dell'applicazione	
Nome Applicazione	<nome applicazione>
Descrizione sintetica	<sintetica descrizione dell'applicazione>
Tipologia dell'utenza	<Intranet – Extranet - Internet>
Modalità di interazione operatore/applicazione	<applicazione WEB - applicazione client/server - batch - web services misto >
Distribuzione geografica degli accessi all'applicazione	< comunale – provinciale – regionale – nazionale - internazionale>
Filiera tecnologica	<java - microsoft - open source>
Stack tecnologico	<indicare sistema operativo, web server, application server, database server >
Lista componenti SW	<indicare eventuali componenti sw utilizzate dall'applicativo>
Protocolli di trasmissione dati	< HTTP - telnet – ftp>
Sistema di cifratura dati	<indicare se viene usato un sistema di cifratura dei dati e descriverne brevemente le caratteristiche>
Sistema di cifratura delle trasmissioni	< SSH – IPSEC – HTTPS – NO Cifratura>
Aspetti relativi alla criticità dell'applicazione	Indicare eventuali vincoli temporali nelle fasi di aggiornamento/elaborazione dei dati
Modalità di gestione dei files generati e/o utilizzati dall'applicazione	Indicare se vengono memorizzati su file system, su database o sul sistema di gestione documentale

Documentazione applicativa (da allegare alle schede in formato elettronico)	
Descrizione dell'architettura sw dell'applicazione	<descrivere l'architettura sw dell'applicazione>
Descrizione del sistema di sicurezza	<effettuare l'analisi dei rischi e descrivere il sistema di sicurezza da implementare (v. Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna”, approvato con Determinazione del Direttore Generale all'Organizzazione, Personale, Sistemi informativi e Telematica n. 4137 del 2014.). Allegare oppure inviare all'atto della richiesta di attivazione dei test di sicurezza anche la check list compilata e motivata. Solo le appendici B1 e B3 se l'applicazione è ospitata sui server gestiti dal Servizio

	SIIR, anche l'appendice B2 nel caso l'applicazione risieda su private cloud regionale o in hosting esterno>
Organizzazione, struttura e semantica della base dati	<descrivere la struttura della base dati: schema concettuale e schema relazionale>
Descrizione flussi dati	<descrivere eventualmente i flussi dei dati previsti dall'applicazione>
Integrazione con il sistema documentale	<indicare se si integra con il sistema documentale regionale e in caso affermativo allegare le griglie compilate presenti nelle Appendici delle "Linee guida per l'integrazione dei sistemi verticali con il sistema documentale regionale" pubblicato su Internos nella sezione "Il protocollo informatico: il sistema di gestione documentale" (https://internos.regione.emilia-romagna.it/sapere-e-fare/funzionamento/gestione-documentale/il-protocollo-informatico)>
Integrazione con i servizi di firma digitale	<indicare se si integra con i servizi di firma digitale e con quale modalità>
Interazione con altri sistemi/servizi	<elencare i sistemi con cui l'applicazione si interfaccia e con quale modalità >
Procedure di avvio e chiusura dei servizi/applicazioni	<descrivere le sequenze di avvio e stop dei servizi e delle applicazioni considerando anche l'interazione con sistemi ed applicazioni esterne>
Specifiche tecnico/funzionali	<descrivere in maniera dettagliata ogni funzionalità prevista inserendo lo schema di navigazione e/o il prototipo dell'interfaccia/pagine ed eventuali integrazioni con altri sistemi>
Manuale utente ¹	<descrivere il funzionamento dell'applicazione per il suo utilizzo da parte dell'utente finale>
Manuale di installazione, gestione. Descrizione della gestione del versioning dei sorgenti ¹	<descrivere le procedure per installare, configurare e gestire l'applicazione; indicare come viene gestito il versioning dei sorgenti >
Piano di Backup/Restore	<indicare eventuali requisiti particolari di gestione del backup/restore dei dati >
Piano di Disaster Recovery	<indicare se vi è obbligo di un piano di Disaster Recovery>
Continuità Operativa¹	<p><indicare i seguenti requisiti:</p> <ul style="list-style-type: none"> • Tempo massimo tollerabile tra la produzione di un dato e il suo salvataggio (RPO, Recovery Point objective) Possibili valori: 1 ora, 4 ore, 1 giorno, 3 giorni, 1 settimana o più • Tempo massimo tollerabile di indisponibilità del servizio (RTO, Recovery Time Objective) Possibili valori: 1 ora, 4 ore, 1 giorno, 3 giorni, 1 settimana • Principale danno per l'Amministrazione in caso di disservizio: Possibili valori: inadempienza amministrativa, danno economico, inefficienza amministrativa, immagine • L'interruzione blocca un altro servizio: Possibili valori: SI, NO • Livello di danno per l'Amministrazione in caso di disservizio: Possibili valori: alto medio basso trascurabile

¹ Da allegare alla richiesta di rilascio in produzione

¹ Da allegare alla richiesta di rilascio in produzione

¹ Da allegare alla richiesta di rilascio in produzione

	>
Verbale di collaudo ¹	<descrivere i casi di test e l'esito relativi al collaudo dell'applicazione >
Accessibilità ¹	<descrivere la rispondenza dei requisiti di accessibilità, allegando la check list compilata>

Requisiti postazione di lavoro	
OS Certificati	<indicare i s.o. certificati: Vista, Windows 7 (32, 64), etc.>
Browser certificati (in caso di applicazione web)	<indicare i browser certificati, le versioni ed eventuali configurazioni particolari>
Citrix (in caso di applicazione client)	<indicare se può essere installato su piattaforma Citrix>
Moduli software necessari	<nessuno> <applet versione ...> <jvm versione ...> <modulo xxx versione ...> <add-on e/o plugin e/o dll >...
Aggiornamenti	<indicare se è previsto che l'applicazione venga aggiornata per tenere conto degli upgrade dei moduli sw necessari>
Interazioni	<indicare se l'applicazione interagisce con Word, Excel, Open office, ecc. o altri SW installati>

Amministrazione degli Utenti	
Sistema di autenticazione	< UserID/password – Smart card – PKI - ...>
Meccanismo di autenticazione	<indicare se applicativo o se centralizzato (AD, IAM, fedERa). Nel caso di IAM o fedERa compilare le relative tabelle presenti negli Allegati tecnici 9 e 9a, paragrafo 4 e inviarle all'atto della richiesta di deploy in test e in produzione>
Amministrazione e consegna delle credenziali di autenticazione	<verificare, conformemente alle procedure dell'Ente, la consegna delle credenziali di autenticazione ed il loro inserimento nel sistema di gestione dell'Ente>
Livelli di profilazione utenti	<descrivere le modalità di implementazione (applicativo, db, AD, IAM) e le tipologie di profili (amministratore, operatore, etc..)>

Specifiche prestazionali	
Massimo numero indicativo di utenti	<indicare il numero massimo indicativo di utenti >
Massimo numero indicativo di utenti contemporanei	<indicare il numero massimo indicativo di utenti contemporanei >
Dimensione DB	<indicare la dimensione iniziale del DB e la percentuale di crescita annuale>
Movimentazione dei dati	<transazionale/batch e relativa distribuzione temporale >

¹ Da allegare alla richiesta di rilascio in produzione

¹ Da allegare alla richiesta di rilascio in produzione

SLA applicativo	
Orario di servizio (specificarlo per ogni componente dell'applicazione, ad esempio: back office, front-office)	<Giorni alla settimana nei quali viene utilizzato il servizio: esempio, 5gg su 7gg oppure 7gg su 7gg > <Ore al giorno nelle quali viene utilizzato il servizio: esempio, 8/24 oppure 12/24 oppure 24/24>

Manutenibilità Software Applicativo (compilare nel caso di prodotti con licenza)	
License Key	
Software Subscription Key	
Software Subscription Scadenza	< gg/mm/aaaa >
Tipologia Licenza	<limitata/illimitata>
Escalation Path per problemi Software	< telefono – e-mail – web application >

FTPS (compilare solo nel caso serva attivare il servizio per l'invio del codice)				
Cognome	Nome	e-mail	telefono	Interno/ esterno

Contatti	
Struttura regionale committente	<indicare la struttura regionale che ha commissionato l'applicazione>
Referente utente regionale dell'applicazione	<indicare cognome, nome, tel., mail>
Referente tecnico regionale dell'applicazione	<indicare cognome, nome, tel., mail>
Referente tecnico del fornitore dell'applicazione	<indicare azienda, cognome, nome, tel., mail>

SCHEMA TECNICA DEI SISTEMI PER L'APPLICAZIONE <nomeapplicazione> ¹

Dati Generali	
Nome Sistema	<nome sistema>
Appartenza Dominio Regione	<SI/NO>
Sistema dedicato	<SI/NO>
IP Address	<indirizzo IP >
Funzionalità – Servizio	<Sintetica descrizione del servizio fornito dal sistema>
Dislocazione Fisica	<Edificio, stanza, rack, ecc.>
Lista del Software installato	<Lista componenti S.O. e applicative e relative versioni >
System Owner	< Amministratore del sistema >

Manutenzione Hardware	
Serial Number	< numero di serie >
Model Type	< marca, tipo e modello >
Fornitore Contratto	< Generalità del fornitore/produttore del sistema >
Tipologia Contratto (8x7, 24 x7, 4 ore)	< Formula contrattuale per l'assistenza hardware in caso di problemi >

Amministrazione degli Utenti			
Utenti O.S	Username	Gruppo	Ruolo/Funzione

Documentazione da allegare	
Architettura - Diagramma fisico del network con, componenti di interconnessioni e.g. switch e router (e area di gestione) e relative porte	< Documento che descrive gli elementi di infrastruttura del sistema dal punto di vista del networking) >
Architettura - Diagramma logico dell'infrastruttura con flussi, DMZ, indirizzi IP	< Documento che descrive il disegno logico delle applicazioni installate nell'ambito dell'infrastruttura complessiva >
Custom script che girano automaticamente, e non, sul	< Documento che descrive le funzionalità degli script >

¹ da compilare unicamente in caso di porting da sistemi hardware pre-esistenti o nuovi progetti che prevedono l'acquisizione di hardware.

sistema	
Soluzione di Backup	< Documento che descrive la soluzione adottata >
Piano di ripristino	< Documento che descrive l'eventuale piano di ripristino >
Standby hardware	<Elencare eventuali componenti hardware per emergenze>

Profilo Hardware	
Modello Macchina	
Modello CPU	
Clock CPU	
Memoria fisica	
Configurazione array dischi	
Configurazione volume logici	

Sistema Operativo	
Nome e Version del Sistema Operativo	
Patch o Service Pack installati	

Interfacce di rete							
Nome	IP	Subnet	Speed	Duplex	Switch	Port	Vlan
eth1c0	down	<subnet>	Fast Ethernet	Full Duplex	<switch nome>	<switch port>	<vlan no.>
eth2c0	xxx.xxx.xxx.xxx	xx	Fast Ethernet	Full Duplex	<switch nome>	x	x

DNS		
Hostname	IP	Ruolo
<Non Presente>		<Primario/Secondario>

Accesso Remoto	
RDP	<ip1>

SSH	<ip1>
-----	-------

Software Installati (per ogni software installato compilare almeno le prime 4 voci)	
Versione	
Build Number	
Patch installati	
Directory di installazione	
Licenza, specificare se locale o centrale	
Eventuale Indirizzo IP della Management	
Lista delle features che non sono standard ma utilizzate	
Clustering	

Manutenibilità Sistema Operativo e Servizi (compilare per ogni servizio installato)	
License Key	
Software Subscription Key	
Software Subscription Scadenza	
Tipologia Licenza	<limitata/illimitata>

Allegato 15: Livelli di servizio

1	Introduzione	1
2	Cooperazione applicativa	1
2.1	Soggetti	1
2.2	Modalità di funzionamento e SLA.....	1
3	fedERa.....	3
3.1	Soggetti	3
3.2	Modalità di funzionamento e SLA.....	3

1 Introduzione

Scopo di questo documento è quello di regolamentare i livelli di servizio nei rapporti tra la Regione e le società partecipate.

2 Cooperazione applicativa

2.1 Soggetti

Lepida SpA

Servizio Sistema Informativo-Informatico Regionale (SIIR)

Direzioni, Agenzie regionali, Assemblea Legislativa (D&A)

2.2 Modalità di funzionamento e SLA

L'intervento di Lepida SpA richiesto e previsto nello sviluppo di nuove applicazioni in cooperazione applicativa, riguarda esclusivamente l'Accordo di Servizio. Si possono distinguere tre fasi in cui può esprimersi la relazione tra i soggetti:

- Fase A – Progettazione, realizzazione e implementazione in ambiente di test dell'Accordo di Servizio;
- Fase B - Passaggio in produzione dell'Accordo di Servizio
- Fase C - Esercizio dell'Accordo di Servizio

Inoltre è necessario distinguere le 2 situazioni di contesto che possono verificarsi in pratica:

- 1 Situazione ordinaria
- 2 Situazione d'urgenza / Applicazioni critiche

	Fase A	Fase B	Fase C
Ordinaria	<p>D&A contatta SIIR che, a pianificazione avvenuta, contatta LepidaSpA con congruo preavviso (almeno 10 giorni lavorativi) per la configurazione in ambiente di test dell'accordo di servizio.</p> <p>D&A effettua i collaudi preliminari al passaggio in produzione comunicando al SIIR gli esiti.</p>	<p>D&A, solo a conclusione del collaudo con esito positivo, contatta SIIR con congruo preavviso (almeno 10 giorni lavorativi prima del passaggio in produzione).</p> <p>Lepida SpA, attivata dal SIIR, si impegna a configurare l'Accordo di Servizio in ambiente di produzione entro 5 giorni lavorativi,</p> <p>D&A effettua il collaudo in produzione, comunicando al SIIR gli esiti.</p>	<p>A fronte di malfunzionamenti D&A contatta contemporaneamente SIIR e LepidaSpA, ognuno dei quali, possibilmente in sinergia, ne esplora le possibili cause e provvede alla risoluzione entro 16 ore lavorative (a meno di interventi complessi sul software)</p>
Urgenza /Applicazioni critiche /guasto bloccante	<p>D&A contatta SIIR che, a pianificazione avvenuta, contatta LepidaSpA con congruo preavviso (almeno 4 giorni lavorativi) per la configurazione in ambiente di test dell'accordo di servizio.</p> <p>D&A effettua i collaudi preliminari al passaggio in produzione, comunicando al SIIR gli esiti.</p>	<p>D&A, solo a conclusione del collaudo con esito positivo, contatta SIIR con congruo preavviso (almeno 4 giorni lavorativi prima del passaggio in produzione).</p> <p>Per la configurazione in ambiente di produzione dell'Accordo di Servizio, SIIR contatta LepidaSpA con preavviso di almeno 2 giorni lavorativi; D&A effettua i collaudi e ne comunica gli esiti al SIIR.</p>	<p>A fronte di malfunzionamenti D&A contattano contemporaneamente SIIR e LepidaSpA, ognuno dei quali, possibilmente in sinergia, ne esplora le possibili cause e provvede alla risoluzione entro 8 ore lavorative (a meno di interventi complessi sul software)</p>

SIIR e LepidaSpA devono poter disporre di tutte le informazioni necessarie. Per tale motivo, D&A deve allegare alla richiesta i moduli compilati (Allegato 12 - Scheda tecnica per nuovo servizio da erogare o fruire tramite Porta di Dominio IcarER) con tutte le informazioni necessarie per permettere la configurazione dell'accordo di servizio. I valori temporali per gli SLA sono al netto del tempo necessario a D&A per fornire ulteriori informazioni, documentazione mancante o chiarimenti su aspetti inizialmente non specificati.

In fase A e B SIIR decide, per l'applicazione in oggetto, se si applicano le condizioni ordinarie o di urgenza e ne dà comunicazione sia a Lepida SPA che a D&A, che dovrà attenersi a tale classificazione nelle comunicazioni previste nelle fasi successive.

In fase A, le comunicazioni sono inviate dalla D&A al SIIR: Inxadmins@regione.emilia-romagna.it e in cc a mailsistema@regione.emilia-romagna.it riportando in oggetto "CONFIGURAZIONI ICAR-ER per D&A + nome servizio" e specificando nel testo se si tratta di condizioni di Urgenza /Applicazioni critiche.

In fase B, le comunicazioni sono inviate dalla D&A al SIIR:, Inxadmins@regione.emilia-romagna.it e in cc a mailsistema@regione.emilia-romagna.it riportando in oggetto

“PASSAGGIO IN PRODUZIONE ICAR-ER + nome servizio” e specificando nel testo la data in cui il servizio dovrà essere in produzione.

In fase C, le comunicazioni sono inviate dalla D&A al SIIR ed a Lepida: Helpdesk@lepida.it Inxadmins@regione.emilia-romagna.it e in cc a: gruppo-icar@lepida.it e a mailsistema@regione.emilia-romagna.it riportando in oggetto “INCIDENT ICAR-ER + nome servizio” e specificando nel testo se si tratta di guasto bloccante o malfunzionamento grave.

Si evidenzia che relativamente alla fase A, dopo la prima attività di configurazione è ragionevole aspettarsi (nella fase di testing del servizio) un cospicuo scambio di mail tra D&A, SIIR e Lepida SpA; per tale casistica si rientra nelle specifiche della fase C per cui lo scambio avverrà contemporaneamente tra i 3 soggetti coinvolti. E' disponibile anche il servizio di help desk telefonico al numero +39 051 633 88 33

Gli orari di servizio ordinari dell'help desk Lepida sono: dal lunedì al venerdì dalle ore 08:30 alle ore 18:30. il sabato dalle ore 08:30 alle ore 13:30. Poiché il presidio del SIIR non è attivo il sabato, le segnalazioni saranno prese in carico a partire dalle ore 8 del lunedì successivo.

Per disfunzioni al di fuori degli orari di servizio ordinari dell'help desk sarà a breve attivo un servizio di monitoraggio per il ripristino dei sistemi, come estensione del servizio attualmente attivo per le reti.

3 fedERa

3.1 Soggetti

Lepida SpA

Servizio Sistema Informativo-Informatico Regionale (SIIR)

Direzioni, Agenzie regionali, Assemblea Legislativa (D&A)

3.2 Modalità di funzionamento e SLA

Scopo di questo paragrafo è quello di regolamentare i livelli di servizio nei rapporti fra la Regione e la società Lepida spa per la gestione dei malfunzionamenti che riguardano l'autenticazione federata nella fase di esercizio per le applicazioni che risiedono sull'infrastruttura regionale che utilizzano il sistema di autenticazione federata fedERa secondo le specifiche dell'Allegato 9a.

I livelli di servizio normati riguardano esclusivamente i sistemi che concorrono all'erogazione del servizio dell'autenticazione federata fedERa gestiti rispettivamente da SIIR e da Lepida SpA. In particolare:

- Sistemi SIIR: IdP e Service provider della Regione Emilia-Romagna (AM – Access Manager)
- Sistemi Lepida SpA: Gateway e IdP di Enti che ne hanno affidato la gestione a Lepida Spa

Nella definizione degli SLA si distinguono 2 situazioni di contesto che possono verificarsi in pratica:

- 1 Situazione ordinaria
- 2 Situazione d'urgenza / Guasto bloccante

Ordinaria	A fronte di malfunzionamenti la D&A contatta il SIIR, il quale, ne esplora le possibili cause e arriva all'individuazione della causa entro 8 ore lavorative . Nel caso il malfunzionamento fosse da imputare a sistemi in gestione al SIIR, il SIIR provvede alla risoluzione entro altre 8 ore lavorative (a meno di interventi complessi sul software). Nel caso il malfunzionamento fosse da imputare ai sistemi in gestione a Lepida SpA, il SIIR contatta Lepida Spa, la quale provvede: <ul style="list-style-type: none">• alla risoluzione entro altre 8 ore lavorative (a meno di interventi di manutenzione correttiva sul software), in caso di malfunzionamento sui propri sistemi;• a contattare l'help desk di un Ente terzo nel caso di malfunzionamento ad un IdP gestito esternamente.
Urgenza /guasto bloccante	A fronte di malfunzionamenti D&A contatta contemporaneamente SIIR e LepidaSpA, ognuno dei quali, possibilmente in sinergia, ne esplora le possibili cause e provvede: <ul style="list-style-type: none">• alla risoluzione entro altre 8 ore lavorative (a meno di interventi di manutenzione correttiva sul software), in caso di malfunzionamento sui propri sistemi;• a contattare l'help desk di un Ente terzo nel caso di malfunzionamento ad un IdP.gestito esternamente.

SIIR e LepidaSpA devono poter disporre di tutte le informazioni necessarie. Per tale motivo, D&A deve allegare alla richiesta il modulo compilato (Allegato 9a, paragrafo 4) con tutte le informazioni necessarie. I valori temporali per gli SLA sono al netto del tempo necessario a D&A per fornire ulteriori informazioni, documentazione mancante o chiarimenti su aspetti inizialmente non specificati.

Le comunicazioni sono inviate dalla D&A al SIIR: servicedesk@regione.emilia-romagna.it ed, in caso di situazione d'urgenza o critica guasto bloccante, anche Lepida: Helpdesk@lepida.it servicedesk@regione.emilia-romagna.it riportando in oggetto "INCIDENT fedERa + nome servizio" e specificando nel testo se si tratta di guasto bloccante o meno.

Allegato 16: Cookie: normativa e istruzioni operative

1	<i>Introduzione e finalità del documento</i>	2
2	<i>Normativa di riferimento</i>	2
3	<i>Cookie, tipologie e definizioni</i>	3
4	<i>Editori e terze parti</i>	4
4.1	<i>Cookie tecnici e analitici di prima parte con elaborazione di dati in forma aggregata</i>	4
4.2	<i>Cookie di terze parti</i>	5
4.2.1	<i>Sito che non ospita pubblicità mirata</i>	5
4.2.2	<i>Sito che ospita pubblicità mirata</i>	5
4.2.2.1	<i>Cookie analytic di terze parti</i>	5
4.2.2.2	<i>I social plugin e i cookie di profilazione</i>	6
5	<i>Informativa e consenso</i>	6
5.1	<i>Contenuto obbligatorio del banner</i>	6
5.2	<i>L'informativa estesa</i>	7
6	<i>I cookie di profilazione – obbligo di notificazione</i>	7
7	<i>Istruzioni operative</i>	8
8	<i>Istruzioni per la corretta implementazione dei cookie nell'interazione con gli utenti</i>	8
9	<i>Sinottico adempimenti per utilizzo cookie</i>	9
	<i>Appendice A. Fac-simile di privacy&cookie policy</i>	9
	<i>Appendice B. Fac-simile banner</i>	15
	<i>Appendice B.1. Banner senza richiesta di consenso</i>	15
	<i>Appendice B.2. Banner con richiesta di consenso</i>	15
	<i>Appendice C. Fac-simile clausola di contratto per fornitori esterni</i>	16

Introduzione e finalità del documento

L'art. 122 del Codice in materia di protezione dei dati personali ha recepito la norma dell'art. 5, paragrafo 3, della direttiva 2002/58/CE, come modificato dalla direttiva 2009/136/CE, con la quale è stato previsto l'obbligo del consenso informato prima dell'archiviazione di informazioni o dell'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente.

E' necessario sottolineare che tale normativa espande il proprio ambito di applicazione a tutte le tipologie di informazioni sottoposte ad archiviazione o ad accesso nell'apparecchiatura terminale dell'utente. Quindi la suddetta disposizione concerne non solo i cookie ma tutte le tecnologie che presentino tali caratteristiche tecniche.

Il presente documento assume la finalità di compiere un'esegesi delle norme che dispongono in materia di cookie e di fornire istruzioni operative per i webmaster.

Normativa di riferimento

- Direttiva 2002/58/CE del 12 luglio 2002, del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (<http://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:32002L0058>);
- Direttiva 2009/136/CE del 25 novembre 2009, del Parlamento europeo e del Consiglio, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori (<http://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:32009L0136>);
- Decreto legislativo 28 maggio 2012, n. 69 "Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori" (pubblicato nella Gazzetta Ufficiale del 31 maggio 2012 n. 126) (<http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2012-05-28;69>);
- Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice") e, in particolare, gli artt. 13, comma 3 e 122, comma 1 (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248>);
- Provvedimento del Garante per la protezione dei dati personali dell'8 maggio 2014 "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie" (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884>);
- Faq in materia di Cookie del Garante per la protezione dei dati personali (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2142939>);
- Informativa e consenso per l'uso dei cookie "Domande più frequenti" del Garante per la protezione dei dati personali (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3585077>);
- Opinione 4/2012 del Gruppo di lavoro per la tutela dei dati personali ex art. 29, adottata il 7 giugno 2012 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_it.pdf);
- Chiarimenti del Garante per la protezione dei dati personali del 5/6/2015 (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4006878>);

Cookie, tipologie e definizioni

Sono molteplici i cookie che vengono memorizzati nei terminali degli utenti, e, spesso, di ardua classificazione.

L'elenco di seguito riportato, mutuato dall'opinione n. 4/2012 del Gruppo di lavoro per la tutela dei dati personali ex art. 29, ha carattere meramente esemplificativo e non esaustivo:

1. Cookie tecnici	Sono quelli utilizzati <u>al solo fine</u> di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente di erogare tale servizio
1.1 Cookie Analytic	Sono quelli utilizzati soprattutto dai gestori di siti web per stimare il numero di visitatori unici, al fine di individuare le principali parole chiave per i motori di ricerca che portano a una pagina web oppure per individuare le problematiche di navigazione di un sito web. Sono assimilati ai cookie tecnici laddove siano realizzati e utilizzati direttamente dal sito prima parte (senza, dunque, l'intervento di soggetti terzi) ed elaborati in forma aggregata.
1.2 User input cookie ¹	Sono i cookie utilizzati per tenere traccia dei dati compilati dall'utente in una serie di messaggi scambiati con un prestatore di servizi in maniera coerente.
1.3 Authentication cookie	sono utilizzati per identificare l'utente negli accessi successivi dopo il primo login.
1.4 User centric security cookie	Sono quelli predisposti allo scopo specifico di accrescere la sicurezza del servizio esplicitamente richiesto dall'utente (es. login falliti)
1.5 Multimedia player session cookie	sono utilizzati per archiviare dati tecnici necessari alla riproduzione di contenuti video o audio (ad es. qualità video)
1.6 Load balancing cookie	Sono quelli che consentono di distribuire il trattamento delle richieste su un server web tra vari apparecchi anziché in uno solo.
1.7 User interface customization cookie	sono utilizzati per archiviare una preferenza in merito a un servizio nelle varie pagine web (ad es. lingua) e non sono connessi ad altri codici identificativi persistenti come il nome utente

¹ Dall'1.2 all'1.8 trattasi di cookie di funzionalità assimilati a quelli tecnici perché atti a fornire un servizio richiesto dall'utente.

1.8 Social plug-in content sharing cookie	Sono i plug-in che archiviano e accedono ai cookie nell'apparecchiatura terminale dell'utente al fine di consentire alla rete sociale di individuare i membri quando interagiscono con detti plug-in, consentendo agli utenti delle reti sociali di condividere contenuti a loro graditi con i loro "amici" (e proporre altre funzionalità connesse come la pubblicazione di commenti)
2. Cookie di profilazione	Sono volti a creare profili relativi all'utente e vengono utilizzati al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dallo stesso nell'ambito della navigazione in rete
2.1 Social plug-in tracking cookie	utilizzati per monitorare gli utenti, membri o meno, con cookie di terzi per finalità quali, ad esempio, la pubblicità, l'analitica e le indagini di mercato a carattere comportamentale
2.2 Third party advertising	Sono i cookie di terzi utilizzati per la pubblicità comportamentale

Editori e terze parti

La differenziazione soggettiva proposta dal Provvedimento del Garante per la protezione dei dati personali dell'8 maggio 2014 è effettuata considerando quale soggetto installa i cookie sul terminale dell'utente: o lo stesso gestore del sito che l'utente sta visitando (c.d. "editore") o di un sito diverso che installa cookie per il tramite del primo (c.d. "terze parti").

La distinzione tra i due soggetti è rilevante in ordine agli oneri che discendono dall'installazione dei predetti cookie.

L'onere di adempimento alla normativa è, quindi, prevista in capo all'Editore del sito. Nell'ordinamento regionale tale ruolo si assume in capo al Responsabile del Procedimento di pubblicazione dei contenuti che, in genere, coincide con il Responsabile del trattamento dei dati personali, ai sensi della Delibera di Giunta Regionale n. 2416/2008 – Appendice 5.

Di seguito, vengono fornite alcune indicazioni con riferimento alle diverse tipologie di cookie utilizzabili in stretta connessione con l'evenienza che il sito ospiti pubblicità mirata.

Cookie tecnici e analitici di prima parte con elaborazione di dati in forma aggregata

Nel caso in cui l'editore utilizzi cookie tecnici e analitici di prima parte con elaborazione di dati in forma aggregata, non è necessario lo specifico consenso preventivo dell'utente -limitatamente all'utilizzo da parte dell'editore di tali cookie-, anche nel caso il sito ospiti pubblicità mirata.

Per i gestori dei siti è sufficiente fornire tutte le informazioni di cui al paragrafo 5, senza onere di implementare banner o soluzioni similari.

Nei casi in cui, invece, i cookie analytic di prima parte elaborino le informazioni relative agli utenti e alla loro navigazione in modalità chiara ed estesa, ricadono, conseguentemente, nell'alveo dei cookie di profilazione, cui conseguono oneri e adempimenti di cui al par. 6 del presente documento.

Cookie di terze parti

4.2.1.1 Sito che non ospita pubblicità mirata

Uno degli elementi di assoluto rilievo, rappresentato, per la prima volta, nell'ultimo capoverso del par. 4 dei "Chiarimenti in merito all'attuazione della normativa in materia di cookie" (docweb n. 4006878) pubblicati dal Garante il 5 giugno 2015, è che, in tema di cookie di terze parti, *"l'obbligo di rendere l'informativa e acquisire il consenso nasce dalla scelta del sito di ospitare pubblicità mirata basata sulla profilazione degli utenti tramite i cookie, in luogo di quella generalista offerta indistintamente a tutti"*.

Conseguentemente, nei casi in cui il sito non ospiti pubblicità mirata, non è necessario fornire agli utenti le informazioni prescritte dal Provvedimento del Garante dell'8 maggio 2014 "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie".

Pertanto, i siti degli Enti pubblici, che presumibilmente non ospitano pubblicità né generalista né tantomeno mirata, non sono onerati, con riferimento ai cookie di terze parti, ad adempiere agli obblighi di informazione e consenso.

4.2.1.2 Sito che ospita pubblicità mirata

4.2.2.1 Cookie analytic di terze parti

In tutti i casi in cui il sito ospiti pubblicità mirata basata sulla profilazione tramite cookie, il gestore del sito che utilizza cookie analytic di terza parte deve:

- fornire solo l'informativa se
 - adotta strumenti idonei a ridurre il potere identificativo dei cookie analitici (ad esempio, mediante il mascheramento di porzioni significative dell'indirizzo IP)
 - e
 - la terza parte si impegna a non incrociare le informazioni contenute nei cookie con altre di cui già dispone
- recepire il consenso preventivo degli utenti se
 - non è rispettata anche solo una delle due condizioni sopra indicate, poiché, in tali casi, dovranno essere considerati quali cookie di profilazione. Sorge, quindi, in capo al gestore del sito (editore) l'obbligo di predisporre il banner, fornire un'informativa estesa contenente i riferimenti agli analytic di terza parte e recepire, e documentare, il consenso degli utenti.

All'obbligo di predisporre il banner corrisponde, pertanto, l'onere di bloccare l'invio di tali cookie prima dell'accettazione da parte dell'utente.

4.2.2.2 I social plugin e i cookie di profilazione

Il Garante ha chiarito che se sul sito i banner pubblicitari o i collegamenti con i social network consistono in semplici link a siti terze parti che non installano cookie di profilazione, non è necessario fornire né informativa né consenso.

Inoltre, se si tratta di meri plugin di condivisione, è necessario recepire il consenso preventivo dell'utente solo nei casi in cui lo stesso non sia loggato sul social.

Il plugin di condivisione infatti, nell'interazione con un utente loggato al social, ricadrebbe nell'esenzione dal consenso poiché servizio richiesto dall'utente (Criterio di esenzione B Opinione 4/2012 Gruppo Art. 29). Rimane da valutare la percorribilità tecnica di tale soluzione.

In tutti gli altri casi, e con riferimento anche ai cookie di profilazione di terze parti, il gestore del sito deve predisporre il banner, che genera l'evento idoneo a rendere il consenso documentabile, e indicare i link aggiornati ai siti gestiti dalle terze parti, in cui l'utente potrà effettuare le proprie scelte in merito alle categorie e ai soggetti da cui ricevere cookie di

profilazione. Anche in questi casi è necessario bloccare l'invio dei cookie delle terze parti (per es. evitando di caricare il plugin) finché l'utente non abbia prestato il suo consenso.

Informativa e consenso

Qualora necessario, all'utente che accede a un sito web deve essere presentata una prima informativa "breve", contenuta in un banner a comparsa immediata, in ogni pagina del sito, che deve essere somministrato in discontinuità netta rispetto alla fruizione della pagina web visitata.

La richiesta di consenso all'uso dei cookie, qualora necessaria, deve essere inserita nello stesso banner contenente l'informativa breve. Dei consensi rilasciati dagli utenti è necessario tenere traccia, ad esempio, avvalendosi di un apposito cookie tecnico.

Nel banner deve essere linkata l'informativa estesa con la quale all'utente sono fornite più dettagliate informazioni e dove lo stesso potrà differenziare le proprie scelte in merito ai diversi cookie archiviati tramite il sito visitato. Ad ogni modo all'utente deve essere riconosciuto il diritto di negare il consenso ai cookie.

Le modalità di somministrazione dell'informativa breve agli utenti non sono disposte obbligatoriamente dalla normativa, tanto che il gestore del sito può elaborare modalità tecniche differenti rispetto al modello prospettato dal Garante.

Deve essere, infine, sottolineato che ogniqualvolta si installa un nuovo cookie o un cookie già presente viene utilizzato con finalità differenti rispetto a quelle indicate nell'informativa per il trattamento dei dati personali già somministrata, sarà necessario recepire nuovamente il consenso, tracciando tale operazione per mezzo di un nuovo (e diverso) cookie tecnico.

Per un'analisi maggiormente dettagliata della casistica si rinvia agli allegati in calce al presente documento.

Contenuto obbligatorio del banner

Il contenuto del banner è disciplinato dal succitato Provvedimento del Garante.

Specificatamente deve essere indicato:

- che il sito internet utilizza cookie di profilazione al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete,
- che il sito internet consente anche l'invio di cookie "terze parti",
- il link all'informativa estesa,
- l'indicazione che alla pagina dell'informativa estesa è possibile negare il consenso all'installazione dei cookie,
- l'indicazione che la prosecuzione della navigazione mediante accesso ad altra area del sito o selezione di un elemento dello stesso (ad esempio, di un'immagine o di un link) comporta la prestazione del consenso all'uso dei cookie.

L'informativa estesa

L'informativa estesa deve contenere alcune informazioni obbligatorie:

- le finalità e le modalità del trattamento cui sono destinati i dati personali degli utenti,
- la natura obbligatoria o facoltativa del conferimento dei dati e le conseguenze di un eventuale rifiuto di rispondere,

- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi,
- i diritti di cui all'articolo 7,
- gli estremi identificativi del titolare e dei responsabili.

All'interno dell'informativa estesa, per ciò che concerne i cookie, è necessario:

- descrivere analiticamente finalità e caratteristiche di tutti i cookie utilizzati.
- indicare se il sito utilizza cookie di terze parti e inserire il link aggiornato alle informative e ai moduli di consenso delle terze parti (se non si hanno contatti diretti con le terze parti, devono essere linkati i siti degli intermediari).
- indicare all'utente le modalità di disabilitazione dei cookie, ivi comprese le impostazioni del browser che permettono allo stesso di manifestare le proprie opzioni in merito ai cookie (inserendo anche un collegamento diretto con la sezione del browser dedicato alle impostazioni di base).

I cookie di profilazione – obbligo di notificazione

Per cookie di profilazione si intendono i cookie volti a creare profili degli utenti in base ai gusti, abitudini, scelte ecc. ed utilizzati al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dallo stesso nell'ambito della navigazione in rete.

Il cardine interpretativo è la Titolarità del trattamento di profilazione finalizzata alla pubblicità mirata. Nell'eventualità che l'utilizzo di tale tipologia di cookie debba ravvisarsi in capo all'editore, ivi compresa la finalità di pubblicità mirata, oltre alla informativa sul trattamento dei dati personali (sia in forma sintetica -banner- sia in forma estesa) e alla richiesta di consenso, sorge, in capo allo stesso, l'obbligo di notificazione al Garante di tale trattamento di dati personali ai sensi dell'art. 37, comma 1, lett. d), del Codice, laddove lo stesso sia finalizzato a *"definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti"*.

Cos'è la notificazione?

E' una dichiarazione con la quale un soggetto pubblico o privato rende nota al Garante l'esistenza di un'attività di raccolta e di utilizzazione dei dati personali, svolta quale autonomo titolare del trattamento.

Tale notifica è trasmessa al Garante, telematicamente tramite il sito internet istituzionale, prima che inizi il trattamento e una sola volta, indipendentemente dalla durata, dal tipo e dal numero delle operazioni di trattamento, sia che si effettui un solo trattamento, sia che si curino più attività di trattamento con finalità correlate tra loro. Ciò comporta che, come chiarito inoltre dal Garante, che per coloro che gestiscono più siti web è possibile di effettuare una sola notificazione per tutti i diversi siti web amministrati, indicando tutti i domini nei quali il trattamento effettuato attraverso i cookie si realizza con l'onere di mantenerne aggiornato costantemente l'elenco.

Istruzioni operative

L'onere di adempimento alla normativa è prevista in capo all'Editore del sito. Nell'ordinamento regionale tale ruolo si assume in capo al Responsabile del Procedimento di pubblicazione dei contenuti che, in genere, coincide con il Responsabile del trattamento dei dati personali, ai sensi della Delibera di Giunta Regionale n. 2416/2008 – Appendice 5.

L'Editore del sito, al momento della pubblicazione e ogniqualvolta il sito venga aggiornato, deve:

1. Censire tutti i cookie non di terze parti installati dal sito e verificarne le finalità
2. Censire tutti i cookie installati da terze parti
3. Predisporre l'informativa
3.1 Descrivere per ciascun cookie le finalità e le caratteristiche (permanenti, di sessione, se esente da consenso, ecc.)
3.2 Acquisire i link a informative e moduli di consenso delle terze parti
4. Predisporre, qualora necessario, il banner con l'informativa semplificata

Istruzioni per la corretta implementazione dei cookie nell'interazione con gli utenti

1. E' possibile installare i cookie tecnici (anche di funzionalità) sul terminale dell'utente, sin dal suo primo accesso
2. E' necessario bloccare i cookie di terze parti prima che l'utente abbia prestato il suo consenso, nell'eventualità che il sito ospiti pubblicità mirata
3. Le preferenze espresse dall'utente devono essere memorizzate in un cookie tecnico inviato sul terminale dello stesso
4. Nei successivi accessi al sito un cookie tecnico verificherà se l'utente è alla prima visita e quali preferenze ha espresso
5. Se l'utente fornisce il proprio consenso ai cookie non tecnici, nei successivi accessi non dovrà essergli mostrato il banner con informativa breve e consenso
6. L'utente può esprimere il consenso in diverse modalità: cliccando su ok (o accetto) all'interno del banner, cliccando su uno dei link attivi della pagina, o anche solo con il semplice "scroll" della stessa.
7. Se l'utente non esprime alcuna preferenza il banner sarà riproposto

Sinottico adempimenti per utilizzo cookie

	Informativa estesa	Informativa semplificata / consenso preventivo	Notifica al Garante
Sito con cookie tecnici e analytic esenti propri	Si	No	No
Sito che non ospita pubblicità mirata e che utilizzi cookie tecnici e analytic di terza parte	Si	No	No
Sito che ospita pubblicità mirata e che utilizzi cookie tecnici e analytic di terza parte	Si	Si	No

Sito con cookie tecnici, analytic e di profilazione dell'editore	Si	Si	Si
--	----	----	----

Appendice A. Fac-simile di privacy&cookie policy

Premessa

In questo documento sono descritte le regole di gestione del portale istituzionale della Regione Emilia-Romagna, con specifico riferimento al trattamento dei dati personali dei navigatori che lo consultano.

La Regione Emilia-Romagna si impegna a rispettare e a proteggere la vostra riservatezza trattando i dati personali da voi forniti nel rispetto delle disposizioni di legge atte a garantire la sicurezza, l'esattezza, l'aggiornamento e la pertinenza dei dati rispetto alle finalità dichiarate. I dati personali forniti dagli utenti che inoltrano richieste sono utilizzati al solo fine di dare esecuzione alla richiesta di volta in volta inoltrata, e sono comunicati a terzi nel solo caso in cui ciò sia strettamente necessario e funzionale a tale finalità, nel rispetto delle specifiche informative rese ai sensi dell'**art. 13 D.lgs. 196/03**. I dati sono trattati da personale appositamente incaricato al trattamento dei dati, solo qualora il trattamento sia necessario allo svolgimento delle mansioni assegnate.

Titolare del trattamento dei dati

Il titolare del trattamento dei dati personali è la Regione Emilia-Romagna con sede in Bologna (Italia), Viale Aldo Moro, n. 52 - CAP 40127.

Modalità del trattamento

I dati personali sono trattati con strumenti elettronici per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti.

Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

Facoltatività del conferimento dei dati

A parte quanto di seguito specificato per i dati di navigazione, l'utente è libero di fornire i dati personali necessari al fine di dare esecuzione alle sue specifiche richieste. Il loro mancato conferimento può comportare l'impossibilità di ottenere quanto richiesto.

Per completezza va ricordato che in alcuni casi (non oggetto dell'ordinaria gestione di questo sito), gli organi giudiziari possono richiedere alcuni tipi di dati. In questo caso ovviamente la comunicazione da parte dell'Ente ai predetti organi risulta obbligatoria.

Dati acquisiti durante la navigazione

I sistemi informatici e le procedure software preposte al funzionamento dei siti web dell'Ente acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti. In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la

dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

I dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni del sito: salva questa eventualità, i dati sui contatti web persistono per un tempo non superiore a quello necessario agli scopi per i quali essi sono raccolti e successivamente trattati.

Dati forniti volontariamente dall'utente

L'invio facoltativo, esplicito e volontario di messaggi di posta elettronica agli indirizzi indicati su questo sito comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella stessa richiesta. La registrazione facoltativa, esplicita e volontaria tramite appositi moduli web (form) presenti sul nostro sito comporta la successiva acquisizione di tutti i dati riportati nei campi compilati dall'utente ed il trattamento, conformemente a quanto riportato nelle specifiche informative riportate per ogni singolo form, è effettuato esclusivamente in adempimento di attività istituzionali proprie dell'Ente.

Cookie policy

Cosa sono e per quali finalità sono raccolti

Un "cookie" è un piccolo file di testo creato da alcuni siti web per immagazzinare informazioni sul computer dell'utente al momento in cui questo accede al sito. I cookie sono inviati da un server web al browser dell'utente e memorizzati sul computer di quest'ultimo; vengono, quindi, re-inviati al sito web al momento delle visite successive.

Tipologie di cookie utilizzati

Il portale istituzionale della Regione Emilia-Romagna non utilizza cookie di profilazione: nessun dato personale raccolto dalla Regione Emilia-Romagna durante la navigazione degli utenti viene utilizzato per inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente durante la navigazione in rete.

1) Cookie tecnici e di funzionalità

Sono i cookie necessari a permettere la navigazione nei siti istituzionali dell'Ente e per utilizzare diverse funzioni e servizi richiesti dagli utenti.

L'utilizzo di tali cookie permette all'Ente, ad esempio, di accrescere la sicurezza del servizio richiesto dall'utente bloccando l'accesso a seguito di ripetuti login falliti da un'area riservata, oppure a ricordare la preferenza, ad esempio la lingua, in merito alle pagine web visitate.

2) Cookie analytic di prima parte

Il portale si avvale di cookie analitici di prima parte utilizzati solo dal gestore del portale ad esempio per stimare il numero di visitatori unici, e per finalità di mero monitoraggio, come quella di individuare le principali parole chiave per i motori di ricerca che portano a una pagina web istituzionale oppure di individuare le problematiche di navigazione del sito web.

Tali dati non permettono di identificare personalmente l'utente perché vengono automaticamente "anonimizzati" prima di essere elaborati dal software di analisi statistica degli accessi web.

A norma dell'art. 122 del Codice per la protezione dei dati personali e del provvedimento del Garante per la protezione dei dati personali relativo all'"Individuazione delle modalità semplificate per

l'informativa e l'acquisizione del consenso per l'uso dei cookie" dell'8 maggio 2014, pubblicato sulla Gazzetta Ufficiale n. 126 del 3 giugno 2014, la Regione Emilia-Romagna può installare nel browser degli utenti i cookie tecnici essenziali per il corretto funzionamento di un sito web, nonché quelli analytic e di funzionalità sopra descritti, poiché assimilati dalla normativa a quelli tecnici, anche senza il preventivo consenso degli stessi, fermo restando l'obbligo di informativa ai sensi dell'art. 13 del D. lgs. 196/2013.

3) Cookie analytic di terza parte

Il portale utilizza il servizio di Google Analytics, che si avvale di cookie per effettuare analisi statistiche di monitoraggio sui visitatori, I dati vengono raccolti da Google Analytics in forma anonima (senza le ultime 3 cifre dell'indirizzo IP) e non vengono incrociati con altre informazioni in possesso di Google. Pertanto questi cookie sono assimilabili a quelli tecnici e non necessitano del preventivo consenso degli utenti.

Per maggiori informazioni si può consultare la Guida di Google Analytics sulla "Salvaguardia dei dati": <https://support.google.com/analytics/answer/6004245>

Google inoltre mette a disposizione un componente aggiuntivo del browser per la disattivazione di Google Analytics, reperibile all'indirizzo: <https://tools.google.com/dlpage/gaoptout?hl=it>

4) Cookie di terze parti

In certi casi possono essere utilizzati cookie di "terze parti", gestiti direttamente da terzi e di cui la Regione Emilia-Romagna non effettua alcun trattamento. Possono ad esempio venire trasmessi cookie di terze parti quando si interagisce con i plugin di condivisione o con l'autenticazione dei social media, quando si visualizzano dei video che risiedono su un canale Youtube, quando si visualizza un form contenente il Captcha di Google o si consultano pagine che utilizzano il servizio Google Maps. Alcune di queste funzionalità vengono meglio descritte di seguito.

Utilizzo di plug-in di social network

I Portali della Regione Emilia-Romagna sono integrati con alcuni plug-in di social network, in particolare Facebook, Twitter, Google, per consentire agli utenti di condividere pubblicamente i contenuti dei portali regionali che trovano interessanti.

Quando l'utente visita una pagina di un portale regionale, i plug-in presenti stabiliscono una connessione diretta tra il browser dell'utente e i social network. Tramite questa connessione i social network acquisiscono alcune informazioni relative all'utente, come ad esempio indirizzo IP, data e ora della visita, browser utilizzato, ecc. Inoltre, se l'utente è connesso (e quindi autenticato) su uno di questi social network, le informazioni raccolte possono essere collegate al proprio profilo social. La Regione Emilia-Romagna invece non rileva nessuna delle informazioni che vengono trasmesse al social network tramite il plug-in.

Per maggiori informazioni sui plug-in utilizzati nei portali della Regione Emilia-Romagna si rinvia ai seguenti link:

- Facebook: <http://www.facebook.com/help/social-plugins/>
- Twitter: <http://dev.twitter.com/>
- Google: <https://developers.google.com/+web/buttons-policy?hl=en>

Autenticazione tramite i social network

Su alcuni portali della Regione Emilia-Romagna vengono utilizzati plug-in di social network per permettere agli utenti di autenticarsi ed accedere ad apposite porzioni di sito utilizzando le credenziali con cui si sono registrati sui social network.

I social network utilizzati sono: Facebook, Twitter, Google, LinkedIn. Inoltre si utilizza il sistema FedERa, promosso dalla Regione Emilia-Romagna e condotto dalla società Lepida S.p.A. per far sì che cittadini e imprese possano disporre di un'autenticazione federata, tramite la quale accedere ai servizi on-line forniti da tutti gli enti locali dell'Emilia-Romagna, Regione inclusa.

In questi casi la Regione Emilia-Romagna recepisce alcuni dati personali (Nome, Cognome, Indirizzo e-mail) dal gestore di credenziali di cui si avvale l'utente, al solo fine di permettere l'accesso ai siti istituzionali e ai servizi online dell'Ente.

Sui cookie installati, quindi, dai social network sopra indicati, definiti di Terze parti, l'Ente non ha alcun governo e, pertanto, al fine di permettere agli utenti di conoscere modalità e finalità dei trattamenti delle informazioni degli utenti da parte delle Terze parti, si riportano i seguenti link alle informative e ai moduli di consenso licenziati dalle Terze parti:

- Facebook privacy policy: <http://www.facebook.com/about/privacy/>
- Twitter privacy policy: <https://twitter.com/privacy>
- Google privacy policy: <http://www.google.com/intl/it/policies/privacy/>
- LinkedIn privacy policy: https://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv

Questionari online

Quando si compila un questionario online realizzato tramite il servizio "MiglioraPA" (<http://www.migliorapa.it>), vengono trasmessi cookie utilizzati direttamente dal gestore del servizio. Per maggiori informazioni su questi cookie consultare la relativa privacy policy: <http://qualitapa.gov.it/note/>

Impostazioni dei browser per disattivare i cookie

Disabilitare l'utilizzo dei cookie

E' possibile disabilitare l'utilizzo dei cookie modificando le impostazioni del proprio browser, per esempio:

- Firefox: <https://support.mozilla.org/it/kb/Gestione%20dei%20cookie>
- Internet Explorer: <http://windows.microsoft.com/it-it/windows7/how-to-manage-cookie-in-internet-explorer-9>
- Chrome: <https://support.google.com/chrome/answer/95647?hl=it%20>
- Safari: https://support.apple.com/kb/PH19214?viewlocale=it_IT&locale=en_US
- Safari IOS: <https://support.apple.com/it-it/HT201265>

Se il browser utilizzato non è tra quelli proposti, selezionare la funzione "Aiuto" sul proprio browser per trovare le informazioni su come procedere.

Attivare l'opzione Do Not Track

L'opzione Do Not Track è presente nella maggior parte dei browser di ultima generazione. I siti web progettati in modo da rispettare questa opzione, quando viene attivata, dovrebbero

automaticamente smettere di raccogliere alcuni dati di navigazione. Si tratta di una funzionalità non universalmente implementata.

Attivare la modalità di "navigazione anonima"

Mediante questa funzione disponibile ormai in tutti i browser, è possibile navigare in Internet senza salvare alcuna informazione sui siti e sulle pagine visitate.

Tuttavia, i dati di navigazione, pur attivata tale funzionalità, sono registrati e conservati dai gestori dei siti web e dai provider di connettività.

Eliminare direttamente i cookie

Attualmente quasi tutti i browser consentono di eliminare tutti i cookie installati.

Per maggiori istruzioni, consultare la guida del proprio browser o visitare uno dei seguenti link:

- Impostazioni dei cookie in Internet Explorer: <http://windows.microsoft.com/it-IT/internet-explorer/delete-manage-cookie#ie=ie-9>
- Impostazioni dei cookie in Firefox:
<https://support.mozilla.org/it/kb/Eliminare%20i%20cookie>
- Impostazioni dei cookie in Chrome:
https://support.google.com/chrome/answer/95647?hl=it&ref_topic=3421433
- Impostazioni dei cookie in Safari (iOS): <http://support.apple.com/kb/HT1677>

Tuttavia, ad ogni nuova navigazione saranno installati nuovamente i cookie; in ragione di ciò si invita ad eseguire tale operazione periodicamente o utilizzare funzioni automatizzate per la cancellazione periodica dei cookie.

Link a siti esterni

Questo sito internet contiene collegamenti ipertestuali detti "link" (ossia strumenti che consentono il collegamento ad una pagina web di un altro sito): i siti esterni raggiungibili tramite link attraverso i Portali della Regione Emilia-Romagna sono sviluppati e gestiti da soggetti sui quali l'Ente non ha alcuna titolarità né controllo e non è in alcun modo responsabile circa contenuti, qualità, accuratezza e servizi offerti. La visita e l'utilizzo dei siti consultati dall'utente dal presente sito tramite link, quindi, è rimessa esclusivamente alla totale discrezionalità e responsabilità dell'utente utilizzatore. La presente informativa, pertanto, è resa solo per i siti della Regione Emilia-Romagna e non anche per altri siti web eventualmente consultati dall'utente tramite link.

Diritti degli interessati

I soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione (**art. 7 del d.lgs. n. 196/2003**).

Ai sensi del medesimo articolo si ha il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento.

Al fine di semplificare le modalità di inoltro e ridurre i tempi per il riscontro si invita a presentare le richieste, di cui al precedente paragrafo, alla Regione Emilia-Romagna, Ufficio per le relazioni con il pubblico (Urp), per iscritto o recandosi direttamente presso lo sportello Urp.

L'Urp è aperto dal lunedì al venerdì dalle 9 alle 13 in Viale Aldo Moro 52, 40127 Bologna (Italia): telefono 800-662200, fax 051-5275360, e-mail urp@regione.emilia-romagna.it.

Le richieste di cui all'art.7 del Codice comma 1 e comma 2 possono essere formulate anche oralmente.

Appendice B. Fac-simile banner

Appendice B.1. Banner senza richiesta di consenso

Per offrire informazioni e servizi nel miglior modo possibile, questo sito utilizza cookie tecnici e di terze parti. Per maggiori informazioni sui cookie utilizzati e su come eventualmente disabilitarli leggi la nostra Privacy policy.

Appendice B.2. Banner con richiesta di consenso

Il sito utilizza cookie tecnici, analytic e di terze parti, anche di profilazione, per fornire servizi in linea con le tue preferenze. Per avere maggiori informazioni su tutti i cookie utilizzati, su come disabilitarli o negare il consenso all'utilizzo, leggi l'informativa. Premendo il pulsante OK o proseguendo nella navigazione presti il consenso all'uso di tutti i cookie.

Appendice C. Fac-simile clausola di contratto per fornitori esterni

Art. XX Il Fornitore si obbliga a fornire alla Giunta della Regione Emilia-Romagna un servizio/prodotto conforme alla normativa vigente, con esplicito e non esaustivo riferimento alle disposizioni in materia di protezione dei dati personali, ivi comprese le norme in tema di cookie.

Allegato 17: Regole per Sistemi di Riferimento dei dati geografici e nelle applicazioni GIS

1	Introduzione.....	1
2	Il Sistema di riferimento geodetico nazionale.....	1
3	Adozione del Sistema di riferimento geodetico nazionale.....	2
4	Il Sistema di riferimento UTMREER	2
5	Regole per il trattamento dei diversi Sistemi di riferimento	2
6	Conversione dei Sistemi di Riferimento	3
7	I Sistemi di riferimento nella pubblicazione dei dati	3
8	Evoluzione nel tempo dei Sistemi di riferimento	4
9	Allegati e documenti di riferimento	4
10	Conclusioni	4

1 Introduzione

Scopo di questo documento è quello di illustrare regole per Sistemi di Riferimento dei dati geografici e nelle applicazioni GIS.

Le tematiche trattate della Pubblica Amministrazione ed in particolare dalla Regione Emilia-Romagna coinvolgono molto frequentemente dati di tipo geografico, ed in particolare basi dati geotopografiche, prodotti cartografici o basi dati tematiche. In tali tipologie di dati è fondamentale la conoscenza delle modalità di georeferenziazione ed in particolare delle caratteristiche dei Sistemi di Riferimento (SR) adottati allo scopo di garantire la necessaria confrontabilità geografica fra dati di tipologia, fonti e periodi temporali diversi.

Questi aspetti sono già sottolineati nella Del. Reg. 848/2003 (Atto di indirizzo e coordinamento tecnico Art. 27 LR 20/2000); essa individua l'adozione di un unico sistema di riferimento che rappresenta, infatti, il principale presupposto per la fruibilità e lo scambio dei dati territoriali tra le pubbliche amministrazioni centrali, regionali e locali, ed ora estesa anche al di fuori della Pubblica Amministrazione.

2 Il Sistema di riferimento geodetico nazionale

Nel 2012 è stato pubblicato in G.U. il DPCM del 10 novembre 2011 (v. allegato 1) relativo all'Adozione del Sistema di Riferimento Geodetico Nazionale che:

- individua la realizzazione ETRF2000 – all'epoca 2008.0 -, del Sistema di riferimento geodetico europeo ETRS89, come il Sistema di riferimento geodetico adottato dalle Amministrazioni italiane (Art. 2);
- indica il Sistema di riferimento geodetico nazionale come il sistema da utilizzare per le nuove realizzazioni di dati di tipo geografico o territoriale (Art.3);
- richiede che i dati pregressi disponibili nelle Amministrazioni siano resi disponibili nel Sistema di riferimento geodetico nazionale secondo opportune conversioni; per quanto riguarda i Sistemi di Riferimento già in uso in Italia, ROMA40 ED50, ETRF89, le conversioni dovranno essere operate secondo dati e procedure che l'Istituto Geografico Militare rende disponibili.

3 Adozione del Sistema di riferimento geodetico nazionale

Allo scopo quindi di dare attuazione a quanto richiesto sia dalla D.R n.848/2003 (Dir. A27) e dal DPCM del 10 novembre 2011 (Adozione del Sistema di riferimento geodetico nazionale):

- viene adottato come Sistema di riferimento geodetico della Regione Emilia-Romagna il Sistema ETRS89 nella realizzazione ETRF2000 all'epoca 2008.0
- nell'ambito dei prodotti cartografici e delle applicazioni GIS, sono adottati: il relativo sistemi di coordinate geografico ETRS89 (codice EPSG:4258) e i relativi Sistemi di coordinate proiettate ETRS89 / UTM Zone 32N e ETRS89 / UTM Zone 33N (rispettivamente EPSG:25832; EPSG:25833);
- al fine di supportare le applicazioni GIS/cartografiche nel continuo territoriale, il Sistema di Riferimento proiettato ETRS89 / UTM Zone 32N (EPSG:25832) è esteso alla parte di territorio regionale compresa convenzionalmente nel fuso 33;
- i dati geografici pubblicati o resi fruibili tramite servizi, devono essere resi disponibili in ETRS89 o in uno dei relativi sistemi proiettati indicati sopra.

4 Il Sistema di riferimento UTMER

Il Sistema di Riferimento definito localmente al territorio della regione Emilia-Romagna a partire dagli anni '90 e indicato nella Dir. A27 nel 2003 come UTM-ED'50*, convenzionalmente indicato come UTMA, è stato ridefinito al fine di supportare correttamente le conversioni di coordinate tramite i dati e le modalità procedurali indicate dal IGM. A questo scopo:

- è definito il Sistema di Riferimento denominato UTMER come Gauss-Boaga Fuso Ovest con falsa origine in Est e in Nord (v. allegato 2). Il Sistema UTMER è recepito da EPSG con la denominazione Monte Mario / TM Emilia-Romagna con codice EPSG:5659;
- al fine di supportare correttamente la conversione dei dati verso il Sistema di Riferimento ETRF2000 (ETRS89), i dati geografici dichiarati nel sistema di riferimento UTM-ED'50* (o UTMA) andranno dichiarati nel Sistema UTMER, senza alcuna trasformazione di coordinate; si tratta quindi solamente del cambiamento della dichiarazione del sistema di riferimento e non di un cambiamento del valore delle coordinate (es: per il formato ESRI shape file si tratta della sola sostituzione del file *.prj);
- Il Sistema di riferimento UTM-ED'50* (o UTMA), per come è originato, non è adeguato a supportare correttamente le conversioni verso ETRS89 e risulta pertanto deprecato. Il sistema di riferimento regionale UTMER (EPSG:5659), definito a partire dal Sistema di inquadramento originario della CTR 1:5000 regionale, sostituisce il sistema UTMA come sistema di riferimento dei dati pregressi con falsa origine nord di -4.000.000.

5 Regole per il trattamento dei diversi Sistemi di riferimento

Considerando che attualmente sono presenti ed utilizzati un numero consistente di dati ed applicazioni di tipo geografico con diversi sistemi di riferimento e che è necessario che gli utenti e le applicazioni geografiche possano opportunamente interpretarli e trattarli:

- sono definiti i sistemi di riferimento supportati dalla Regione Emilia-Romagna ed identificati tramite opportuni file di proiezione (*.prj) e/o tramite codice EPSG (v. allegato 3);
- le applicazioni di tipo geografico devono poter riconoscere il SR di un dato geografico in input tramite il file di proiezione (*.prj), codice EPSG o analogo codice proprietario univoco del SR (es: SRID di Oracle SDO);

- i dati trattati da applicazioni gis oppure pubblicati tramite i servizi dell'infrastruttura geografica o tramite il geoportale, devono avere il SR definito tramite file di proiezione (*.prj) o tramite codice EPSG (o altro codice proprietario benché documentato);
- sono definite le modalità, i dati e le procedure di conversione dei dati da un SR ad un altro tra quelli supportati dalla Regione Emilia-Romagna (v. allegato 2), in coerenza con quanto indicato dal DPCM e i dati e le procedure fornite da IGM.

6 Conversione dei Sistemi di Riferimento

Allo scopo di supportare le opportune conversioni di coordinate tra sistemi ed in particolare per supportare la conversione nel Sistema di Riferimento Geodetico Nazionale, la Regione Emilia-Romagna rende disponibili metodologie, dati e procedure di conversione garantendo un grado di compatibilità con quanto indicato e proposto da IGM, adeguato alla maggior parte delle applicazioni geografiche e cartografiche. In particolare sono messi a disposizione:

- indicazione delle metodologie di trasformazione da applicare per la conversione tra i vari sistemi gestiti dalla regione Emilia-Romagna;
- le costanti di trasformazione tra sistemi basati sul medesimo Datum o tra sistemi approssimati (es: Gauss-Boaga, UTMER, UTMA);
- i grigliati di isotrasformazione tra SR basati su Datum differenti (es: ROMA40, ED'50, ETRS89); i grigliati sono forniti in versioni diverse ed in particolare nella versione NTV2 binaria riconosciuta dalla maggior parte dei software GIS / CAD e dalle librerie di conversione di coordinate;
- il software di conversione di coordinate ConvER (attualmente alla ver. 2013) che applica le metodologie di cui sopra; il software ConvER può essere utilizzato anche a linea di comando e richiamato da applicazioni o script batch;
- un pacchetto per l'installazione delle metodologie di trasformazione e dei grigliati sopraindicati in ambiente ESRI ArcGIS sia server che desktop;
- un pacchetto per l'installazione delle metodologie di trasformazione e dei grigliati sopraindicati in ambiente Quantum GIS;
- sono esposti tramite i servizi del geoportale i Servizi WCTS (Web Coordinate Transformation Service) per la conversione di coordinate tramite le metodologie sopra esposte (analogamente il geoportale espone tramite specifica interfaccia una funzionalità di conversione di coordinate immediatamente utilizzabile da un utente).

Al fine di garantire la corretta conversione tra Sistemi di Riferimento utilizzati in Regione Emilia-Romagna, è opportuno che le diverse applicazioni geografiche o i diversi ambienti di tipo geografico server o desktop:

- riconoscano i sistemi di riferimento utilizzati in Regione ed elencati nell'allegato;
- nel caso di conversioni di coordinate, possano operare secondo le metodologie, i dati e le procedure di conversione sopra indicate.

7 I Sistemi di riferimento nella pubblicazione dei dati

Nella pubblicazione di dati e/o servizi di tipo geografico i dati possono essere esposti, previa conversione del Sistema di Riferimento, anche in SR diversi da quello dei dati geografici. Questo consente:

- pubblicare od esporre dati geografici nel Sistema di riferimento geodetico nazionale, anche se per diverse ragioni i dati non sono in tale sistema;

- pubblicare od esporre i medesimi dati in più Sistemi di riferimento allo scopo di garantire:
 - la massima fruibilità ed efficienza di utilizzo da parte dei diversi utenti;
 - l'applicazione delle modalità di conversione adeguate al contesto garantendo a priori il necessario grado di correttezza e confrontabilità geografica.

8 Evoluzione nel tempo dei Sistemi di riferimento

Le regole e le indicazioni contenute in questo documento e negli allegati relativi possono essere soggette a evoluzioni e aggiornamenti, con versioni successive del documento, allo scopo di mantenere il necessario allineamento con i Sistemi di riferimento nazionali (ora materializzata dalla Rete Dinamica nazionale), aggiornare le codifiche dei sistemi in funzione delle evoluzioni delle funzionalità dei software, migliorare dati e procedure di conversione di coordinate in funzione delle metodologie di utilizzo e degli standard di qualità richiesti dagli utenti.

9 Allegati e documenti di riferimento

Allegato 1: Supplemento ordinario n.37 alla G.U. n. 48 del 27 febbraio 2012 – Serie generale.

Allegato 2: Sistemi di Coordinate Geografiche e Cartografiche in Regione Emilia Romagna e loro trasformazioni, <http://geoportale.regione.emilia-romagna.it> nella sezione sui Sistemi di Riferimento.

Allegato 3: Elenco dei Sistemi di riferimento gestiti, relativi file di proiezione (*.prj) e relativi codici EPSG, <http://geoportale.regione.emilia-romagna.it> nella sezione sui Sistemi di Riferimento.

10 Conclusioni

Le indicazioni di cui sopra hanno complessivamente lo scopo di governare la tematica dei Sistemi di Riferimento dei dati geografici ed in particolare per ciò che riguarda la definizione e l'adozione dei SR, le metodologie di conversione di SR e regole di pubblicazione, intendendo in tal senso garantire la necessaria omogeneità e confrontabilità geografica tra i numerosi dati di tipo territoriale trattati in Regione Emilia-Romagna.

Allegato 18: Linee guida per l'integrazione dei sistemi verticali con il sistema documentale regionale

INDICE DEL DOCUMENTO

1	INTRODUZIONE	2
2	Architettura generale del sistema di gestione documentale regionale	3
2.1	Macro componenti del sistema documentale Regionale	4
2.2	Il sistema Doc/er	7
2.2.1	<i>Funzioni e utilizzo del sistema di Front End</i>	<i>7</i>
2.2.2	<i>Integrazione con lam e gestione della sessione</i>	<i>7</i>
2.2.3	<i>Gestione delle anagrafiche</i>	<i>7</i>
2.2.4	<i>Gestione dei diritti di accesso su Doc/er</i>	<i>8</i>
2.2.4.1	<i>Struttura dei gruppi</i>	<i>8</i>
2.2.4.2	<i>Strutture di organigramma sincronizzate sui gruppi Doc/er</i>	<i>9</i>
2.2.4.3	<i>Esempio di gruppi derivati da Organigramma</i>	<i>12</i>
2.2.4.4	<i>Esempio di gruppi derivati da Organigramma</i>	<i>13</i>
2.2.5	<i>Gestione dei fascicoli</i>	<i>13</i>
2.2.6	<i>Gestione dei documenti</i>	<i>13</i>
3	Progettazione dell'integrazione dei SV con DOC/ER	15
3.1	Autenticazione	15
3.2	Definizione delle tipologie documentarie e dei metadati	16
3.3	Definizione delle integrazioni per gli oggetti trattati dal SV	16
3.4	Gestione delle anagrafiche	16
3.5	Gestione dei fascicoli e dei documenti	17
3.5.1	<i>Sincronizzazione di documenti in fase di produzione</i>	<i>17</i>
3.5.2	<i>Richieste di protocollazione e/o fascicolazione</i>	<i>18</i>
3.5.3	<i>Richieste di repertoriazione (Registrazione Particolare)</i>	<i>19</i>
3.5.4	<i>Azioni di Modifica documento</i>	<i>20</i>
3.5.5	<i>Creazione nuovi fascicoli</i>	<i>21</i>
3.5.6	<i>Modifica fascicoli</i>	<i>21</i>
3.5.7	<i>Modello di integrazione per l'aggiornamento di documenti, fascicoli e loro ACL : sincrona o asincrona</i>	<i>22</i>
3.6	Attribuzione dei diritti di accesso agli oggetti documentali	23
3.6.1	<i>Traduzione in ACL Doc/er dei diritti del SV</i>	<i>23</i>
3.7	SV di registro	24
4	Modello organizzativo dell'integrazione	25
5	L'ambiente per il test di integrazione con Doc/er	27
5.1	Servizi WEB	27
5.2	Front End	30
6	Ambiente di produzione	31
7	Appendici	32
7.1	Appendice 1: Specifiche tecniche dei servizi e delle interfacce del modello GeDoc	32
7.2	Appendice 2: Check list di controllo delle azioni di integrazione con il sistema documentale	32
7.3	Appendice 3: Tabella per il censimento di azioni, attori e permessi per il progetto di integrazione di un Sistema Verticale	34
7.4	34	
7.5	Appendice 4: Tipologie documentarie gestite e relativi metadati aggiuntivi	34
7.6	Appendice 5: Metadati comuni di versamento Doc/er	44
7.7	Appendice 6: Modulo di definizione delle tipologie documentarie gestite dal Sistema Verticale	52
7.8	Appendice 7: Tabella per il Censimento Anagrafiche custom	54
7.9	Appendice 8: Tabella per il Censimento Gruppi di business da gestire	56
7.10	Appendice 9: Interfacce per realizzazione provider di repertoriazione	56

1 INTRODUZIONE

L'elaborazione del presente documento si colloca nell'ambito dell'intervento A1.3 – “Definizione delle specifiche per l'integrazione con il Sistema documentale” contenuto all'interno del Piano degli interventi per la semplificazione, approvato con DGR n. 2013 del 17 dicembre 2012. Gli obiettivi dell'intervento sono quelli di:

- definire le specifiche tecniche per l'integrazione di Sistemi informativi verticali con il sistema di gestione documentale regionale
- stabilire un iter propedeutico al rilascio di tali Sistemi che garantisca il rispetto delle policy di gestione documentale adottate dalla Regione.

Le linee guida si configurano quindi come strumento a disposizione di tutte le strutture organizzative regionali che devono realizzare sistemi che hanno necessità di trattare oggetti documentali digitali.

Per quanto riguarda il glossario, i concetti archivistici fondamentali, la formazione e il trattamento dei documenti, i formati ammessi nelle varie fasi del ciclo di vita dei documenti si rimanda alle Linee Guida di Gestione documentale e al relativo allegato.

Ai fini di una maggiore comprensione del documento e di facilità di aggiornamento dei suoi contenuti, il documento è stato strutturato in due parti:

- una sezione principale, in cui sono descritti gli elementi essenziali, l'architettura del sistema regionale e le sue caratteristiche principali relative alle tematiche di integrazione con altri sistemi informativi, le specifiche per la progettazione e la realizzazione di tali integrazioni e il modello di processo della loro validazione a salvaguardia del rispetto delle policy regionali di gestione documentale.
- una serie di allegati, sia di approfondimento e di dettaglio tecnico, sia di supporto alle attività di progettazione. Gli allegati dovranno essere mantenuti aggiornati rispetto alla evoluzione del sistema tecnologico in uso ed eventualmente arricchirsi per fornire indicazioni su casi specifici che via via venissero a presentarsi.

Ne deriva quindi che le presenti linee guida non possono configurarsi come un documento statico e definito per sempre, ma necessiteranno di una costante attenzione ed evoluzione per adeguarsi ai mutamenti di contesto amministrativo, organizzativo, tecnologico e normativo.

2 ARCHITETTURA GENERALE DEL SISTEMA DI GESTIONE DOCUMENTALE REGIONALE

Il Sistema di Gestione Documentale Regionale (da ora GDR) è la componente trasversale fondamentale del sistema informativo regionale che oltre ai servizi di front end offre una gamma completa di servizi di gestione documentale (ERDMS) ai sistemi applicativi sia interni, mediante integrazione tramite servizi, che esterni all'Ente, in cooperazione applicativa o mediante servizi o, nei casi meno strutturati, in interoperabilità o via PEO/PEC.

Il modello di gestione documentale ispiratore del nuovo paradigma che verrà adottato dalla Regione Emilia Romagna è quello di GeDoc che prevede:

- l'adozione di un'architettura modulare in cui il documentale, oltre a servizi di front end, eroghi i servizi di back end di gestione documentale e in cui il protocollo sia visto come un modulo applicativo dello stack dei sistemi verticali, esclusivamente dedicato al servizio di certificazione dei flussi documentali (vedi Linee Guida Gestione Documentale), con tutte le caratteristiche previste dal CAD e dalle successive regole tecniche;
- la reingegnerizzazione dei processi: le applicazioni verticali che trattano documenti, tra cui il protocollo dell'ente, si interfacciano unicamente con il sistema di GDR.

Il paradigma deve peraltro essere realizzato nell'ottica della massima astrazione possibile, ovvero prevedendo di mantenersi il più possibile indipendente non solo dai sw di base ma anche dai Sistemi verticali di protocollo/registro, costruendo delle interfacce standard sia da che verso il sistema GDR.

La concretizzazione di questi principi ispiratori ha portato alla costruzione del sistema Doc/er che eroga uno strato intermedio di servizi documentali per l'archiviazione/indicizzazione dei documenti, per la protocollazione e fascicolazione di documenti, per la gestione dei fascicoli, per la timbratura. Tali servizi sono indipendenti sia dal sw di base sottostante sia dai sistemi che erogano ciascuna di queste funzioni ma integrati con questi sistemi in modo trasparente per i sistemi consumer; Doc/er inoltre è integrato in modo trasparente anche con il sistema regionale di conservazione.

Allo stato attuale i servizi Doc/er erogano le seguenti macro funzionalità:

- servizi di gestione dell'intero ciclo di vita dei documenti indipendentemente dal sistema di EDMS sottostante;
- servizio di timbro digitale;
- servizio di invio in conservazione automatica dei documenti archiviati all'interno del sistema documentale (al ParER);
- servizi di protocollazione, di repertoriazione, di fascicolazione e di invio PEC dei documenti (richiamando omologhi servizi del protocollo con interfacce standard comuni a tutti i sistemi qualificati Doc/er)
- servizi di verifica delle firme e dei formati.

2.1 Macro componenti del sistema documentale Regionale

Analizziamo di seguito più in dettaglio le componenti del sistema GDR complessivo:

Componenti di base:

- Il sistema EDRMS di servizi documentali di base: implementa l'archiviazione, la metadattazione, l'indicizzazione e la ricerca full text di fascicoli e documenti. Nel caso RER è stato selezionato il prodotto OS Alfresco.
- il sistema PKI che eroga servizi di firma e verifica
- il sistema della posta certificata

Sistema Conservazione

- il sistema Sacer di conservazione a norma gestito da ParER

Protocollo

- il sistema di protocollo a norma E-Grammata (registrazione di protocollo, classificazione e fascicolazione) e integrato con Doc/er stesso in modo bidirezionale

Sistema di repertori (registri particolari)

- sistema di gestione di repertori (registrazione, classificazione e fascicolazione) e integrato con Doc/er stesso in modo bidirezionale. Tale funzione è svolta attualmente da E-Grammata

Doc/er:

Costituisce il "middleware" applicativo intermedio di servizi documentali, timbro, conservazione, verifica formati indipendente dai servizi di base sottostanti e che "ingloba" all'interno l'integrazione con EDRMS, protocollo, registri particolari e Sistemi verticali.

Costituisce il "middleware" applicativo intermedio di servizi documentali, timbro, conservazione, verifica formati indipendente dai servizi di base sottostanti e che "ingloba" all'interno l'integrazione con EDRMS, protocollo, registri particolari e Sistemi verticali.

Esso consiste di diverse componenti:

- un sistema di front end che fornisce l'accesso in visualizzazione e in gestione (creazione, modifica, eliminazione) ai fascicoli (composti anche da documenti provenienti da SV diversi), ai documenti e al monitoraggio e gestione dello stato di conservazione in Sacer (oltre a funzioni di timbro digitale, invio PEC etc.)
- un set di servizi documentali per:
 - gestione delle anagrafiche del sistema MW/EDRMS:
 - Ente
 - AOO
 - Titolare
 - Fascicoli
 - Gruppi
 - Anagrafiche custom

- gestione del ciclo di vita dei “document”
- integrazione con “Protocollo” / “Repertori” mediante richiamo dei relativi servizi
 - Protocolla Documento
 - Repertoria Documento
 - Crea fascicolo
 - Fascicola documento
 - InviaPEC
- timbratura
 - getTimbro
 - applicaTimbro
- verifica formato e firme
- un back office deputato all’invio in conservazione dei documenti:
 - un agente di popolamento della coda di conservazione a partire dall’archivio documentale (documenti marcati per la conservazione, in modo diretto dal front end o dai vari Sistemi verticali)
 - un agente di invio in conservazione (richiamo dei servizi di conservazione sugli oggetti della coda)
 - un agente di importazione e mappatura dei gruppi di utenti, associati alle strutture organizzative dell’ente seconda la logica di organica organigramma (vedi paragrafo sull’argomento).
 - un sistema di gestione delle operazioni massive a seguito di eventi massivi sulla struttura organizzativa (disponibile nei prossimi rilasci)

Il GDR, articolato nei suoi sottosistemi, è uno dei componenti fondamentali dei servizi trasversali dell’ente. Graficamente le correlazioni tra le componenti del sistema GDR e i sistemi verticali possono essere così sintetizzate:

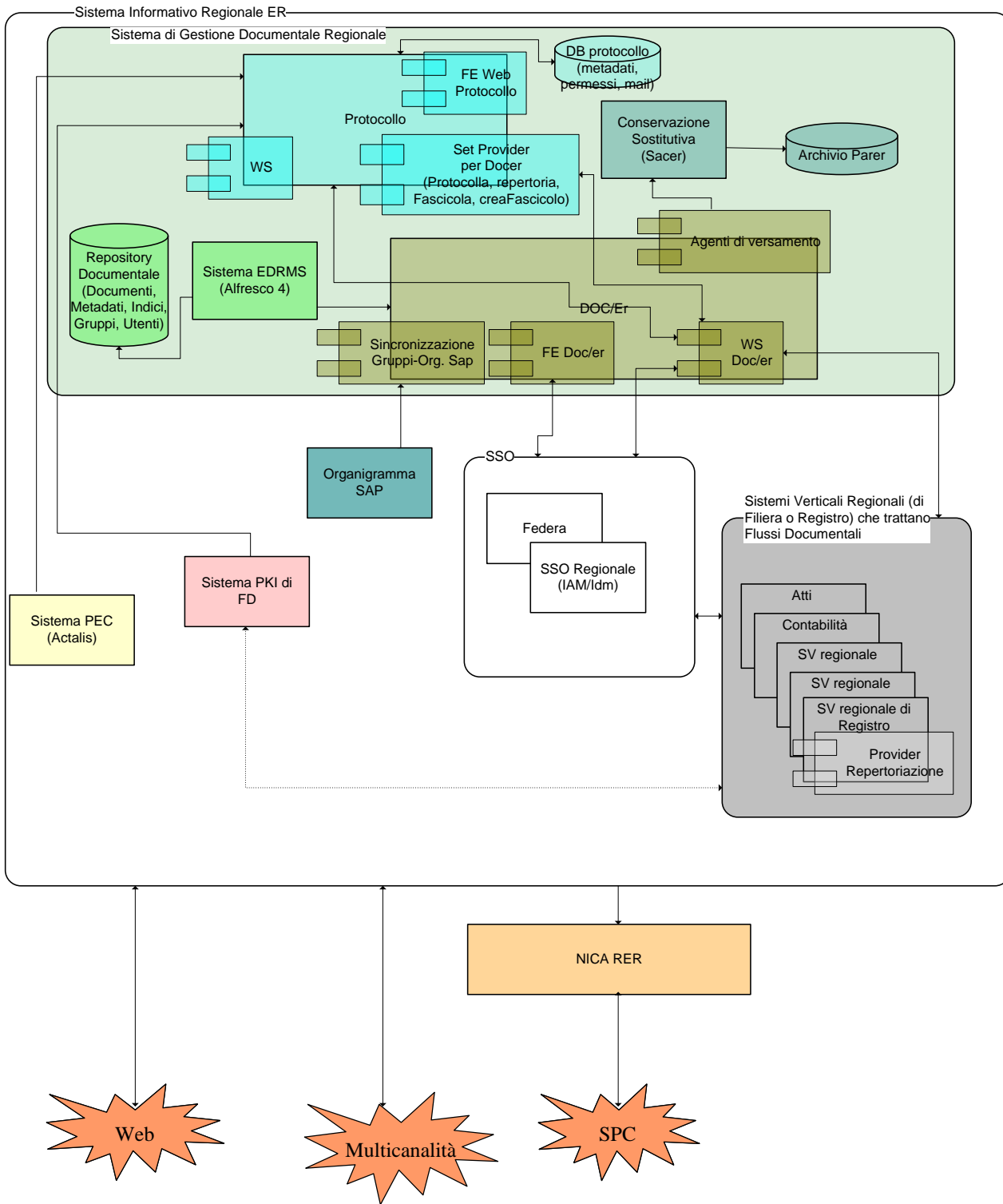


Fig. 1

2.2 Il sistema Doc/er

In questo paragrafo si forniscono le caratteristiche fondamentali per il progettista di applicazioni integrate con il sistema GDR relativamente agli eventi di produzione e gestione di oggetti documentali.

Si rimanda all'appendice 1 per una descrizione dettagliata del sistema Doc/er e delle sue caratteristiche tecniche.

2.2.1 Funzioni e utilizzo del sistema di Front End

Il sistema di Front End è integrato con il sistema SSO dell'ente, pertanto l'accesso avviene essenzialmente con l'utenza di dominio.

A tendere tutta la documentazione dell'Ente sarà accessibile attraverso il front end di Doc/er: per raggiungere questo obiettivo sarà necessario completare l'adeguamento al paradigma della nuova versione di Doc/er di tutte le applicazioni verticali, E-Grammata compreso.

Dopo l'avvio del nuovo Doc/er, tutti i documenti creati su E-Grammata saranno accessibili attraverso il FE Doce/er agli utenti che hanno su di essi diritti di visibilità a qualche titolo (come snodi del flusso di lavoro di una pratica) solo quando l'adeguamento del protocollo necessario a questo funzionamento sarà disponibile. Tale attività è prevista per la seconda fase del progetto (vedi Scheda A3.2 della delibera 2013/2012). Attraverso il Front End ogni utente dovrà poter consultare i fascicoli (anche composti da documenti creati da verticali diversi, compreso il FE di Doc/er) di tutte le pratiche su cui ha diritto di accesso in perfetta coerenza con i diritti di accesso sui sistemi verticali.

I documenti prodotti dai sistemi verticali sono modificabili solo dal SV e non attraverso il front end (non sarà possibile alterare metadati, classifica e fascicolo originale o allegati e annessi dei documenti di pertinenza dei verticali); l'unica possibilità attualmente offerta dal sistema è quella di creare un nuovo documento come copia dell'originale e inserirlo all'interno dei fascicoli delle proprie pratiche.

2.2.2 Integrazione con iam e gestione della sessione

Il sistema di FE è integrato con IAM e Federa.

Il richiamo dei servizi Doc/er da parte dei SV avviene mediante l'utilizzo di utenze applicative.

Nella seconda fase i WS Doc/er saranno richiamabili anche utilizzando utenze di dominio censite su Rersdm o Federa. Le utenze applicative continueranno ad essere utilizzate per le applicazioni che non sono ancora adeguate e nel caso in cui il sistema cliente funzioni come automatismo per conto di un'entità non direttamente identificabile con un'utenza di dominio.

2.2.3 Gestione delle anagrafiche

Su Doc/er le principali anagrafiche da gestire tramite SV integrati sono di seguito elencate:

- eventuali anagrafiche custom necessarie per i metadati di profilo dei documenti
- gruppi

- utenti
- cartelle (entità che aggrega documenti informalmente, utile ad esempio in fase di produzione di documenti, prima della registrazione)

Deve essere opportunamente garantito l'allineamento tra il SV e il sistema Doc/er di eventuali modifiche a oggetti delle anagrafiche.

2.2.4 Gestione dei diritti di accesso su Doc/er

I seguenti oggetti del sistema documentale sono soggetti a diritti di accesso basati su logiche specifiche:

- documenti
- fascicoli
- voci di classifica.

Questo significa che non tutti gli utenti possono vedere tutti i documenti, tutti i fascicoli e tutte le voci di titolare. I diritti di accesso su un oggetto possono essere concessi puntualmente a utenti o a raggruppamenti logici di utenti denominati **gruppi**.

In pratica i gruppi di Doc/er sono unità logiche che condividono diritti di accesso omogenei agli oggetti sopra citati. E' prevista la gestione in una logica gerarchica dei gruppi che si ripercuote sui diritti di accesso: gli utenti che appartengono a un gruppo sovraordinato hanno oltre ai diritti di accesso specifici, anche l'unione dei diritti di tutti i gruppi figli.

Doc/er implementa la logica gerarchica dei diritti di accesso propagando l'appartenenza di un utente a un nodo padre anche ai nodi figli.

Nell'ambito regionale, tra i gruppi di Doc/er particolare rilevanza assumono quelli identificabili con le strutture dell'organigramma e relativa gerarchia ad albero fino al livello di PO/Professional.

Viene comunque mantenuta la possibilità di creare ulteriori gruppi, costruiti sulla base di specifiche logiche di particolari processi, ma nell'ambito del progetto attualmente non esistono ipotesi di costruzione di automatismi su logiche di sincronizzazione diversa da quella della pianta organica.

Eventuali altre logiche sono quindi da implementare a cura del SV cliente mediante l'utilizzo dei servizi di amministrazione di gruppi e utenti o tramite il FE di Doc/er.

2.2.4.1 Struttura dei gruppi

Doc/er permette di importare gruppi, strutture e utenti o di sincronizzarsi con un LDap dell'ente.

Nell'ambito regionale un sistema automatico tiene sincronizzato il sistema di gruppi di Doc/er con l'organigramma regionale, mentre qualsiasi altra struttura di gruppi legati a logiche di processo di specifici sistemi verticali sarà curata manualmente dal Front End di Doc/er stesso o in modo automatico dai SV attraverso i servizi di amministrazione messi a disposizione nel middleware.

Questo significa che con periodicità almeno giornaliera verrà prodotto uno scarico delle strutture dell'organigramma fino al III livello con la loro strutturazione gerarchica, che verranno riportate come gruppi e relativa gerarchia in Doc/er.

Di default i collaboratori vengono collegati ai gruppi corrispondenti alle strutture in base alla loro appartenenza in organigramma o nel sistema delle posizioni lavorative (per le strutture di terzo livello).

La logica gerarchica dei diritti di accesso dei gruppi introduce il problema di distinguere i dipendenti appartenenti a un nodo padre dell'organigramma con diritti di visibilità sui nodi subordinati dai dipendenti appartenenti allo stesso nodo che non hanno questi diritti.

Per risolvere questo problema, per ogni struttura padre di I (Direzioni, Istituti, Agenzie) e di II livello (Servizi), viene generato, oltre al gruppo che gli corrisponde, anche un gruppo fittizio (staff della struttura), a livello delle altre strutture figlie.

Il sistema di sincronizzazione automatica associa al gruppo padre il responsabile della struttura e al gruppo fittizio tutti gli altri collaboratori della struttura: questo fa sì che solo il responsabile abbia visibilità oltre che su tutti gli oggetti della struttura anche su quelli di tutte le strutture sottostanti, mentre il collaboratori avranno accesso solo a quelli della struttura.

Inoltre, per ogni struttura di organigramma viene anche creato un gruppo a cui andranno assegnati gli utenti con diritti di visibilità sui documenti riservati.

L'attribuzione di utenti a un gruppo con diritti di visibilità sui riservati e di ulteriori utenti oltre il Responsabile ai gruppi "padre" non viene gestita in automatico ma in modalità manuale attraverso il FE Doc/er o dal SV tramite gli opportuni servizi Doc/er.

I codici dei gruppi coincidono con i codici delle strutture. Per i gruppi "staff" e "riservati" il codice sarà il codice della struttura seguito da "_F" e "_R" rispettivamente.

2.2.4.2 Strutture di organigramma sincronizzate sui gruppi Doc/er

Le strutture che verranno sincronizzate su Doc/er come gruppi sono quelle per cui viene definita una relazione tra l'AOO e una struttura dell'Organigramma che diventa la radice della gerarchia delle strutture da sincronizzare coi gruppi Doc/er.

Tale relazione sarà gestibile direttamente dall'interfaccia Sap per la gestione delle strutture e sarà quindi possibile selezionare nuove strutture da sincronizzare a livello di gruppi e utenti in Doc/er, in modo da sfruttare la logica di base per l'attribuzione dei diritti di accesso.

Attualmente le strutture che verranno censite su Doc/er alla partenza della fase I sono le strutture afferenti alle seguenti unità "genitrici":

AOO Giunta:

Codice Struttura	Denominazione
00000940	AGENZIA SANITARIA E SOCIALE REGIONALE
D0000021	DIR. GEN. CENTRALE RISORSE FINANZIARIE E PATRIMONIO
D0000022	DIR. GEN. CENTRALE ORGANIZZAZIONE,PERS.,SIST.INF.E TELEMAT.
D0000023	DIR. GEN. CENTRALE AFFARI ISTITUZIONALI E LEGISLATIVI
D0000024	DIR. GEN. AGRICOLTURA, ECONOMIA ITTICA, ATT.FAUNISTICO-VEN.
D0000025	DIR. GEN. AMBIENTE E DIFESA DEL SUOLO E DELLA COSTA
D0000026	DIR. GEN. PROGRAMMAZIONE TERRITORIALE E NEGOZIATA, INTESE
D0000027	DIR. GEN. CULTURA, FORMAZIONE E LAVORO
D0000028	DIR. GEN. ATTIVITA' PRODUTTIVE, COMMERCIO, TURISMO
D0000029	DIR. GEN. SANITA' E POLITICHE SOCIALI

D0000031	DIR. GEN. RETI INFRASTRUTTURALI, LOGISTICA E SISTEMI MOBIL.
F0000032	GABINETTO DEL PRESIDENTE DELLA GIUNTA
P0000686	SEGR.PRESIDENTE DELLA GIUNTA REGIONALE
P0000762	SEGR.DEL SOTTOSEGRETARIO ALLA PRESIDENZA
P0000763	SEGR.VICEPRESIDENTE FINANZE.EUROPA.COOP. SISTEMA AUTONOMIE
P0000764	SEGR.ASS.PROGR.TERRIT.,URBANISTICA.RETI INFRASTR.MAT.E IMMAT
P0000765	SEGR.ASS.ATTIVITA' PRODUTTIVE.PIANO ENERG.E SVIL.SOSTENIBILE
P0000766	SEGR.ASS.AGRICOLTURA
P0000767	SEGR.ASS.AMBIENTE, RIQUALIFICAZIONE URBANA
P0000768	SEGR.ASS.SICUR.TERRITORIALE.DIFESA SUOLO E COSTA.PROT.CIVILE
P0000769	SEGR.ASS.TURISMO. COMMERCIO
P0000770	SEGR.ASS.CULTURA. SPORT
P0000771	SEGR.ASS.SCUOLA.FORM.PROF.NALE.UNIVERSITA' E RICERCA.LAVORO
P0000772	SEGR.ASS.POLITICHE PER LA SALUTE
P0000773	SEGR.ASS.PROM.POLITICHE SOCIALI E INT.IMMIGRAZIONE.VOLONTAR.
P0000774	SEGR.ASS.SVIL.RIS.UMANE E ORGANIZZ.NE.COOP.SVIL.PROG.GIOVANI

AOO Intercenter:

Codice Struttura	Denominazione
000INCER	INTERCENT-ER - AGENZIA REGIONALE SVILUPPO MERCATI TELEMATICI

AOO AGREA:

Codice Struttura	Denominazione
000AGREA	AGREA - AGENZIA REGIONALE PER LE EROGAZIONI IN AGRICOLTURA

AOO Ibc:

Codice Struttura	Denominazione
A0000019	IBACN - ISTITUTO PER I BENI ARTISTICI, CULTURALI E NATURALI

AOO Ag. Protezione Civile:

Codice Struttura	Denominazione
00ARPCIV	AGENZIA REGIONALE DI PROTEZIONE CIVILE

AOO Atersir:

Codice Struttura	Denominazione
ATER-SIR	AGENZIA TERRITORIALE DELL'EMILIA-ROMAGNA

AOO Assemblée Legislativa:

Codice Struttura	Denominazione
D0000013	DIR. GEN. ASSEMBLEA LEGISLATIVA REGIONALE
00000396	GABINETTO DEL PRESIDENTE DELL'ASSEMBLEA LEGISLATIVA

2.2.4.3 Esempio di gruppi derivati da Organigramma

Si fornisce un esempio pratico per spiegare meglio la struttura di gruppi proposta come base per l'attribuzione di default dei diritti di accesso. Supponiamo che sotto l'AOO in esame ci sia solo l'apicale DG1, e che DG1 abbia solo il servizio S1, il quale a sua volta ha come strutture di III livello la PO PO1 e il Professional Pf1.

La corrispondente struttura dei gruppi e degli utenti assegnati in Doc/er diventa:

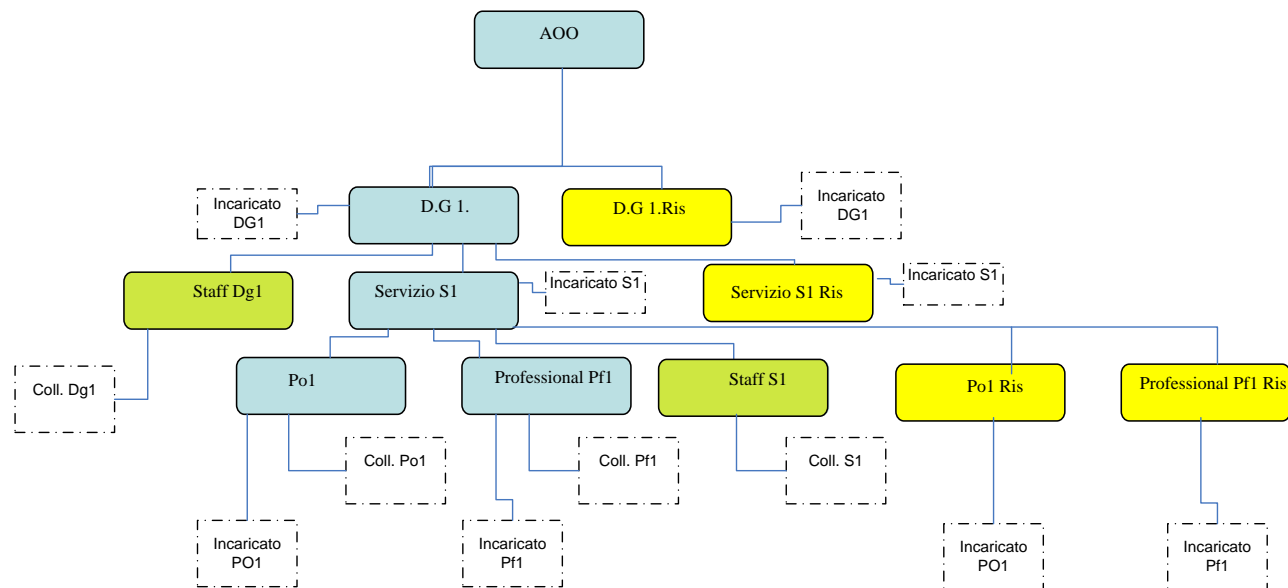


Fig. 2

Dove i gruppi corrispondenti alle strutture "reali" sono in celeste, i gruppi corrispondenti alle strutture fittizie di staff e per i riservati rispettivamente in verde e giallo.

2.2.4.4 Esempio di gruppi derivati da Organigramma

Gli utenti di dominio (RERSDM) vengono sincronizzati da pianta organica sulle strutture di Doc/er, coerentemente con le logiche delle assegnazioni e degli incarichi.

Poiché la gerarchia si declina propagando verso i nodi figli gli utenti afferenti ai nodi padri, a livello di dipendenza degli utenti dai gruppi si ha la seguente situazione:

Declinazione della gerarchia	DG	Servizio	PO/Prof	Componenti di default (alimentazione automatica)
Gruppo DG1	DG1			Responsabile DG1
Gruppo DG1 Staff	DG1	Staff DG1		Responsabile DG1 Dipendenti di staff del Direttore e non afferenti a PO/Prof
Gruppo S1	DG1	S1		Responsabile DG1 Responsabile S1
Gruppo S1 Staff	DG1	Staff S1		Responsabile DG1 Responsabile S1 Dipendenti dal servizio S1 e non afferenti a PO/Prof
Gruppo PO1	DG1	S1	PO1	Responsabile DG1 Responsabile S1 Responsabile PO1 Dipendenti da PO1
Gruppo PF1	DG1	S1	PF1	Responsabile DG1 Responsabile S1 Responsabile PF1 Dipendenti da Prof PF1
Gruppo DG1Ris	DG1			Responsabile DG1
Gruppo S1Ris	DG1	S1		Responsabile DG1 e S1
Gruppo PO1Ris	DG1	S1	PO1	Responsabile DG1, S1, PO1
Gruppo PF1Ris	DG1	S1	PF1	Responsabile DG1, S1, PF1

2.2.5 Gestione dei fascicoli

I fascicoli su Doc/er sono gestiti in corrispondenza a voci di titolare.

Per un generico SV integrato con Doc/er l'allineamento con il protocollo è gestito da Doc/er.

Allo stesso tempo i SV attualmente integrati con eG che manipolano fascicoli non devono preoccuparsi dell'allineamento anche di Doc/er perché EG aggiorna in automatico e in modo trasparente Doc/er (a tendere tutti i SV devono adeguare le loro interfacce per integrarsi pienamente con Doc/er).

Le ACL dei fascicoli devono essere sempre comunque specificate dai SV: peraltro esse non verranno automaticamente ereditate dai documenti ad essi appartenenti.

2.2.6 Gestione dei documenti

Per un generico SV integrato con Doc/er, eventuali necessità di integrazione con il sistema di protocollo o altri SV di registro legati a specifici repertori sono gestite attraverso Doc/er.

Allo stesso tempo i SV attualmente integrati con eG che manipolano documenti non devono preoccuparsi dell'allineamento anche verso Doc/er perché EG aggiorna in automatico e in modo trasparente Doc/er (anche se, come già detto, a tendere tutti i SV devono adeguare le loro interfacce per integrarsi pienamente con Doc/er).

Per i documenti e i loro permessi di accesso si ritiene preferibile l'adozione della modalità sincrona di allineamento tra il SV e Doc/er e viceversa, ma è comunque accettabile l'adozione di una modalità asincrona di invio, con l'implementazione di opportuni sistemi di allarme specifici in caso di fallimento delle operazioni di sincronizzazione.

Nel modello attuale, le ACL dei documenti ereditano al minimo le acl dei sottofascicoli/fascicoli di pertinenza.

3 PROGETTAZIONE DELL'INTEGRAZIONE DEI SV CON DOC/ER

La progettazione dell'integrazione del sistema SV con DOC/ER comprende le seguenti attività:

- la definizione delle problematiche di autenticazione (tipo di utenze da utilizzare, richiesta di credenziali applicative)
- il censimento sistematico delle tipologie documentarie trattate dal SV e dei metadati associati e gli opportuni accordi con ParER per la loro conservazione
- la definizione dei processi per l'individuazione delle azioni gestite dal SV che producono o gestiscono oggetti documentali e, per ciascuna, le esigenze di sincronizzazione tra il sistema Doc/er e il sistema verticale.

In particolare:

- devono essere definiti tutti le possibili azioni sui sistemi verticali che scatenano logicamente un aggiornamento verso Doc/er di oggetti documentali, anagrafiche, metadati, permessi di accesso
- devono essere definite delle azioni specifiche da intraprendere in caso di fallimento dell'aggiornamento.
- devono essere definite le modalità di integrazione tra il SV e sistema Doc/er (sincrona o asincrona) rispetto ai documenti e ai loro permessi di accesso
- la mappatura su Doc/er delle abilitazioni del verticale (gruppi e strutture organizzative alla base dei permessi documentali per fascicoli e documenti).

3.1 Autenticazione

In una prima fase solo il front end Doc/er è integrato con IAM.

Nel colloquio tra SV e Doc/er, la creazione della sessione avverrà attraverso il richiamo del metodo login del WS di autenticazione, che attualmente richiede uno userid e una password applicative. Al termine delle operazioni è buona norma richiamare il metodo di logout dello stesso WS per chiudere la sessione utente.

Nel presente documento si ipotizzerà che l'accesso ai servizi Docer avvenga sempre previa autenticazione e creazione di una sessione, e che la sessione sia poi correttamente conclusa al termine delle operazioni.

Solo in un secondo momento, per i SV integrati con i sistemi Iam o Federa, che necessitano di integrarsi con Doc/er con l'utente autenticato sul FE del SV, sarà possibile richiamare i servizi con tale utente. Al rilascio di questa implementazione saranno opportunamente aggiornate le linee guida.

Rimarrà peraltro possibile anche nella seconda fase del progetto l'utilizzo di utenze applicative, sia a salvaguardia dei SV non ancora integrati con IAM o Federa, o non adeguati alla logica di SSO a livello di back end, e per la integrazione dei processi attivati da agenti automatici.

3.2 Definizione delle tipologie documentarie e dei metadati

Il progettista del SV dovrà compilare il modulo fornito in appendice 6 con le tipologie documentarie che deve gestire, selezionandole dall'elenco fornito in appendice 4.

Se il SV ha necessità di gestire tipologie documentarie non ancora censite sul GDR o metadati aggiuntivi (rispetto ai metadati comuni a tutte le tipologie documentarie forniti in appendice 5) relativi a tipologie documentarie già in uso, si deve provvedere alla compilazione completa delle opportune informazioni sul modulo in appendice 6.

3.3 Definizione delle integrazioni per gli oggetti trattati dal SV

La definizione dei processi gestiti dal SV in termini di azioni, attori e ruoli, deve fornire al progettista del SV le informazioni che gli permettono di compilare la tabella in appendice 3 in cui, per ogni azione che preveda il trattamento di un oggetto documentale, dovranno essere compilate le chiamate dei WS opportuni, i parametri della chiamata, gli attori e i permessi relativi. In appendice 2 viene fornita una check list di azioni che richiedono l'integrazione del SV con Doc/er.

Per l'elenco dei servizi e dei metodi disponibili su Doc/er e i dettagli delle relative chiamate si rimanda all'appendice 1.

Nei paragrafi che seguono si intende illustrare il flusso delle chiamate per i casi d'uso più comuni e le regole d'uso definite per il sistema GDR in ambito regionale.

3.4 Gestione delle anagrafiche

Tramite il SV è possibile gestire le seguenti anagrafiche del sistema GDR:

- Anagrafiche custom
- gruppi
- utenti
- cartelle

È possibile accedere all'anagrafica di titolare in sola lettura; in questo caso vengono gestiti i diritti di accesso alle voci di indice sulla base della logica dei gruppi.

Se il SV ha necessità di gestire anagrafiche custom o gruppi specifici in relazione a logiche di business diverse da quella dei gruppi derivati dalle strutture dell'organigramma, il progettista dovrà compilare le opportune griglie fornite rispettivamente in appendice 7 e 8.

Deve essere opportunamente garantito l'allineamento tra il SV e il sistema Doc/er in maniera **sincrona** di eventuali modifiche a oggetti delle anagrafiche.

L'allineamento avviene attraverso i WS di amministrazione associati:

- create/update anagrafica custom
- create/update gruppo
- create/update utente
- create/update folder

Per la gestione degli utenti e dalla loro appartenenza ai gruppi, si evidenzia che:

- per inserimento di un nuovo gruppo le chiamate sono le seguenti:
 - Metodo `createGroup` del servizio di gestione documentale con tutti i metadati previsti per l'anagrafica;
 - Metodi `setUsersOfGroup`, `updateUsersOfGroup`, `setGroupsOfUser` o `updateGroupsOfUser` per gestire le associazioni di utenti e gruppi (membership);
- per l'aggiornamento di un gruppo esistente le chiamate sono le seguenti:
 - Metodo `updateGroup` del servizio di gestione documentale con tutti i metadati previsti per l'anagrafica;
 - Metodi `setUsersOfGroup`, `updateUsersOfGroup`, `setGroupsOfUser` o `updateGroupsOfUser` per gestire le associazioni di utenti e gruppi.

3.5 Gestione dei fascicoli e dei documenti

3.5.1 Sincronizzazione di documenti in fase di produzione

Il riversamento dei documenti nella fase di produzione (document) riguarda la realizzazione dei seguenti casi d'uso:

- A. riversamento dei *document* prodotti all'interno del sistema verticale di filiera e non presenti nel sistema Doc/er;
- B. aggiornamento dei *document* presenti in Doc/er (profilo e diritti).

Nel primo caso è richiesto che il sistema verticale riversi l'intera unità documentaria all'interno del sistema Doc/er depositando metadati, file e diritti nel sistema documentale e procedendo come segue:

- creazione documento principale: devono essere invocati nell'ordine i seguenti metodi:
 - Metodo `createDocument` del servizio di gestione documentale con tutti i metadati previsti e con i metadati `TIPO_COMPONENTE=PRINCIPALE` e `TYPE_ID` valorizzato alla tipologia documentaria;
 - Metodo `setACLDocument` del servizio di gestione documentale per l'assegnazione dei diritti al documento;
- creazione allegati (annessi/annotazioni): per ogni allegato devono essere invocati nell'ordine i seguenti metodi:
 - Metodo `createDocument` del servizio di gestione documentale con tutti i metadati previsti e con i metadati `TIPO_COMPONENTE=ALLEGATO` (o `ANNESSO/ANNOTAZIONE`) e `TYPE_ID` valorizzato alla tipologia documentaria;
 - Metodo `setACLDocument` del servizio di gestione documentale per l'assegnazione dei diritti all'allegato; Quando il document diventa Record (attraverso la protocollazione o la repertoriazione ovvero registrazione particolare) gli allegati diventano parte integrante del documento e i diritti degli allegati sono allineati con quelli del documento principale; gli annessi e le annotazioni anche dopo la trasformazione in Record mantengono i loro diritti distinti da quelli del documento principale.

- correlazione documenti dell'unità documentaria: con la lista degli identificativi restituiti dai metodi createDocument deve essere costruita la catena dei correlati ai fini della protocollazione/registrazione/fascicolazione invocando il seguente metodo:
 - Metodo addRelated del servizio di gestione documentale con tutti i dati previsti;

Infine, nei casi di aggiornamento del profilo dei documenti o dei diritti si devono invocare i seguenti metodi:

- Metodo updateProfileDocument del servizio di gestione documentale per la modifica del profilo;
- Metodo setACLDocument del servizio di gestione documentale per l'assegnazione dei diritti.

3.5.2 Richieste di protocollazione e/o fascicolazione

Il SV che abbia necessità di protocollazione e/o fascicolazione deve inoltrare le rispettive richieste a Doc/er, in particolare i casi d'uso da implementare sono i seguenti:

- Protocollazione ed eventuale fascicolazione di documenti prodotti all'interno del sistema verticale e non ancora presenti nel sistema Doc/er (creazione contestuale di "Document" e "Record");
- Protocollazione ed eventuale fascicolazione di documenti già presenti in Doc/er ;
- Fascicolazione di documenti prodotti all'interno del sistema verticale e non ancora presenti nel sistema Doc/er;
- Fascicolazione di documenti presenti in Doc/er;
- Aggiornamento di documenti presenti in Doc/er.

Nei casi in cui l'unità documentaria non fosse già presente nel sistema Doc/er è richiesto che il sistema verticale di filiera riversi l'intera unità documentaria all'interno del sistema Doc/er depositando metadati, file e diritti nel sistema documentale e procedendo come segue:

- creazione documento principale: devono essere invocati nell'ordine i seguenti metodi:
 - Metodo createDocument del servizio di gestione documentale con tutti i metadati previsti esclusi i dati di registrazione e fascicolazione e con i metadati:
STATO_ARCHIVISTICO=1 (documento generico) e
TIPO_COMPONENTE=PRINCIPALE;
 - Metodo setACLDocument del servizio di gestione documentale per l'assegnazione dei diritti al documento;
- creazione allegati (annessi/annotazioni): per ogni allegato devono essere invocati nell'ordine i seguenti metodi:
 - Metodo createDocument del servizio di gestione documentale con tutti i metadati previsti esclusi i dati di registrazione e fascicolazione e con i metadati STATO_ARCHIVISTICO=1 (documento generico) e TIPO_COMPONENTE=ALLEGATO (ANNESSO/ANNOTAZIONE);
 - Metodo setACLDocument del servizio di gestione documentale per l'assegnazione dei diritti all'allegato;

- correlazione documenti dell'unità documentaria: con la lista degli identificativi restituiti dai metodi createDocument deve essere costruita la catena dei correlati ai fini della protocollazione/fascicolazione invocando il seguente metodo:
 - Metodo addRelated del servizio di gestione documentale con tutti i dati previsti;

Per le richieste di protocollazione e fascicolazione contestuale si deve procedere come segue:

- Richiesta di protocollazione dell'unità documentaria deve essere invocato il seguente metodo:
 - Metodo protocollaById del servizio di protocollazione con tutti i metadati previsti (compresi quelli di classifica e fascicolo);

Per le richieste di sola fascicolazione si deve procedere come segue:

- Metodo fascicolaById del servizio di protocollazione con tutti i metadati previsti;

Infine, nei casi di aggiornamento del profilo dei documenti o dei diritti si devono invocare i seguenti metodi:

- Metodo updateProfileDocument del servizio di gestione documentale per la modifica del profilo;
- Metodo setACLDocument del servizio di gestione documentale per l'assegnazione dei diritti.

3.5.3 Richieste di repertorizzazione (Registrazione Particolare)

Il SV che abbia necessità di repertorizzazione ovvero registrazione particolare, deve inoltrare la richiesta a Doc/er, in particolare i casi d'uso da implementare sono i seguenti:

- repertorizzazione ed eventuale fascicolazione di documenti prodotti all'interno del sistema verticale e non ancora presenti nel sistema Doc/er;
- repertorizzazione ed eventuale fascicolazione di documenti già presenti in Doc/er ;
- aggiornamento dei documenti presenti in Doc/er.

Nel primo caso è richiesto che il sistema verticale riversi l'intera unità documentaria all'interno del sistema Doc/er depositando metadati, file e diritti nel sistema documentale e procedendo come segue:

- creazione documento principale: devono essere invocati nell'ordine i seguenti metodi :
 - Metodo createDocument del servizio di gestione documentale con tutti i metadati previsti esclusi i dati di protocollazione, registrazione e fascicolazione e con i metadati STATO_ARCHIVISTICO=1 (documento generico), TIPO_COMPONENTE=PRINCIPALE e TYPE_ID valorizzato alla tipologia documentaria;
 - Metodo setACLDocument del servizio di gestione documentale per l'assegnazione dei diritti al documento;

- creazione allegati (annessi/annotazioni): per ogni allegato devono essere invocati nell'ordine i seguenti metodi:
 - Metodo `createDocument` del servizio di gestione documentale con tutti i metadati previsti esclusi i dati di protocollazione, registrazione e fascicolazione e con i metadati `STATO_ARCHIVISTICO=1` (documento generico), `TIPO_COMPONENTE=ALLEGATO` (ANNESSO/ANNOTAZIONE) e `TYPE_ID` valorizzato alla tipologia documentaria;
 - Metodo `setACLDocument` del servizio di gestione documentale per l'assegnazione dei diritti all'allegato;
- correlazione documenti dell'unità documentaria: con la lista degli identificativi restituiti dai metodi `createDocument` deve essere costruita la catena dei correlati ai fini della protocollazione invocando il seguente metodo:
 - Metodo `addRelated` del servizio di gestione documentale con tutti i dati previsti;
- Richiesta di registrazione particolare dell'unità documentaria deve essere invocato il seguente metodo:
 - Metodo `registraById` del servizio di registrazione particolare con tutti i metadati previsti;

Nel secondo caso, ovvero di repertoriazione di documenti già esistenti nel sistema Doc/er è sufficiente effettuare la sola richiesta di registrazione particolare dell'unità documentaria invocando il solo metodo `registraById` del servizio di registrazione particolare di Doc/er.

Infine, nei casi di aggiornamento del profilo dei documenti o dei diritti si devono invocare i seguenti metodi:

- Metodo `updateProfileDocument` del servizio di gestione documentale per la modifica del profilo;
- Metodo `setACLDocument` del servizio di gestione documentale per l'assegnazione dei diritti.

3.5.4 Azioni di Modifica documento

E' necessario censire accuratamente, nella tabella di cui all'appendice 4, tutte le azioni che producono modifiche sugli oggetti documentali gestiti dal SV, sui loro metadati, sulle loro relazioni e ACL.

Ad esempio

- annullamento
- modifica registrazione
- smistamento/invio
- restituzione
- assegnazione
- adozione di un atto

etc

Le modifiche di profilo che non attengono ai dati di registrazione vengono gestite mediante chiamate al metodo *UpdateProfileDocument*.

Le modifiche che attengono ai dati di registrazione vengono invece richieste mediante chiamate al metodo *registraById*

Al contrario Doc/er non mette a disposizione non espone nessun servizio con cui richiedere al Sistema di protocollo o a un SV di registro di annullare una registrazione. Pertanto se il SV deve verificare che un documento sia annullato deve richiederne lo stato a Doc/er.

3.5.5 Creazione nuovi fascicoli

Il generico SV può richiedere la creazione di nuovi fascicoli al sistema Doc/er che la inoltra al sistema di protocollo e restituisce l'esito della richiesta.

- La richiesta di creazione di un nuovo fascicolo deve invocare il seguente metodo:
 - Metodo *createFascicolo* del servizio di fascicolazione con tutti i metadati previsti;
- La creazione deve seguire la seguente logica che prevede nel caso più generale:
 - Verifica esistenza voce di indice in Doc/er
 - Verifica esistenza del fascicolo (eventuale)
 - Chiamata ws *creaFascicolo* in Doc/er
 - Impostazione delle ACL
- Questo avviene mediante le seguenti chiamate:
 - Metodo *GetTitolario*
 - Metodo *GetFascicolo*
 - Metodo *CreateFascicolo*
 - Metodo *SetAcclFascicolo*

Nelle ACL vanno specificati i permessi con la logica dei gruppi sopra descritta.

La chiamata deve essere sincrona. Nei casi in cui il SV non possa permettersi di far fallire l'operazione che ha generato la chiamata, si deve prevedere un meccanismo di recupero asincrono per le chiamate andate in errore.

3.5.6 Modifica fascicoli

La modifica di un fascicolo esistente in Doc/er deve essere gestita attraverso le seguenti chiamate:

- Metodo ws *UpdateFascicolo* in Doc/er
- Impostazione permessi su Doc/er (*SetAcclFascicolo*)

Esistono azioni che anche implicitamente modificano i diritti di accesso ai fascicoli.

Pertanto l'operazione di sincronizzazione dei diritti di accesso deve essere fatta andando a intercettare tutte le azioni della vita del fascicolo che cambiano l'ACL, censendole in fase di analisi nella tabella di cui all'appendice 4:

- modifica profilo
 - invia
 - smista
 - prendi in carico
 - restituisci
 - modifica permessi
- etc

Il metodo da chiamare è setACLFascicolo.

3.5.7 Modello di integrazione per l'aggiornamento di documenti, fascicoli e loro ACL : sincrona o asincrona

Laddove non esistono criticità particolari, l'integrazione tra il SV e Doc/er sarà sincrona: il Sistema verticale invoca i web services esposti da Doc/er; se Doc/er è disponibile allora tali web services, in caso di successo, restituiscono immediatamente i risultati dell'elaborazione al Sistema verticale che li ha invocati.

Nel caso di aggiornamento sincrono deve essere decisa la strategia da intraprendere nel caso di fallimento della chiamata:

- fallimento dell'operazione master del SV
- invio a una coda di elaborazione asincrona e sollevamento di un alert, in particolare in caso di errori di sistema.

Nel secondo caso si deve prevedere una procedura di integrazione asincrona per gestire le chiamate fallite.

Devono essere implementate le seguenti funzioni:

- gestione di una coda di chiamate ancora da elaborare rispetto al Sistema Doc/er che memorizzi tutte le informazioni utili alla ripresa del colloquio con Doc/er
- creazione di una procedura batch che sistematicamente vada ad interrogare la disponibilità del Sistema Doc/er. Nel momento in cui tale procedura trova il Sistema Doc/er disponibile, allora si occuperà di elaborare gli oggetti presenti nella coda di elaborazione, seguendo l'ordine di inserimento previsto dal SV.

In base allo stato di elaborazione rispetto al Sistema Doc/er dell'oggetto in elaborazione, la procedura completerà le attività previste invocando i web services opportuni e aggiornando le informazioni dello stato dell'oggetto nel SV.

Nel caso invece che venga implementato un sistema di aggiornamento asincrono, devono essere previsti sistemi di allarme specifici in caso di fallimento delle operazioni di integrazione.

3.6 Attribuzione dei diritti di accesso agli oggetti documentali

A fronte della strutturazione dei gruppi sopra descritta, sono state definite le seguenti linee guida per le attribuzioni agli oggetti documentali delle liste di controllo di accesso;

- i diritti agli oggetti documentali sono definiti a livello di gruppo e non di singolo utente
- i sistemi verticali, per ogni oggetto (documento, voce di indice, fascicolo) che manipolano su Doc/er, devono produrre una ACL adatta al linguaggio di Doc/er, ovvero definire con la logica applicativa quali sono i gruppi che corrispondono alla logica di visibilità dell'oggetto di business, e trasferirle a Doc/er che li scrive nell'ACL del documento.

Fino a quando si utilizzeranno utenze applicative per il colloquio tra SV e Doc/er, è necessario inserire anche l'utenza applicativa nell'ACL dell'oggetto, ovviamente anche con diritti di modifica nel caso il SV gestisca azioni che modificano il documento.

- dal FE Doc/er l'accesso di un utente a documenti, fascicoli, voci di titolare, viene permesso se appartiene a un gruppo scritto nell'ACL dell'oggetto, oltre che alla stessa utenza applicativa.
- i sistemi verticali devono fare una chiamata a Doc/er di modifica dell'ACL di un oggetto ogni volta che un evento anche implicito può modificarla.
- per un documento/fascicolo riservato, deve venire inserita nell'ACL dell'oggetto il gruppo dei riservati corrispondente alla struttura a cui si vuole attribuire il documento/fascicolo.
- gli oggetti (documenti/fascicoli) prodotti dai sistemi verticali **non** sono modificabili attraverso il FE di Doc/er, poiché questo significherebbe che le modifiche significative ai metadati dovrebbero essere a loro volta riportate sul verticale, innescando ulteriori meccanismi di sincronizzazione quindi se si vuole evitare la onerosa sincronizzazione bidirezionale delle modifiche, i sistemi verticali dovrebbero scrivere solo ACL come la seguente:

Id Oggetto	Gruppo	Azioni possibili
NNN	Gruppo yyy	Read

3.6.1 Traduzione in ACL Doc/er dei diritti del SV

Le logiche di attribuzione di diritti di accesso agli oggetti documentali sui SV integrati con Doc/er dovrebbero essere semplificate a causa della difficoltà di tradurre in un linguaggio comune concetti come ruoli e profili assenti su Doc/er.

Di norma quindi dovrebbe essere sufficiente una logica basata sull'appartenenza degli utenti, che hanno diritti sugli oggetti documentali, alle strutture della pianta organica, poiché l'allineamento dei gruppi e dei loro componenti è garantito come servizio automatico di Doc/er e quindi fruibile da tutti i SV.

In questo caso è consigliabile attribuire i diritti di accesso fino alle strutture di III livello, definite più sopra, ed evitare il più possibile attribuzioni puntuali a singoli utenti.

Ad esempio: se sul SV l'ACL di un oggetto è scritta come segue:

Id Doc o Id Fasc	Struttura o matricola	Codice	Azioni possibili
NNN	Matricola	123	Read

Supponendo che l'utente con matricola 123 appartenga alla struttura X di codice 00000456, su Doc/er dovrebbe venire tradotta come segue:

Id Doc o Id Fasc	Gruppo	Azioni possibili
NNN	00000456	Read

Nei casi in cui ruoli e profili siano fondamentali per l'attribuzione dei permessi di visibilità, è necessario che il SV crei, curi e gestisca gruppi omologhi alle logiche di processo che sottendono le logiche di attribuzione dei diritti.

3.7 SV di registro

I SV di registro oltre che implementare tutte le funzionalità previste per i SV di filiera, gestiscono anche:

- la sincronizzazione verso Doc/er di tutte le operazioni relative alla registrazione particolare dei documenti, nello specifico: Memorizzazione dei metadati di registrazione e trasformazione in un Record, procedendo come segue
 - Riversamento dell'unità documentaria in Doc/er con le stesse modalità previste per i SV di filiera;
 - Metodo registraDocumento del servizio di gestione documentale con tutti i metadati previsti;
- l'allineamento di eventuali modifiche alla registrazione particolare (per esempio in caso di annullamento della registrazione e/o modifica dell'oggetto della registrazione e/o modifica di mittenti, destinatari) tramite
 - Metodo registraDocumento del servizio di gestione documentale con tutti i metadati previsti;

Per consentire a un SV di filiera di poter richiedere una registrazione particolare (repertoriazione), i SV di registro devono prevedere un componente, definito "provider", la cui interfaccia in termini di request e response è standard, con xsd definiti dal modello (appendice 9), che implementi la registrazione di repertorio con specificazione del tipo di registro.

Questa modalità permette di esporre verso Doc/er la registrazione particolare dei documenti da parte del SV di registro.

Nei casi di registrazione particolare dei documenti attraverso il "provider" di registrazione, quando cioè un documento viene registrato attraverso l'invocazione da parte di un SV di filiera del servizio di registrazione particolare di Doc/er, non è necessario che il SV di registro effettui alcun riversamento dell'unità documentaria in Doc/er, in quanto già creato in Doc/er dal SV di filiera, ed inoltre non sarà necessaria la memorizzazione dei metadati di registrazione e trasformazione in un Record, in quanto tale operazione è effettuata automaticamente dal servizio di registrazione particolare esposto da Doc/er stesso.

4 MODELLO ORGANIZZATIVO DELL'INTEGRAZIONE

Poiché il sistema di gestione documentale è trasversale a tutto l'Ente e deve essere utilizzato nel rispetto delle policy e delle regole che lo governano, ogni volta che un SV ha necessità di integrazioni con il sistema di GDR, è necessario prevedere una serie di azioni per la verifica e la garanzia del rispetto di tali regole.

Nella tabella seguente sono riportate le azioni da eseguire.

N.Step	Fase	Azione	Attori	Input	Output	Note
1	Progettazione	Invio dei moduli per l'analisi di integrazione con GDR al Responsabile GDR e Archivio	Progettista del SV		Moduli in appendice 3, 6, 7, 8	
2	Progettazione	Supporto al progettista per la definizione degli oggetti di integrazione, verifica e approvazione delle specifiche documentali e archivistiche di integrazione	Responsabile GDR e Archivio	Moduli in appendice 3, 6, 7, 8	Moduli in appendice 3, 6, 7, 8 approvati	
3	Progettazione	Invio dei moduli per l'analisi di integrazione con GDR al Responsabile Governance IT	Progettista del SV	Moduli in appendice 3, 6, 7, 8 approvati	Moduli in appendice 3, 6, 7, 8 approvati	
4	Progettazione	Verifica della compatibilità del SV con le presenti linee guida, e comunicazione al progettista di eventuali nuove configurazioni	Responsabile Governance IT	Moduli in appendice 3, 6, 7, 8 approvati	Moduli in appendice 3, 6, 7, 8 approvati e visti da Responsabile Governance IT	Ogni modifica delle specifiche fino alle verifiche preliminari al rilascio in produzione deve essere sottoposta allo stesso flusso di approvazione e verifica

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

N.Step	Fase	Azione	Attori	Input	Output	Note
5	Verifiche tecniche preliminari al rilascio in produzione	Richiesta al Responsabile Governance IT dei test di compatibilità con GDR	Progettista del SV		SV da verificare	Da richiedere contestualmente alla richiesta di verifica di accessibilità e sicurezza
6	Verifiche tecniche preliminari al rilascio in produzione	Verifica tecnica di compliance con GDR	Responsabile Governance IT	SV da verificare	Esito della verifica	Da reiterare fino a esito positivo
7	Collaudo finale	Collaudo finale congiunto di compliance tecnica e archivistica con GDR	<ul style="list-style-type: none"> • Progettista SV • Responsabile GDR e Archivio • Responsabile Governance IT 	Esito verifica test IT Governance positivo	Esito finale del collaudo	

5 L'AMBIENTE PER IL TEST DI INTEGRAZIONE CON DOC/ER

E' a disposizione dei progettisti un ambiente di test utilizzabile per il test di integrazione dei SV con Doc/er.

5.1 Servizi WEB

Attualmente sono a disposizione i seguenti WS:

- **Autenticazione**

<https://docer-test.ente.regione.emr.it/docersystem/services/AuthenticationService?wsdl>

login

logout

getUserInfo

VerifyToken

- **DocerServices**

<https://docer-test.ente.regione.emr.it/WSDocer/services/DocerServices?wsdl>

I cui metodi attualmente a disposizione sono:

createDocument

getACLDocument

setACLDocument

getProfileDocument

updateProfileDocument

protocollaDocumento

registraDocumento

fascicolaDocumento

downloadDocument

downloadVersion

getVersions

addNewVersion

replaceLastVersion

deleteDocument

lockDocument

unlockDocument

getLockStatus

getHistory

getUserRights

getRelatedDocuments

addRelated

removeRelated
getRiferimentiDocuments
addRiferimentiDocuments
removeRiferimentiDocuments
searchDocuments
getDocumentTypes
createEnte
updateEnte
getEnte
createAOO
updateAOO
getAOO
createTitolario
updateTitolario
getTitolario
getACLTitolario
setACLTitolario
createFascicolo
updateFascicolo
getFascicolo
getACLFascicolo
setACLFascicolo
createAnagraficaCustom
updateAnagraficaCustom
getAnagraficaCustom
searchAnagrafiche
createFolder
updateFolder
deleteFolder
setACLFolder
getACLFolder
getFolderDocuments
addToFolderDocuments
removeFromFolderDocuments
searchFolders
createUser
updateUser
getUser
searchUsers

createGroup
updateGroup
getGroup
searchGroups
setUsersOfGroup
updateUsersOfGroup
getUsersOfGroup
setGroupsOfUser
updateGroupsOfUser
getGroupsOfUser

- **WSProtocollazione**

<https://docer-test.ente.regione.emr.it/WSProtocollazione/services/WSProtocollazione?wsdl>

I cui metodi attualmente a disposizione sono:

readConfig
writeConfig
protocollaById

- **WSRegistrazione**

<https://docer-test.ente.regione.emr.it/WSRegistrazione/services/WSRegistrazione?wsdl>

I cui metodi attualmente a disposizione sono:

readConfig
writeConfig
protocollaById

- **WSFascicolazione**

<https://docer-test.ente.regione.emr.it/WSFascicolazione/services/WSFascicolazione?wsdl>

I cui metodi attualmente a disposizione sono:

readConfig
writeConfig
CreaFascicolo
fascicolaById
forzaNuovoFascicolo
updateAclFascicolo
updateFascicolo

- **WSConservazione**

<https://docer-test.ente.regione.emr.it/WSConservazione/services/WSConservazione?wsdl>

I cui metodi attualmente a disposizione sono:

readConfig

writeConfig

versamento

5.2 Front End

Il FE web è disponibile all'indirizzo:

<https://docer-test.ente.regione.emr.it/docer>

6 AMBIENTE DI PRODUZIONE

(da completare al rilascio, compresi i limiti fisici degli oggetti trattati, ovvero dimensioni massime dei files caricabili sul sistema, etc)

7 APPENDICI

7.1 Appendice 1: Specifiche tecniche dei servizi e delle interfacce del modello GeDoc

v. All. 1

7.2 Appendice 2: Check list di controllo delle azioni di integrazione con il sistema documentale

Azione	Descrizione	Altre specifiche o note
Sincronizzazione Gruppi Specifici	Gruppi specifici diversi dalla struttura organizzativa che è necessario sincronizzare da parte del sistema verticale	In caso di Richiesto=SI, specificare perché la struttura organizzativa non è sufficiente per assegnare diritti ai documenti e riempire il foglio "Gruppi Specifici"
Sincronizzazione Anagrafiche Custom	Anagrafiche custom che è necessario sincronizzare da parte del sistema verticale	In caso di Richiesto=SI, descrivere l'anagrafica custom e riempire il modulo "Anagrafiche Custom"
Riversamento Document	Riversamento dei documenti in fase di formazione o dei documenti che poi devono essere registrati al protocollo o qualche registro particolare	
Riversamento Record	Riversamento dei documenti già registrati all'interno del sistema verticale di registro	Riservato ai soli verticali che gestiscono in autonomia dei propri registri (verticali di registro). Specificare se i documenti sono riversati con indicazioni di conservazione oppure se questi documenti vanno conservati indipendentemente dalle informazioni di profilo con cui sono riversati
Richieste di protocollazione	Richiesta di protocollazione di Document o Record riversati dal sistema verticale	Specificare se le richieste di protocollazione sono in entrata e/o uscita e/o interne

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Azione	Descrizione	Altre specifiche o note
Richieste di creazione nuovi fascicoli	Richiesta di creazione nuovi fascicoli	Specificare quali fascicoli devono essere creati dal sistema verticale
Richieste di fascicolazione	Richieste di fascicolazione o modifica della fascicolazione dei Document e dei Record già riversati	Specificare i fascicoli utilizzati dal sistema verticale per la fascicolazione dei documenti
Richieste di registrazione particolare	Richiesta di registrazione particolare di Document riversati dal sistema verticale	Specificare i registri ai quali è richiesta la registrazione dei documenti da parte del sistema verticale
Recupero informazioni conservazione	Recupero dello stato di conservazione sostitutiva dei documenti riversati	
Richieste invio PEC	Richieste di invio tramite PEC ai destinatari di registrazioni di protocollo in uscita	Indicare per quali destinatari si richiede l'invio tramite PEC
Interrogazione titolare e fascicoli	Accesso al titolare di classificazione e ai fascicoli da parte del sistema verticale	Indicare quali voci di titolare e quali fascicoli si deve poter accedere da parte del sistema verticale
Ricerche di documenti	Ricerche di documenti già riversati	Indicare se il sistema verticale accede esclusivamente ai propri documenti o se deve poter accedere anche a documenti versati da altre applicazioni (p.e. accesso al fascicolo completo, ecc...)
Richieste di Verifiche delle firme di un documento	Verifica validità, CRL, ecc... di tutte le firme digitali di un documento	
Richieste di Verifiche del formato di un documento	Verifica del formato di un documento indipendentemente dalla sua estensione	
Messa a disposizione di un servizio per la registrazione particolare	Esposizione da parte del verticale di registro del Provider per rendere possibile la registrazione particolare dei documenti nel proprio registro da parte degli altri verticali	Riservato ai soli verticali che gestiscono in autonomia dei propri registri (verticali di registro). Specificare il registro gestito e le tipologie documentarie trattate.

7.3 Appendice 3: Tabella per il censimento di azioni, attori e permessi per il progetto di integrazione di un Sistema Verticale

Dati archivistici e di processo					Dati tecnici/informatici		
Azione	Funzione per eseguire l'azione sul SV	Metadati di chiamata	Attori	Note	WS Doc/er invocato	Invocazione sincrona o asincrona	Previste azioni di ripristino

7.4

7.5 Appendice 4: Tipologie documentarie gestite e relativi metadati aggiuntivi

Ente /Area	Codice Ente	Codice Area	Tipologia documentaria	Tipo atto	Metadati opzionali	Tipo
Giunta	R_emiro	AOO_EMR				
			Atti dell'Assessore	Atto collegiale	NUMERO DI ADOZIONE	VARCHAR2
					DATA DI ADOZIONE	DATE
					LUOGO DI ADOZIONE	VARCHAR2
					FIRMATARIO	VARCHAR2
					STRUTTURA ADOTTANTE	VARCHAR2
					ESTREMI DI PUBBLICAZIONE SUL BUR	VARCHAR2
					DATA PUBBLICAZIONE BU	DATE
					ESTREMI DI PUBBLICAZIONE SUL SUPPLEMENTO BUR	VARCHAR2
					DATA PUBBLICAZIONE SBU	DATE
			PROTOCOLLO REVOCA ATTO	VARCHAR2		

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Ente /Area	Codice Ente	Codice Area	Tipologia documentaria	Tipo atto	Metadati opzionali	Tipo	
					DATA REVOCA	DATE	
			Contratti di lavoro COMPARTO				
			Contratti di lavoro DIRIGENZA				
			Documenti del Commissario Delegato per la ricostruzione				
			Delibere del Consiglio delle Autonomie Locali				
			Decreti del Commissario delegato per la ricostruzione				
			Decreti del Commissario Straordinario per interventi relativi al rischio idrogeologic				
			Atti monocratici Giunta	Atti del dirigente	NUMERO DI ADOZIONE	VARCHAR2	
						DATA DI ADOZIONE	DATE
						LUOGO DI ADOZIONE	VARCHAR2
						FIRMATARIO	VARCHAR2
						STRUTTURA ADOTTANTE	VARCHAR2
						ESTREMI DI PUBBLICAZIONE SUL BUR	VARCHAR2
						DATA PUBBLICAZIONE BU	DATE
						ESTREMI DI PUBBLICAZIONE SUL SUPPLEMENTO BUR	VARCHAR2
						DATA PUBBLICAZIONE SBU	DATE
						PROTOCOLLO REVOCA ATTO	VARCHAR2
						DATA REVOCA	DATE

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Ente /Area	Codice Ente	Codice Area	Tipologia documentaria	Tipo atto	Metadati opzionali	Tipo
			Documento Unico Regolarità Contributiva			
			Repertorio Fatture in ingresso		COD.FISC. /P.IVA BENEFICIARIO	VARCHAR2
					DATA SCADENZA	DATE
			Delibere di giunta	Delibere	NUMERO DI ADOZIONE	VARCHAR2
					DATA DI ADOZIONE	DATE
					LUOGO DI ADOZIONE	VARCHAR2
					ESTREMI DI PUBBLICAZIONE SUL BUR	VARCHAR2
					DATA PUBBLICAZIONE BU	DATE
					ESTREMI DI PUBBLICAZIONE SUL SUPPLEMENTO BUR	VARCHAR2
					DATA PUBBLICAZIONE SBU	DATE
					PROTOCOLLO REVOCA ATTO	VARCHAR2
					DATA REVOCA	DATE
					NUMERO PROT INVIO ASSEMBLEA LEGISLATIVA	VARCHAR2
					DATA INVIO ASSEMBLEA LEGISLATIVA	DATE
					NUMERO PROT ISCRIZIONE ASSEMBLEA LEGISLATIVA	VARCHAR2
					DATA ISCRIZIONE ASSEMBLEA LEGISLATIVA	DATE
					NUMERO PROT RECEPIMENTO ASSEMBLEA LEGISLATIVA	VARCHAR2
					DATA RECEPIMENTO ASSEMBLEA LEGISLATIVA	DATE
					APPROVATE DA ASSEMBLEA LEGISLATIVA	CHECK
			NUMERO DI LEGGE	VARCHAR2		
			DATA DI LEGGE	DATE		
			NUMERO REGOLAMENTO	VARCHAR2		

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Ente /Area	Codice Ente	Codice Area	Tipologia documentaria	Tipo atto	Metadati opzionali	Tipo	
					DATA REGOLAMENTO	DATE	
					NUMERO DELIBERA ASSEMBLEARE	VARCHAR2	
					DATA DELIBERA ASSEMBLEARE	DATE	
					NUMERO DELIBERAZIONE LEGISLATIVA	VARCHAR2	
					DATA DELIBERAZIONE LEGISLATIVA	DATE	
			Intese del commissario delegato per la ricostruzione				
			Non Protocollati				
			Ordinanze del Commissario delegato per la ricostruzione	Ordinanze			
			Circolari del Commissario delegato per la ricostruzione	Circolari			
			Provvedimendi della Commissione Unica				
			Decreti del presidente	Decreti			
			Protocolli di intesa		LUOGO DI FIRMA DEL PROTOCOLLO / ACCORDO	VARCHAR2	
						DATA DI FIRMA DEL PROTOCOLLO/ACCORDO	DATE
						FIRMATARI PER CONTO DELLA REGIONE	VARCHAR2
						LUOGO DI CONSERVAZIONE DELL'ORIGINALE	VARCHAR2
Intercenter	r_emiro	AOO_IC					
			Atti monocratici IC	Atti dirigente	NUMERO DI ADOZIONE	VARCHAR2	
					DATA DI ADOZIONE	DATE	

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Ente /Area	Codice Ente	Codice Area	Tipologia documentaria	Tipo atto	Metadati opzionali	Tipo
					LUOGO DI ADOZIONE	VARCHAR2
					FIRMATARIO	VARCHAR2
					STRUTTURA ADOTTANTE	VARCHAR2
					ESTREMI DI PUBBLICAZIONE SUL BUR	VARCHAR2
					DATA PUBBLICAZIONE BU	DATE
					ESTREMI DI PUBBLICAZIONE SUL SUPPLEMENTO BUR	VARCHAR2
					DATA PUBBLICAZIONE SBU	DATE
					PROTOCOLLO REVOCA ATTO	VARCHAR2
					DATA REVOCA	DATE
			Non protocollati			

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Ente /Area	Codice Ente	Codice Area	Tipologia documentaria	Tipo atto	Metadati opzionali	Tipo
Agrea	r_emiro	AOO_AG				
			Fatture			
			Atti monocratici AG	Atti dirigente	NUMERO DI ADOZIONE	VARCHAR2
					DATA DI ADOZIONE	DATE
					LUOGO DI ADOZIONE	VARCHAR2
					FIRMATARIO	VARCHAR2
					STRUTTURA ADOTTANTE	VARCHAR2
					ESTREMI DI PUBBLICAZIONE SUL BUR	VARCHAR2
					DATA PUBBLICAZIONE BU	DATE
					ESTREMI DI PUBBLICAZIONE SUL SUPPLEMENTO BUR	VARCHAR2
					DATA PUBBLICAZIONE SBU	DATE
					PROTOCOLLO REVOCA ATTO	VARCHAR2
			DATA REVOCA	DATE		
			Non protocollati			
			Liquidazioni			
			Convenzioni			
			Durc			
Ibacn	R_emiro	AOO_IB				
			Atti monocratici IB	Atti dirigente	NUMERO DI ADOZIONE	VARCHAR2
					DATA DI ADOZIONE	DATE
					LUOGO DI ADOZIONE	VARCHAR2
					FIRMATARIO	VARCHAR2
					STRUTTURA ADOTTANTE	VARCHAR2
					ESTREMI DI PUBBLICAZIONE SUL BUR	VARCHAR2

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

					DATA PUBBLICAZIONE BU	DATE
					ESTREMI DI PUBBLICAZIONE SUL SUPPLEMENTO BUR	VARCHAR2
					DATA PUBBLICAZIONE SBU	DATE
					PROTOCOLLO REVOCA ATTO	VARCHAR2
					DATA REVOCA	DATE
			Atti collegiali IB	Delibere di consiglio	NUMERO DI ADOZIONE	VARCHAR2
					DATA DI ADOZIONE	DATE
					LUOGO DI ADOZIONE	VARCHAR2
					ESTREMI DI PUBBLICAZIONE SUL BUR	VARCHAR2
					DATA PUBBLICAZIONE BU	DATE
					ESTREMI DI PUBBLICAZIONE SUL SUPPLEMENTO BUR	VARCHAR2
					DATA PUBBLICAZIONE SBU	DATE
					PROTOCOLLO REVOCA ATTO	VARCHAR2
					DATA REVOCA	DATE
					NUMERO PROT INVIO ASSEMBLEA LEGISLATIVA	VARCHAR2
					DATA INVIO ASSEMBLEA LEGISLATIVA	DATE
					NUMERO PROT ISCRIZIONE ASSEMBLEA LEGISLATIVA	VARCHAR2
					DATA ISCRIZIONE ASSEMBLEA LEGISLATIVA	DATE
					NUMERO PROT RECEPIMENTO ASSEMBLEA LEGISLATIVA	VARCHAR2
					DATA RECEPIMENTO ASSEMBLEA LEGISLATIVA	DATE
					APPROVATE DA ASSEMBLEA LEGISLATIVA	CHECK
					NUMERO DI LEGGE	VARCHAR2
					DATA DI LEGGE	DATE

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

					NUMERO REGOLAMENTO	VARCHAR2
					DATA REGOLAMENTO	DATE
					NUMERO DELIBERA ASSEMBLEARE	VARCHAR2
					DATA DELIBERA ASSEMBLEARE	DATE
					NUMERO DELIBERAZIONE LEGISLATIVA	VARCHAR2
					DATA DELIBERAZIONE LEGISLATIVA	DATE
			Protocolli di intesa		LUOGO DI FIRMA DEL PROTOCOLLO / ACCORDO	VARCHAR2
					DATA DI FIRMA DEL PROTOCOLLO/ACCORDO	DATE
					FIRMATARI PER CONTO DELLA REGIONE	VARCHAR2
					LUOGO DI CONSERVAZIONE DELL'ORIGINALE	VARCHAR2

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Ente /Area	Codice Ente	Codice Area	Tipologia documentaria	Tipo atto	Metadati opzionali	Tipo
Atersir	r_emiro	AOO_ATER SIR				
			Atti monocratici AT	Atti dirigente	NUMERO DI ADOZIONE	VARCHAR2
					DATA DI ADOZIONE	DATE
					LUOGO DI ADOZIONE	VARCHAR2
					FIRMATARIO	VARCHAR2
					STRUTTURA ADOTTANTE	VARCHAR2
					ESTREMI DI PUBBLICAZIONE SUL BUR	VARCHAR2
					DATA PUBBLICAZIONE BU	DATE
					ESTREMI DI PUBBLICAZIONE SUL SUPPLEMENTO BUR	VARCHAR2
					DATA PUBBLICAZIONE SBU	DATE
					PROTOCOLLO REVOCA ATTO	VARCHAR2
			DATA REVOCA	DATE		
			Delibere del Consiglio d'Ambito			
			Delibere del Consiglio locale di Bologna			
			Delibere del Consiglio locale di Forlì-Cesena			
			Delibere del Consiglio locale di Ferrara			
			Delibere del Consiglio locale di Modena			
			Delibere del Consiglio locale di Piacenza			
			Delibere del Consiglio locale di Parma			
			Delibere del Consiglio locale di Ravenna			

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Ente /Area	Codice Ente	Codice Area	Tipologia documentaria	Tipo atto	Metadati opzionali	Tipo
			Delibere del Consiglio locale di Reggio Emilia			
			Delibere del Consiglio locale di Rimini			
			Documento unico regolarità contributiva			
			Repertorio emergenza per proposte atto			
			Fatture			
			Documento non protocollato			

7.6 Appendice 5: Metadati comuni di versamento Doc/er

La tabella seguente elenca i metadati comuni a tutte le Tipologie Documentarie

Metadati Generici		Significato	Valori Ammessi	web-methods Doc/ER delegati
TYPE_ID	obbligatori in creazione	Tipologia Documentaria	Stringa. Sono ammessi i soli identificativi delle tipologie documentarie configurate nel sistema	createDocument updateProfileDocument
COD_ENTE	obbligatori in creazione	Codice Ente	stringa	createDocument updateProfileDocument
COD_AOO	obbligatori in creazione	Codice Area Organizzativa Omogenea	stringa	createDocument updateProfileDocument
DOCNAME	obbligatori in creazione	Nome documento con estensione del file	stringa	createDocument updateProfileDocument
ABSTRACT	opzionale	Descrizione del documento	stringa	createDocument updateProfileDocument
CREATION_DATE	opzionale	Data di creazione del documento (se non specificato e' gestito internamente)	datetime	createDocument updateProfileDocument
TIPO_COMPONENTE	opzionale (raccomandato)	Raccomandato (se non specificato e' gestito internamente)	Vuoto PRINCIPALE ALLEGATO ANNESSO ANNOTAZIONE	createDocument updateProfileDocument

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Metadati Generici		Significato	Valori Ammessi	web-methods Doc/ER delegati
ARCHIVE_TYPE	opzionale	<p>Natura del documento riversato:</p> <ul style="list-style-type: none"> ▪ Archive=Documento Digitale; ▪ Paper=Documento copia elettronica dell'originale cartaceo quale ad esempio una scansione di un documento cartaceo; ▪ Uri=Documento di tipo link ad una Url Esterna) <p>Un documento con ARCHIVE_TYPE vuoto viene considerato di default un documento di tipo ARCHIVE</p>	vuoto ARCHIVE URL PAPER	createDocument updateProfileDocument
DOC_URL	opzionale	Indica la URL a cui punta il documento. Deve essere valorizzato quando ARCHIVE_TYPE=URL	stringa di tipo URI	createDocument updateProfileDocument
APP_VERSANTE	opzionale	Identificativo dell'applicazione versante	stringa	createDocument updateProfileDocument
DOC_HASH	opzionale	Hash del documento	stringa	createDocument updateProfileDocument
STATO_BUSINESS	opzionale	Stato del workflow sul documento (metadato gestito esternamente da eventuali workflow di processo)	0 (non definito) 1 (da protocollare) 2 (da fascicolare) 3 (da registrare) 4 (da_firmare)	createDocument updateProfileDocument

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Metadati Generici		Significato	Valori Ammessi	web-methods Doc/ER delegati
STATO_ARCHIVISTICO	sono opzionalmente specificabili i valori:0 (generico) 1 (generico definitivo)gli altri stati sono assegnati automaticamente dal sistema	Indica lo stato archivistico del documento in base al ciclo di vita del documento	-1 (non definito) 0 (generico) 1 (generico definitivo) 2 (registrato) 3 (protocollato) 4 (classificato) 5 (fascicolato) 6 (in_archivio_di_deposito)	createDocumentupdateProfileDocument
DOCNUM	READONLY	identificativo univoco del documento assegnato dal sistema	intero	
DOCNUM_PRINC	READONLY	e' il DOCNUM del documento che nell'unita' documentaria ha il ruolo di documento PRINCIPALE	intero	
DOCNUM_RECORD	READONLY	e' il DOCNUM del documento principale del RECORD che nella catena delle Versioni Avanzate rappresenta la sua formalizzazione attraverso il workflow di firma e registrazione.	intero	
VISTO	opzionale	Indica lo stato dei visti da apporre al documento da parte dei diversi utenti che devono vistare il documento. È normalmente utilizzato dai workflow esterni	stringa in formato XML con specifico XSD	createDocumentupdateProfileDocument
AUTHOR_ID	opzionale	Indica la user id dell'autore che ha creato il documento. Se non specificato e' gestito internamente	user id dell'utente creatore del documento	
TYPIST_ID	opzionale	Indica la user id dell'autore dell'ultima versione del documento. Se non specificato e' gestito internamente	user id dell'utente autore dell'ultima modifica del documento	

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Metadati di Registrazione		Significato		web-methods Doc/ER delegati
ID_REGISTRO	obbligatori per la Registrazione	identificativo del registro particolare	stringa	registraDocumento (*)
N_REGISTRAZ	obbligatori per la Registrazione	numero di registrazione	intero	registraDocumento (*)
D_REGISTRAZ	obbligatori per la Registrazione	data di registrazione	datetime	registraDocumento (*)
TIPO_FIRMA	obbligatori per la Registrazione	tipo di firma	FD (firmato digitalmente) FE (firmato non digitalmente) F (da inoltrare alla firma) NF (non firmato)	createDocument updateProfileDocument registraDocumento(*) protocollaDocumento(**)
FIRMATARIO	si deve specificare solo se TIPO_FIRMA=F	Firmatari del documento (applicabile per i soli documenti da avviare alla firma o per i documenti firmati)	formato XML con specifico XSD	createDocument updateProfileDocument registraDocumento(*) protocollaDocumento(**)
ANNULL_REGISTRAZ	opzionale	registrazione annullata	ANNULLATO vuoto	registraDocumento (*)
D_ANNULL_REGISTRAZ	opzionale	data annullamento della registrazione	datetime	registraDocumento (*)
M_ANNULL_REGISTRAZ	opzionale	motivo annullamento della registrazione	stringa	registraDocumento (*)
A_REGISTRAZ	opzionale	anno di registrazione	intero	registraDocumento (*)
O_REGISTRAZ	opzionale	oggetto della registrazione	stringa	registraDocumento (*)
MITTENTI	opzionale	Mittenti del documento	stringa in formato XML con specifico XSD	createDocument updateProfileDocument registraDocumento(*) protocollaDocumento(**)

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Metadati di Registrazione		Significato		web-methods Doc/ER delegati
DESTINATARI	opzionale	Destinatari del documento	stringa in formato XML con specifico XSD	createDocument updateProfileDocument registraDocumento(*) protocollaDocumento(**)

Metadati di Protocollazione		Significato	Valori Ammessi	web-methods Doc/ER delegati
TIPO_PROTOLLAZIONE	obbligatori per la Protocollazione	Tipo Protocollazione	E (in entrata) I (interna) U (in uscita) ND (non definita)	protocollaDocumento(**)
NUM_PG	obbligatori per la Protocollazione	Numero di Protocollo	intero	protocollaDocumento(**)
REGISTRO_PG	obbligatori per la Protocollazione	Registro di Protocollo	stringa	protocollaDocumento(**)
DATA_PG	obbligatori per la Protocollazione	Data di Protocollo	datetime	protocollaDocumento(**)
TIPO_FIRMA	obbligatori per la Protocollazione		FD (firmato digitalmente) FE (firmato non digitalmente) F (da inoltrare alla firma) NF (non firmato)	createDocument updateProfileDocument registraDocumento(*) protocollaDocumento(**)
FIRMATARIO	obbligatorio solo se TIPO_FIRMA=F		stringa in formato XML con specifico XSD	createDocument updateProfileDocument registraDocumento(*) protocollaDocumento(**)

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Metadati di Protocollazione		Significato	Valori Ammessi	web-methods Doc/ER delegati
ANNO_PG	opzionale, viene ricavato da DATA_PG	Anno Protocollo	intero	protocollaDocumento(**)
OGGETTO_PG	opzionale	Oggetto Protocollo	stringa	protocollaDocumento(**)
ANNULLATO_PG	opzionale	protocollo annullato	ANNULLATO vuoto	protocollaDocumento(**)
D_ANNULL_PG	opzionale	data annullamento protocollo	datetime	protocollaDocumento(**)
M_ANNULL_PG	opzionale	motivo annullamento protocollo	stringa	protocollaDocumento(**)
MITTENTI	opzionale	Mittenti del documento	stringa in formato XML con specifico XSD	createDocument updateProfileDocument registraDocumento(*) protocollaDocumento(**)
DESTINATARI	opzionale	Destinatari del documento	stringa in formato XML con specifico XSD	createDocument updateProfileDocument registraDocumento(*) protocollaDocumento(**)
NUM_PG_MITTENTE	opzionale	numero protocollo mittente	stringa	createDocument updateProfileDocument protocollaDocumento(**)
DATA_PG_MITTENTE	opzionale	data protocollo mittente	datetime	createDocument updateProfileDocument protocollaDocumento(**)
COD_ENTE_MITTENTE	opzionale	codice ente mittente	stringa	createDocument updateProfileDocument protocollaDocumento(**)

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Metadati di Protocollazione		Significato	Valori Ammessi	web-methods Doc/ER delegati
COD_AOO_MITTENTE	opzionale	codice aoo mittente	stringa	createDocument updateProfileDocument protocollaDocumento(**)
CLASSIFICA_MITTENTE	opzionale	classifica mittente	stringa	createDocument updateProfileDocument protocollaDocumento(**)
FASCICOLO_MITTENTE	opzionale	fascicolo mittente	stringa	createDocument updateProfileDocument protocollaDocumento(**)

Metadati di Classificazione		Significato	Valori Ammessi	web-methods Doc/ER delegati
CLASSIFICA	obbligatorio per la Classificazione	classifica del documento	stringa	classificaDocumento fascicolaDocumento(**)
COD_ENTE	opzionale	codice ente	stringa	
COD_AOO	opzionale	codice AOO	stringa	

Metadati di Fascicolazione		Significato	Valori Ammessi	web-methods Doc/ER delegati
PROGR_FASCICOLO	opzionale	progressivo fascicolo	stringa	fascicolaDocumento(**)
ANNO_FASCICOLO	opzionale	anno fascicolo	intero	fascicolaDocumento(**)
CLASSIFICA	opzionale	classifica del fascicolo	stringa	classificaDocumento fascicolaDocumento(**)
FASC_SECONDARI	opzionale	fascicoli secondari	stringa	fascicolaDocumento(**)
COD_ENTE	opzionale	codice ente	stringa	
COD_AOO	opzionale	codice AOO	stringa	

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

Metadati di Pubblicazione		Significato	Valori Ammessi	web-methods Doc/ER delegati
REGISTRO_PUB	obbligatori per la Pubblicazione	identificativo del registro di pubblicazione	stringa	pubblicaDocumento(***)
NUMERO_PUB	obbligatori per la Pubblicazione	numero pubblicazione	intero	pubblicaDocumento(***)
DATA_INIZIO_PUB	obbligatori per la Pubblicazione	data inizio pubblicazione	datetime	pubblicaDocumento(***)
DATA_FINE_PUB	obbligatori per la Pubblicazione	data fine pubblicazione	datetime	pubblicaDocumento(***)
PUBBLICATO	obbligatori per la Pubblicazione	documento pubblicato	true false	pubblicaDocumento(***)
OGGETTO_PUB	opzionale	oggetto pubblicazione	stringa	pubblicaDocumento(***)
ANNO_PUB	opzionale	anno di pubblicazione	intero	pubblicaDocumento(***)

Metadati di Conservazione		Significato	Valori Ammessi	web-methods Doc/ER delegati
STATO_CONSERV	deve essere impostato a 1 se si vuole mandare il documento in conservazione, altrimenti si imposta a 0	<ul style="list-style-type: none"> ▪ Stato Conservazione: ▪ 0 --> da non conservare ▪ 1 --> da conservare ▪ 2 --> inviato in conservazione ▪ 3 --> conservato ▪ 4 --> in errore 	<ul style="list-style-type: none"> ▪ 0 ▪ 1 ▪ 2 ▪ 3 ▪ 4 	createDocument updateProfileDocument
FORZA_COLL	opzionale	forza collegamento	true false	createDocument updateProfileDocument
FORZA_ACCETTAZ	opzionale	forza accettazione	true false	createDocument updateProfileDocument
FORZA_CONSERV	opzionale	forza conservazione	true false	createDocument updateProfileDocument

Metadati di Conservazione		Significato	Valori Ammessi	web-methods Doc/ER delegati
FLAG_CONSERV	opzionale	flag conservazione. Per alcune tipologie documentarie per le quali non tutti i documenti vanno inviati in conservazione, indica quali di essi devono essere o meno inviati	vuoto S N	createDocument updateProfileDocument
T_CONSERV	opzionale	tipo di conservazione sostitutiva da applicare al documento	vuoto SOSTITUTIVA FISCALE	createDocument updateProfileDocument
D_CO_CER	opzionale	data controllo certificato	datetime	createDocument updateProfileDocument
USA_D_CO_CER	opzionale	usa data controllo certificato	vuoto SI NO	createDocument updateProfileDocument
T_D_CONTR_CER	opzionale	tipo data controllo certificato	stringa	createDocument updateProfileDocument

(*) funzionalità riservata esclusivamente al sistema verticale di registro. Le altre applicazioni non possono invocare tale metodo.

(**) funzionalità riservata esclusivamente al sistema di protocollo. Le altre applicazioni non possono invocare tale metodo.

(***) funzionalità riservata esclusivamente ai sistemi che effettuato la pubblicazione dei documenti. Le altre applicazioni non possono invocare tale metodo.

7.7 Appendice 6: Modulo di definizione delle tipologie documentarie gestite dal Sistema Verticale

TYPE_ID	Tipologia documentaria	Protocollo	Repertori	Tipo di Firme	Conservazione Sostitutiva (SI/NO)	Voce di titolare/Classifica	Fascicoli di appartenenza	Visibilità (Ente, AOO, UO, riservato)

Compilare la seguente tabella se servono ulteriori metadati rispetto a quelli comuni o a quelli aggiuntivi già gestiti da GDR

TYPE_ID	Tipologia documentaria	Nome del Metadato Specifico in Doc/er	Descrizione del Metadato Specifico	Tipo di metadato (stringa, intero, date, datetime, numeri decimali)	Controlli Formali sui metadati	Valori Ammessi	Visibile sul profilo (SI/NO)

Legenda: Solo i campi in bianco sono da compilare a cura del progettista.

I campi in rosso saranno restituiti dal Siir nello step 4.

7.8 Appendice 7: Tabella per il Censimento Anagrafiche custom

TYPE_ID Anagrafica	Nome Anagrafica	Nome del Metadato Doc/er	Nome Attributo	Nome del Metadato Doc/er che individua il	Nome Attributo che individua il campo DESCRIZIONE	Nomi e tipi (stringa, intero, date, datetime, numeri decimali)

Linee guida per la *governance* del sistema informatico regionale: Allegato 18

		che individua il campo CODICE	che individua il campo CODICE	campo DESCRIZIONE		dei restanti metadati che completano il profilo dell'anagrafica custom

Legenda: Solo i campi in bianco sono da compilare a cura del progettista.

I campi in rosso saranno restituiti dal Siir nello step 4.

7.9 Appendice 8: Tabella per il Censimento Gruppi di business da gestire

ID GRUPPO	Nome gruppo	Gruppo padre	Descrizione gruppo
Legenda: Solo i campi in bianco sono da compilare a cura del progettista.			

I campi in rosso saranno restituiti dal Siir nello step 4

7.10 Appendice 9: Interfacce per realizzazione provider di repertoriazione

v. All. 2,3,4