REGIONE EMILIA-ROMAGNA
Atti amministrativi
INTERCENTER

Atto del Dirigente DETERMINAZIONE

Num. 366 del 26/05/2023 BOLOGNA

Proposta:	DIC/2023/370 del 26/05/2023
Struttura proponente:	INTERCENT-ER - AGENZIA REGIONALE DI SVILUPPO DEI MERCATI TELEMATICI
Oggetto:	NUOVA RETTIFICA BANDO ED ULTERIORE PROROGA DEI TERMINI DELLA PROCEDURA APERTA PER L'ACQUISIZIONE DI SERVIZI DI IT SYSTEM MANAGEMENT E SICUREZZA INFORMATICA 2
Autorità emanante:	IL RESPONSABILE - AREA INNOVAZIONE TECNOLOGICA E TRASFORMAZIONE DIGITALE
Firmatario:	ALESSIA ORSI in qualità di Responsabile di area di lavoro dirigenziale
Responsabile del procedimento:	Gianluca Imperato

Firmato digitalmente

LA DIRIGENTE FIRMATARIA

Visti:

- la L.R. 24 maggio 2004 n. 11 "Sviluppo regionale della società dell'Informazione" e ss.mm.ii.;
- il Decreto del Presidente della Giunta Regionale n. 293/2004 di attivazione dell'Agenzia regionale per lo sviluppo dei mercati telematici – Intercent-ER;

Viste le seguenti deliberazioni della Giunta regionale:

- n. 2163/2004 "Approvazione di norme organizzative relative all'avvio dell'Agenzia regionale per lo sviluppo dei mercati telematici, ex L.R. n. 11/2004", come modificata dalle deliberazioni n. 1389/2009, n. 2191/2010 e n. 1353/2014";
- n. 426 del 21/03/2022 "Riorganizzazione dell'ente a seguito del nuovo modello di organizzazione e gestione del personale. Conferimento degli incarichi ai direttori generali e ai direttori di Agenzia";

Vista la determinazione n. 8732/2023 della Direzione generale Cura della Persona, Salute e Welfare con la quale è stato adottato il Masterplan relativo al biennio 2023-2024;

Viste, inoltre, le seguenti determinazioni del Direttore di Intercent-ER:

- n. 265/2016 recante "Modifiche al Regolamento di Organizzazione di Intercent-ER", approvata dalla Giunta regionale con deliberazione n. 1825/2016, e successivamente modificata con deliberazione n. 29/2018;
- n. 410/2017 recante "Recepimento degli artt. 5, 7, e 12 della delibera di giunta regionale n. 468/2017 e modifica del regolamento di organizzazione di Intercent-ER" e ss.mm.ii.;
- n. 154/2022 "Riorganizzazione dell'Agenzia Intercent-ER, conferimento incarichi dirigenziali e proroga delle posizioni organizzative";

Richiamati:

- il D.Lgs. n. 50/2016 "Codice dei Contratti pubblici" e ss.mm.ii;

- il Regolamento regionale n.6 del 2019 recante "Disciplina per la corresponsione degli incentivi per le funzioni tecniche previsti dall'articolo 113 del Decreto legislativo n.50 del 2016";

- la legge n. 190/2012 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità della pubblica amministrazione";

- il Decreto Legislativo n. 33/2013 avente ad oggetto "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni" e ss.mm.ii.;

- la deliberazione della Giunta regionale n. 380/2023 avente ad oggetto "Approvazione Piano Integrato delle Attività e dell'Organizzazione 2023-2025";

Premesso che:

- con determinazione n.200 del 21/03/2023 è stata indetta la procedura aperta per l'acquisizione di servizi di IT System Management e Sicurezza informatica 2, suddivisa in due lotti;

- l'entità complessiva dell'appalto a base d'asta, coincidente con l'importo massimo spendibile, è determinata in Euro 95.000.000,00 (IVA esclusa). I lotti sono così articolati:

    - Lotto 1: Acquisizione di servizi di IT System Management, per una base d'asta coincidente con l'importo massimo spendibile pari ad Euro 65.000.000,00(IVA esclusa);

    - Lotto 2: Acquisizione di servizi di Sicurezza informatica, per una base d'asta coincidente con l'importo massimo spendibile pari ad Euro 30.000.000,00(IVA esclusa);

- entrambe le Convenzioni che verranno stipulate a seguito della presente gara avranno durata di 36 mesi(trentasei) mesi, a decorrere dalla data di sottoscrizione, e potranno essere rinnovate fino ad ulteriori 24 (ventiquattro) mesi, dietro comunicazione scritta dell'Agenzia, fermo restando l'importo massimo spendibile per ciascun lotto, incrementabile di un quinto ai sensi dell'art. 106 comma 12 del D.Lgs. 50/2016;

- i singoli Ordinativi di Fornitura (contratti), effettuati dagli Enti aderenti alla Convenzione durante il periodo di vi-

genza della stessa, avranno una durata minima annuale per i servizi a canone, mentre per i fabbisogni professionali, la durata degli Ordinativi di fornitura potrà essere variabile. La data di scadenza degli Ordinativi di fornitura non potrà essere superiore alla data di scadenza, originaria o eventualmente rinnovata, della Convenzione stessa;

- con determinazione n.274 del 21/04/2023 è stato rettificato il punto II.2.7) del bando di gara e sono stati prorogati i termini previsti per la presentazione delle richieste di chiarimenti e delle offerte, rispettivamente al 05/05/2023 e al 30/05/2023;

Considerato che le numerose richieste di chiarimenti pervenuti alla Stazione appaltante dagli operatori economici hanno evidenziato, soprattutto, l'esigenza di precisare per il Lotto 2 il parametro/la misura necessaria a dimensionare l'offerta per il canone annuale dei servizi continuativi e segnalato sempre per il medesimo lotto, la non esatta corrispondenza tra i servizi richiesti in capitolato e le voci dello schema di offerta economica di cui all'allegato 5 della documentazione di gara;

Ritenuto pertanto necessario, al fine di consentire la corretta formulazione dell'offerta da parte degli operatori economici, correggere i refusi e rettificare la documentazione di gara, in particolare lo schema di offerta economica e l'importo a base d'asta del Lotto 2, come segue:

- **Progetto tecnico:**
  - rettificato il Cap.3 limitatamente all'aggiornamento ad € 40.000.000,00 (IVA esclusa) del valore a base d'asta del Lotto 2;
- **Disciplinare:**
  - nel par. 3 è stato aggiornato ad € 40.000.000,00 (IVA esclusa) il valore a base d'asta (coincidente con l'importo massimo spendibile) del Lotto 2;
  - nel par.7 pag. 19 è stato sostituito il riferimento al par.6 con il par.5;
  - nel par. 9 pag. 20 è stato chiarito il punto in cui il riferimento (in caso di aggiudicazione) è alla garanzia definitiva e non a quella provvisoria;
  - nel par.9 pag.21 è stato corretto il riferimento normativo allo schema tipo da utilizzare per la garanzia fideiussoria;

- nel par. 14.1 pag. 29 sono state aggiunte delle precisazioni relative al pagamento dell'imposta di bollo da parte RTI, Consorzi e Aggregazioni di rete;
- nel par.16, pagg.34,35 è stata modificata la tabella in modo corrispondente al Capitolato e allo Schema di offerta economica;

- **All.3 Capitolato tecnico:**
  - nel par.4.1.1, pag.11 è stata eliminata la frase che impediva sempre l'utilizzo da parte del fornitore della banda trasmissiva a disposizione dell'Amministrazione;
  - nel par.4.2.2 è stato eliminato qualsiasi riferimento alla modalità "as a service";
  - nel cap.5 sono state modificate le tabelle relative ai Lotti 1 e 2 in modo corrispondente al Disciplinare e allo Schema di offerta economica e aggiunte delle note;
  - nel par.5.1 è stata riscritta la definizione di presidio on site e da remoto (per renderla più chiara) e a pag.54 sono state introdotte le fasce di EPS per il servizio di Monitoraggio SOC (Lotto 2);
  - nel par.7.1, in calce, è stato eliminato qualsiasi riferimento al servizio di manutenzione hardware (non richiesto);
- **All.3a Profili professionali:**
  - nelle premesse è stata aggiunta un'eccezione per le certificazioni che per loro stessa natura non scadono e che quindi si ritengono ammissibili sebbene conseguite prima dei 3 anni;
  - in tutto il documento sono stati eliminati i riferimenti alle certificazioni Microsoft MCSA e MCSE oramai obsolete;
- **All.5 Schema di offerta economica:**
  - per entrambi i Lotti è stata aggiunta una colonna "*Note di Agenzia*" che precisa cosa rappresentano le quantità e il parametro/la misura di riferimento per determinare il canone annuo dei servizi continuativi;
  - nel Lotto 2:
    - il servizio di monitoraggio SOC è stato suddiviso in 4 fasce di EPS, sia per l'orario base che per l'orario continuato;
    - i "Sistemi Firewall IDS/IPS" orario base e continuato sono stati distinti dai "Sistemi Antivirus e di telemetria (xDR o EDR, NDR)" orario base e continuato, per cui le voci da due sono diventate quattro;
    - è stata aggiunta la voce: Servizio di User and entity behavior analytics (UEBA) - ORARIO BASE;
    - sono state aggiunte le seguenti voci, corrispondenti a servizi a canone già contenuti

e descritti in Capitolato: Servizio di Vulnerability Management (sistema di monitoraggio dell'amministrazione o del fornitore) ORARIO BASE; Servizio di Application Security Testing (sistema di test dell'amministrazione o del fornitore) ORARIO BASE;

- sono state ricalcolate le quantità stimate per ogni voce rapportandole al parametro indicato nella colonna "*Note di Agenzia*";
- è stato aggiornato ad € 40.000.000,00 (IVA esclusa) il valore a base d'asta;

- **All.6 Schema di Convenzione:**
  - Art. 4 "Oggetto", comma 2 è stato aggiornato ad € 40.000.000,00 (IVA esclusa) il valore del Lotto 2;
  - Art.14 "Adeguamento prezzi", sono stati modificati il comma 1 ed il comma 4, è stato eliminato il comma 5;
  - Art.15 comma 3, è stato sostituito "semestrale" con "trimestrale" conformemente a quanto stabilito in Capitolato;

Considerate, inoltre, la quantità di chiarimenti pervenuti e a cui l'Agenzia deve ancora dare risposta, l'ampiezza della rettifica relativa al Lotto 2, la complementarità dei due lotti e la particolare complessità e rilevanza dell'appalto;

Rilevato che è interesse dell'Agenzia garantire il buon esito della procedura di gara e la massima partecipazione alla stessa;

Ritenuto opportuno, pertanto, prorogare il termine di scadenza per la presentazione delle offerte, fissando di conseguenza una nuova data per la scadenza dei termini per la presentazione dei chiarimenti e per la seduta pubblica di apertura e verifica della documentazione amministrativa, come segue:

- il termine di scadenza dei chiarimenti è fissato alle ore 12:00 del 01/06/2023;

- il termine di ricezione delle offerte è fissato alle ore 16:00 del 04/07/2023;

- il giorno di apertura delle offerte (documentazione amministrativa) è fissato alle ore 10:00 del 05/07/2023;

Dato atto che la presente rettifica sarà pubblicata sulla Gazzetta Ufficiale dell'Unione Europea (G.U.U.E.), sulla Gazzetta Ufficiale della Repubblica Italiana (G.U.R.I.), sul Bollettino Ufficiale della Regione Emilia-Romagna e sul sito internet https://intercenter.regione.emilia-romagna.it e dello stesso sarà

data notizia sul sito informatico dell'Osservatorio Regionale dei Contratti pubblici e con avviso pubblicato su quattro quotidiani di cui due a carattere nazionale e due a particolare diffusione nella Regione, secondo quanto previsto dagli articoli 72 e 73 del precitato D. Lgs. 50/2016;

Confermato, sotto ogni altro profilo, il contenuto della restante documentazione di gara, già approvata con determinazione dirigenziale n.200 del 21/03/2023, rettificata con determinazione dirigenziale n.274 del 21/04/2023;

Dato atto che il Responsabile del procedimento ha dichiarato di non trovarsi in situazione di conflitto, anche potenziale, di interessi;

Attestato che il sottoscritto dirigente non si trova in situazione di conflitto, anche potenziale, di interessi;

Attestata la regolarità amministrativa del presente atto;

D E T E R M I N A

per le ragioni espresse in premessa e qui integralmente richiamate:

1) di rettificare come indicato nelle premesse e sostituire la seguente documentazione della procedura aperta, suddivisa in due lotti, per l'acquisizione di servizi di IT System Management e Sicurezza informatica 2:

   a) Progetto tecnico;
   b) Disciplinare;
   c) All.3 Capitolato tecnico;
   d) All.3a Profili professionali;
   e) All.5 Schema di Offerta economica;
   f) All.6 Schema di Convenzione.

2) di rettificare il valore a base d'asta (coincidente con l'importo massimo spendibile) del Lotto 2 da € 30.000.000,00 ad € 40.000.000,00, lasciando invariato il valore a base d'asta del Lotto 1 pari ad € 65.000.000,00;

3) di prorogare i termini del bando di gara come segue:

   • il termine di scadenza dei chiarimenti è fissato alle ore 12:00 del 01/06/2023;

   • il termine di ricezione delle offerte è fissato alle ore 16:00 del 04/07/2023;

- il giorno di apertura delle offerte (documentazione amministrativa) è fissato alle ore 10:00 del 05/07/2023;

4) di confermare, sotto ogni altro profilo, il contenuto della restante documentazione di gara, già approvata con determinazione dirigenziale n.200 del 21/03/2023, rettificata con determinazione dirigenziale n.274 del 21/04/2023;

5) di precisare che la presente ulteriore rettifica sarà pubblicata sulla Gazzetta Ufficiale dell'Unione Europea (G.U.U.E.), sulla Gazzetta Ufficiale della Repubblica Italia (G.U.R.I.), sul Bollettino Ufficiale della Regione Emilia-Romagna (BUR) e sul sito internet http://intercenter.regione.emilia-romagna.it e che dello stesso sarà data notizia sul sito informatico dell'Osservatorio Regionale dei Contratti pubblici e con avviso pubblicato su quattro quotidiani di cui due a carattere nazionale e due a particolare diffusione nella Regione, secondo quanto previsto dagli articoli 72 e 73 del D. Lgs. 50/2016;

6) di dare atto che le spese necessarie per la pubblicazione della rettifica e proroga dei termini al bando di gara e del suo estratto saranno sostenute con fondi provenienti dal Bilancio Regionale;

7) di dare atto che la rettifica e proroga dei termini del bando di gara sarà consultabile sul sito Web: https://intercenter.regione.emilia-romagna.it;

8) di confermare, quale Responsabile del procedimento per la presente procedura, ai sensi e per gli effetti dell'art. 31 del D.Lgs n. 50/2016, Gianluca Imperato;

9) di provvedere alle ulteriori pubblicazioni previste dal PIAO 2023-2025 ai sensi dell'art. 7 bis, comma 3, del D.lgs. n. 33 del 2013.

La Responsabile di Area
(Dr.ssa Alessia Orsi)

AGENZIA INTERCENT-ER
REGIONE EMILIA-ROMAGNA
RETTIFICA BANDO DI GARA

Sezione I: Amministrazione aggiudicatrice

Intercent-ER – Agenzia regionale per lo sviluppo dei mercati telematici 0000246017 Via dei Mille 21 Bologna 40121 Tel. 051.5273081 - Fax 051.5273084; Codice NUTS: ITH5; e-mail: intercenter@regione.emilia-romagna.it PEC: intercenter@postacert.regione.emilia-romagna.it
Persona di contatto: Gianluca Imperato - tel.051.5273430 - mail: gianluca.imperato@regione.emilia-romagna.it
Indirizzo internet e profilo committente: https://intercenter.regione.emilia-romagna.it

Sezione II: Oggetto

II.1.1) Denominazione: Procedura aperta per l'acquisizione di servizi di IT System Management e Sicurezza informatica 2
II.1.2) Codice CPV principale: 72250000-2
II.1.3) Tipo di appalto: Servizi
II.1.4) Breve descrizione: Acquisizione di servizi di assistenza sistemistica - IT System Management e di servizi relativi alla sicurezza informatica

Sezione IV Procedura

IV.2.2) Proroga termine ricezione offerte a rettifica del bando di gara relativo alla procedura di cui al punto II.1.1 pubblicato nella GURI 5^ Serie Speciale n. 35 del 24/03/2023 e rettificato nella GURI 5^ Serie Speciale n. 47 del 24/04/2023

Sezione VII: Modifiche

VII.1) Informazioni da correggere o aggiungere
VII.1.2) Testo da correggere nell'avviso originale. Numero della sezione: II.1.5) Valore totale stimato: anziché 95.000.000,00 IVA esclusa leggi: € 105.000.000,00 IVA esclusa; Numero della sezione: II.2.1) Descrizione Lotti: Lotto2: Servizi di Sicurezza Informatica per un importo anziché: di Euro 30.000.000,00 IVA esclusa leggi: Euro 40.000.000,00 IVA esclusa; Numero della sezione: IV.2.2 Termine per il ricevimento delle offerte o delle domande di partecipazione, anziché: Data: 30/05/2023 Ora locale: 16:00 leggi: Data: 04/07/2023 Ora locale 16:00; Numero della sezione: IV.2.7: Modalità di apertura delle offerte, anziché: Seduta Pubblica Virtuale, Data: 31/05/2023 Ora locale: 10:00 leggi: Seduta Pubblica Virtuale, Data: 05/07/2023 Ora locale: 10:00.
VII.2) Altre informazioni complementari: Sono modificati e, pertanto, sostituiti sul sito http://intercenter.regione.emilia-romagna.it. i seguenti documenti di gara: Progetto tecnico; Disciplinare; All.3 Capitolato tecnico; All.3a Profili professionali; All.5 Schema di Offerta economica; All.6 Schema di Convenzione. Le richieste di chiarimenti dovranno pervenire esclusivamente tramite SATER entro le ore 12:00 del 01/06/2023.
Determina dirigenziale n. …. del …/05/2023.
Data di invio alla GUUE: …/05/2023.

Il Direttore dell'Agenzia Intercent ER
Dott. Adriano Leli

AGENZIA INTERCENT-ER

REGIONE EMILIA ROMAGNA

ESTRATTO RETTIFICA BANDO DI GARA

Ente Appaltante: Intercent-ER - Via Dei Mille n. 21, 40121 Bologna - Tel. 051 5273081 - E-mail: intercenter@regione.emilia-romagna.it Pec: intercenter@postacert.regione.emilia-romagna.it - Sito: https://intercenter.regione.emilia-romagna.it **Oggetto della gara:** Procedura aperta per l'acquisizione di servizi di IT System Management e Sicurezza informatica 2. **Importo complessivo posto a gara:** Euro 105.000.000,00 IVA esclusa così suddiviso: Lotto1: Euro 65.000.000,00 IVA esclusa; Lotto2: Euro 40.000.000,00 IVA esclusa; **Termine e luogo presentazione offerte**: le offerte devono essere collocate per via telematica entro le ore 16:00 del 04/07/2023. **Bando integrale e documentazione di gara**: https://intercenter.regione.emilia-romagna.it - sezione "Bandi e Avvisi" **Data di invio del bando alla GUUE**: …/…/….

IL DIRETTORE
(Dott. Adriano Leli)

PROCEDURA APERTA PER L'ACQUISIZIONE DI SERVIZI DI IT SYTEM MANAGEMENT E SICUREZZA INFORMATICA 2

PROGETTO – RELAZIONE TECNICA

(RETTIFICATO)

1. OGGETTO

La procedura di gara si compone di due lotti:

- **il Lotto 1** “SERVIZI DI IT SYSTEM MANAGEMENT” riguarda i servizi di gestione, manutenzione, sviluppo delle architetture informatiche e supporto specialistico per le infrastrutture hardware e software di base utilizzati dalle Amministrazioni della Regione Emilia-Romagna a supporto delle proprie attività informatizzate (IT System Management);
- **il Lotto 2** “SERVIZI DI SICUREZZA INFORMATICA” riguarda i servizi necessari e funzionali a garantire adeguati livelli di sicurezza dei sistemi IT nel loro complesso, dei dati trattati e in generale delle informazioni (Sicurezza Informatica).

L’ambito tecnologico nel quale dovranno essere erogati i servizi previsti comprende le principali tecnologie presenti nel mercato dell’ICT e della Sicurezza Informatica, ampiamente utilizzate dalle Pubbliche Amministrazioni.

2. ANALISI DELLA DOMANDA

L’analisi della domanda per tali servizi è stata condotta attraverso una rilevazione dei fabbisogni effettuata con l’invio di un questionario agli Enti della Regione Emilia-Romagna, analizzando con gli esperti del Gruppo di lavoro, costituito per predisporre il capitolato tecnico, le risposte ricevute, in particolare, dalle Aziende sanitarie, da Lepida S.C.p.A e dalle Amministrazioni più rilevanti come la Regione Emilia-Romagna e il Comune di Bologna.

Inoltre, per i servizi di IT System Management sono stati analizzati anche gli Ordinativi effettuati dalle amministrazioni aderenti alla Convenzione precedente stipulata dall’Agenzia e scaduta il 31/12/2022.

Si è tenuto conto anche del rapporto tra il numero di risposte ricevute ed il totale degli Enti potenzialmente aderenti; la spesa storica dei consumi effettivi rilevati dal cruscotto di monitoraggio dell’Agenzia e, in particolare, per i servizi di sicurezza informatica della crescente necessità di tali servizi, soprattutto in funzione preventiva, visto le varie minacce informatiche e, in particolare, il rischio di attacchi hacker, anche collegati alla situazione internazionale, dalle onerose conseguenze per le Amministrazioni pubbliche.

3. ANALISI DELL’OFFERTA E CALCOLO DELLA BASE D’ASTA

Il valore complessivo di ciascuna Convenzione è stato stimato facendo riferimento:

- per i prezzi unitari del Lotto 1 a quelli risultanti dalle offerte ricevute nella precedente gara, a quelli per analoghe figure professionali presenti in gare svolte di recente dall’Agenzia e alle quotazioni sul mercato business con il riscontro fornito dagli esperti del Gruppo di lavoro;

- per i prezzi unitari del Lotto 2 a quelli delle ultime Convenzioni Consip, a quelli per analoghe figure professionali presenti in gare svolte di recente dall'Agenzia e alle quotazioni sul mercato business con il riscontro fornito dagli esperti del Gruppo di lavoro.

Conformemente a quanto previsto dal comma 16 dell'art. 23 del d.lgs. 50/2016, come modificato dal d.lgs. 56/2017, che dispone che «nei contratti di lavori e servizi la stazione appaltante, al fine di determinare l'importo a base di gara, individua nei documenti posti a base di gara i costi della manodopera […]», non si è proceduto alla stima di tali costi in quanto trattasi di servizi di natura intellettuale e per lo stesso motivo, ai sensi dell'art. 95, comma 10, del sopracitato decreto legislativo, anche l'operatore economico non dovrà indicare i propri costi della manodopera né gli oneri aziendali per la sicurezza, pur dovendone tenere conto nella formulazione della propria offerta economica.

Pertanto, l'importo a base di gara, corrispondente all'importo massimo spendibile, per il **Lotto 1** è pari ad **€ 65.000.000,00** e per il **Lotto 2** è pari ad **€ 40.000.000,00** al netto di Iva e/o di altre imposte e contributi di legge, nonché degli oneri per la sicurezza dovuti a rischi da interferenze calcolati pari a 0,00.

4. DURATA DELLA CONVENZIONE

La durata della Convenzione è di 36 mesi, decorrenti dalla data di sottoscrizione della stessa.

Gli Ordinativi di fornitura emessi dalle singole Aziende sanitarie/Amministrazioni contraenti avranno durata minima annuale per i servizi a canone a far data dalla loro emissione; mentre per i servizi relativi alla richiesta di fabbisogni professionali la durata degli Ordinativi di Fornitura potrà essere variabile in relazione alla quantità di giornate richieste per le figure professionali previste.

La data di scadenza degli ordinativi di fornitura non potrà essere superiore alla data di scadenza, originaria o eventualmente rinnovata della Convenzione stessa.

5.OPZIONI E RINNOVI

La Convenzione potrà essere rinnovata fino ad ulteriori **24** mesi, su comunicazione scritta dell'Agenzia, nell'ipotesi in cui alla scadenza del termine, **non** sia stato esaurito l'importo massimo spendibile del singolo Lotto.

6.CRITERI DI AGGIUDICAZIONE

L'aggiudicazione verrà effettuata, in entrambi i Lotti, con il criterio della offerta economicamente più vantaggiosa ai sensi dell'art.95, c.2 del Codice dei contratti pubblici con la seguente ripartizione: **80 punti per l'offerta tecnica e 20 punti per l'offerta economica.**
I criteri di valutazione sono esplicitati nel Disciplinare di gara.

Quanto all’offerta economica, è attribuito all’elemento economico un coefficiente, variabile da zero ad uno, calcolato tramite la seguente formula:

Formula del “ribasso massimo non lineare”

Ci = (Ra/Rmax)α , dove:

Ci = coefficiente attribuito al concorrente i-esimo;

Ra = ribasso dell’offerta del concorrente i-esimo;

Rmax = ribasso dell’offerta più conveniente.

α = 0,50

7.1 Metodo per il calcolo dei punteggi

La commissione giudicatrice, terminata l’attribuzione dei coefficienti agli elementi qualitativi e quantitativi, procederà, in relazione a ciascuna offerta, all’attribuzione dei punteggi per ogni singolo criterio secondo il metodo aggregativo compensatore.

Il punteggio è dato dalla seguente formula:

Pi = Cai x Pa + Cbi x Pb+….. Cni x Pn

dove

Pi = punteggio concorrente i;

Cai = coefficiente criterio di valutazione a, del concorrente i;

Cbi = coefficiente criterio di valutazione b, del concorrente i;

.....

Cni = coefficiente criterio di valutazione n, del concorrente i;

Pa = peso criterio di valutazione a;

Pb = peso criterio di valutazione b;

.....

Pn = peso criterio di valutazione n.

PROCEDURA APERTA PER L'ACQUISIZIONE DI SERVIZI DI IT SYSTEM MANAGEMENT E SICUREZZA INFORMATICA 2

DISCIPLINARE DI GARA

(RETTIFICATO)

INDICE

PREMESSE

Con determina di indizione n. ..... del …… l'Agenzia Intercent-ER (in seguito: Agenzia) ha deliberato di acquisire servizi di IT System Management e Sicurezza informatica mediante la stipula di una Convenzione/ai sensi dell'articolo 21 della Legge Regionale dell'Emilia-Romagna 24 maggio 2004, n. 11.

L'affidamento avverrà mediante procedura aperta, suddivisa in due lotti e con applicazione del criterio dell'offerta economicamente più vantaggiosa individuata sulla base del miglior rapporto qualità prezzo ai sensi degli artt. 44,52,58,60 e 95 del d.lgs. 18 aprile 2016, n. 50 – Codice dei contratti pubblici (in seguito: Codice).

La presente procedura è interamente svolta tramite il sistema informatico per le procedure telematiche di acquisto della Regione Emilia-Romagna (di seguito SATER) accessibile dal sito all'indirizzo www.http://intercenter.regione.emilia-romagna.it/ (in seguito Sito) e conforme alla normativa vigente.

Il luogo di svolgimento del servizio è la Regione Emilia-Romagna [codice NUTS ITH5]

NUMERO DI GARA: 9005713

LOTTO 1 CIG: 97219284C8

LOTTO 2 CIG: 972192959B

Il **Responsabile del procedimento**, ai sensi dell'articolo 31 del Codice, è **Gianluca Imperato**.

Con l'aggiudicatario (di seguito: Fornitore) verrà stipulata una Convenzione con la quale il Fornitore medesimo si obbliga ad accettare gli Ordinativi di fornitura (i.e. contratti), emessi dalle Amministrazioni contraenti, per l'erogazione dei servizi oggetto della presente gara.

Nel periodo di validità della Convenzione, le singole Amministrazioni contraenti, previa registrazione sul sito http://intercenter.regione.emilia-romagna.it/, potranno emettere Ordinativi di fornitura sottoscritti da persona autorizzata (Punto ordinante) ad impegnare la spesa delle Amministrazioni contraenti stesse fino a concorrenza dell'importo massimo spendibile pari al valore complessivo a base d'asta per ciascun lotto.

Gli Ordinativi di fornitura possono essere effettuati solo da Punti ordinanti registrati al Sistema informatico messo a disposizione dall'Agenzia e devono essere inviati e/o trasmessi dalle Amministrazioni contraenti, mediante documenti informatici sottoscritti con firma digitale, attraverso il Sistema, secondo le modalità specificate nello Schema di Convenzione.

La registrazione delle Amministrazioni contraenti non implica una verifica da parte dell'Agenzia dei poteri d'acquisto di ciascun Punto ordinante; l'Agenzia non risponde quindi di Ordinativi di fornitura sottoscritti da Punti ordinanti non autorizzati dalle Amministrazioni contraenti di appartenenza.

Le Aziende sanitarie, la Regione Emilia-Romagna e gli Enti ad essa afferenti, di cui alla L. n. 11/2004 e s.m., sottoposti all'applicazione degli obblighi di cui all'articolo 1, commi da 209 a 214, della Legge

24 dicembre 2007, n. 244 (l'elenco di tali Enti è disponibile sul sito http://intercenter.regione.emilia-romagna.it/), emettono gli ordini/richieste di consegna esclusivamente in forma elettronica.

Il Fornitore dovrà garantire l'invio dei documenti di trasporto elettronici, a fronte degli ordini ricevuti e delle consegne effettuate.

Il Fornitore dovrà pertanto dotarsi degli strumenti informatici idonei alla gestione degli adempimenti telematici. Per i dettagli tecnici si rimanda alla sezione dedicata presente sul sito http://intercenter.regione.emilia-romagna.it/, che contiene tutti i riferimenti del Sistema regionale per la dematerializzazione del ciclo passivo degli acquisti nonché del Nodo Telematico di Interscambio (No-TIER).

In alternativa, il Fornitore potrà utilizzare le funzionalità per la ricezione degli ordini e l'invio dei documenti di trasporto elettronici che saranno messe a disposizione sul SATER all'indirizzo https://piattaformaintercenter.regione.emilia-romagna.it/portale/, previa registrazione.

1. PIATTAFORMA TELEMATICA

1.1 LA PIATTAFORMA TELEMATICA DI NEGOZIAZIONE (SATER)

Il funzionamento della piattaforma SATER - Sistema per gli Acquisti Telematici dell'Emilia-Romagna - avviene nel rispetto della legislazione vigente.

L'utilizzo di SATER comporta l'accettazione tacita ed incondizionata di tutti i termini, le condizioni di utilizzo e le avvertenze contenute nei documenti di gara e nel regolamento di utilizzo del sistema, nonché di quanto portato a conoscenza degli utenti tramite le comunicazioni sul SATER.

L'utilizzo di SATER avviene nel rispetto dei principi di autoresponsabilità e di diligenza professionale, secondo quanto previsto dall'articolo 1176, comma 2, del Codice civile ed è regolato, tra gli altri, dai seguenti principi:

- parità di trattamento tra gli operatori economici;
- trasparenza e tracciabilità delle operazioni;
- standardizzazione dei documenti;
- comportamento secondo buona fede, ai sensi dell'articolo 1375 del Codice civile;
- comportamento secondo correttezza, ai sensi dell'articolo 1175 del Codice civile;
- segretezza delle offerte e loro immodificabilità una volta scaduto il termine di presentazione della domanda di partecipazione;
- gratuità. Nessun corrispettivo è dovuto dall'operatore economico e/o dall'aggiudicatario per il mero utilizzo di SATER.

L'Agenzia Intercent-ER non assume alcuna responsabilità per perdita di documenti e dati, danneggiamento di file e documenti, ritardi nell'inserimento di dati, documenti e/o nella

presentazione della domanda, malfunzionamento, danni, pregiudizi derivanti all'operatore economico, da:

- difetti di funzionamento delle apparecchiature e dei sistemi di collegamento e programmi impiegati dal singolo operatore economico per il collegamento a SATER;
- utilizzo della piattaforma SATER da parte dell'operatore economico in maniera non conforme al Disciplinare e a quanto previsto nel Regolamento di utilizzo del sistema.

In caso di mancato funzionamento di SATER o di malfunzionamento della stessa, non dovuti alle predette circostanze, che impediscono la corretta presentazione delle offerte, al fine di assicurare la massima partecipazione, l'Agenzia può disporre la sospensione del termine di presentazione delle offerte per un periodo di tempo necessario a ripristinare il normale funzionamento di SATER e la proroga dello stesso per una durata proporzionale alla durata del mancato o non corretto funzionamento, tenuto conto della gravità dello stesso, dandone tempestiva comunicazione sulla pagina del sito https://intercenter.regione.emilia-romagna.it/ dove sono accessibili i documenti di gara nonché attraverso ogni altro strumento ritenuto idoneo.

L'Agenzia Intercent-ER si riserva di agire in tal modo anche quando, esclusa la negligenza dell'operatore economico, non sia possibile accertare la causa del mancato funzionamento o del malfunzionamento.

Il SATER garantisce l'integrità dei dati, la riservatezza delle offerte e delle domande di partecipazione.

La piattaforma SATER è realizzata con modalità e soluzioni tecniche che impediscono di operare variazioni sui documenti definitivi, sulle registrazioni di sistema e sulle altre rappresentazioni informatiche e telematiche degli atti e delle operazioni compiute nell'ambito delle procedure, sulla base della tecnologia esistente e disponibile.

Le attività e le operazioni effettuate nell'ambito di SATER sono registrate e attribuite all'operatore economico e si intendono compiute nell'ora e nel giorno risultanti dalle registrazioni di sistema.

Il sistema operativo di SATER è sincronizzato sulla scala di tempo nazionale di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591, tramite protocollo NTP o standard superiore.

L'utilizzo e il funzionamento di SATER avvengono in conformità a quanto riportato nel Regolamento di utilizzo del sistema, disponibile all'indirizzo https://intercenter.regione.emilia-romagna.it/sistema-acquisti-sater/regolamenti che costituisce parte integrante del presente disciplinare.

L'acquisto, l'installazione e la configurazione dell'hardware, del software, dei certificati digitali di firma, della casella di PEC o comunque di un indirizzo di servizio elettronico di recapito certificato qualificato, nonché dei collegamenti per l'accesso alla rete Internet, restano a esclusivo carico dell'operatore economico.

SATER è sempre accessibile all'indirizzo https://piattaformaintercenter.regione.emilia-romagna.it/portale_ic/ e raggiungibile anche tramite il portale dell'Agenzia Intercent-ER https://intercenter.regione.emilia-romagna.it/.

1.2 DOTAZIONI TECNICHE

Ai fini della partecipazione alla presente procedura, ogni operatore economico deve dotarsi, a propria cura, spesa e responsabilità della strumentazione tecnica ed informatica conforme a quella indicata nel presente disciplinare e nel Regolamento di utilizzo del sistema.

In ogni caso è indispensabile:

a) disporre almeno di un personal computer conforme agli standard aggiornati di mercato, con connessione internet e dotato di un comune browser idoneo ad operare in modo corretto su SATER;
b) disporre di un indirizzo di posta elettronica certificata ai sensi dell'articolo 48 del Codice dell'Amministrazione Digitale, ovvero, in caso di operatori economici aventi sede in altri Stati, possedere un indirizzo di posta elettronica ordinaria;
c) avere da parte del legale rappresentante dell'operatore economico (o da persona munita di idonei poteri di firma) un certificato di firma digitale, in corso di validità, rilasciato da un organismo incluso nell'elenco pubblico dei certificatori tenuto dall'Agenzia per l'Italia Digitale (previsto dall'articolo 29 del decreto legislativo n. 82/05).

1.3 REGISTRAZIONE DELLE DITTE E IDENTIFICAZIONE

Ai fini della partecipazione alla presente procedura è indispensabile essere registrati a SATER, secondo le modalità esplicitate nelle guide per l'utilizzo della piattaforma accessibili dal sito http://intercenter.regione.emilia-romagna.it/help/guide.

La registrazione a SATER deve essere richiesta unicamente dal legale rappresentante e/o procuratore generale o speciale e/o dal soggetto dotato dei necessari poteri per richiedere la registrazione e impegnare l'operatore economico medesimo.

L'operatore economico, con la registrazione e, comunque, con la presentazione dell'offerta, dà per valido e riconosce, senza contestazione alcuna, quanto posto in essere all'interno di SATER dall'account riconducibile all'operatore economico medesimo; ogni azione inerente all'account all'interno di SATER si intenderà, pertanto, direttamente e incontrovertibilmente imputabile all'operatore economico registrato. Per poter presentare offerta è necessario accedere a SATER.

L'accesso è gratuito ed è consentito a seguito dell'identificazione online dell'operatore economico; l'identificazione può avvenire mediante le credenziali rilasciate al momento della registrazione ovvero tramite il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID) o tramite carta di identità elettronica.

Eventuali richieste di assistenza di tipo informatico riguardanti l'identificazione e l'accesso a SATER possono essere effettuate tramite Call Center che risponde ai numeri 800 810 799 (rete fissa) e 089 9712796 (rete mobile e dall'estero), lun-ven, ore 9-13 e 14-18.

2. DOCUMENTAZIONE DI GARA, CHIARIMENTI E COMUNICAZIONI

2.1 DOCUMENTI DI GARA

La documentazione di gara comprende:

1) Progetto ai sensi dell'articolo 23, commi 14 e 15, del Codice;
2) Bando di gara;
3) Disciplinare di gara;
4) Allegato 1 - DGUE (Deve essere compilato su SATER dall'operatore economico e dall'eventuale ausiliaria. In caso di RTI dovranno compilarlo sia la mandataria che le mandanti);
5) Allegato 1a - Domanda di partecipazione;
6) Allegato 1b - Patto di integrità, approvato dalla Regione Emilia-Romagna con delibera della giunta del 13 aprile 2022 n. 565;
7) Allegato 2a - Schema dichiarazioni concordato preventivo;
8) Allegato 2b - Schema dichiarazione avvalimento;
9) Allegato 3 - Capitolato tecnico;
10) Allegato 3.A - Figure professionali;
11) Allegato 4a - Schema di offerta tecnica Lotto 1;
12) Allegato 4b - Schema di offerta tecnica Lotto 2;
13) Allegato 5 - Schema di offerta economica Lotti 1 e 2;
14) Allegato 6 - Schema di Convenzione Lotti 1 e 2;
15) Allegato 7 - Modulo per attestazione pagamento imposta di bollo.

La presente procedura di gara ha ad oggetto servizi di natura intellettuale, pertanto, ai sensi dell'articolo 26, comma 3-bis, del d.lgs. n. 81/2008 e s.m.i., non è stato redatto il Documento Unico di Valutazione dei Rischi da Interferenza (DUVRI), in quanto non sussiste l'obbligo di cui all'articolo 26, comma 3, del decreto sopra citato. Resta inteso che, qualora l'Amministrazione contraente ritenga che, con specifico riferimento ai luoghi in cui si svolge la singola prestazione, possano sussistere rischi da interferenza, procederà alla redazione del documento che, sottoscritto per accettazione dal Fornitore, integrerà l'Ordinativo di fornitura.

È comunque onere di ciascun Fornitore elaborare, relativamente ai costi della sicurezza afferenti all'esercizio della propria attività, il documento di valutazione dei rischi e di provvedere all'attuazione

delle misure di sicurezza necessarie per eliminare o ridurre al minimo i rischi specifici connessi all'attività svolta dallo stesso.

La documentazione di gara è disponibile sul sito internet: http://intercenter.regione.emilia-romagna.it/ e sul SATER.

2.2 CHIARIMENTI

É possibile ottenere chiarimenti sulla presente procedura mediante la proposizione di quesiti inviati tramite SATER secondo le modalità esplicitate nelle guide per l'utilizzo della piattaforma accessibili dal sito http://intercenter.regione.emilia-romagna.it/help/guide da inoltrare entro le ore **12:00** del **01/06/2023** in via telematica, attraverso la sezione riservata alla richiesta di chiarimenti, previa registrazione alla Piattaforma.

Non verranno evase richieste di chiarimento pervenute in modalità diversa da quella esplicitata.

Le richieste di chiarimenti e le relative risposte sono formulate esclusivamente in lingua italiana.

Le risposte a tutte le richieste presentate in tempo utile verranno fornite almeno sei giorni prima della scadenza del termine fissato per la presentazione delle offerte, tramite SATER e con la pubblicazione in forma anonima all'indirizzo internet http://intercenter.regione.emilia-romagna.it/, nella sezione "Bandi aperti" dedicata alla presente procedura. Si invitano i concorrenti a visionare costantemente tale sezione di SATER o il sito istituzionale.

2.3 COMUNICAZIONI

Tutte le comunicazioni e gli scambi di informazioni di cui alla presente procedura sono eseguiti utilizzando mezzi di comunicazione elettronici.

Le comunicazioni tra stazione appaltante e operatori economici avvengono tramite la Piattaforma e sono accessibili nella sezione Comunicazioni (Ricevute e Inviate). È onere esclusivo dell'operatore economico prenderne visione. La Piattaforma invia automaticamente agli operatori economici una segnalazione di avviso.

Le comunicazioni relative: a) all'aggiudicazione; b) all'esclusione; c) alla decisione di non aggiudicare l' appalto; d) alla data di avvenuta stipulazione del contratto con l'aggiudicatario; e) all'attivazione del soccorso istruttorio; f) al subprocedimento di verifica dell'anomalia dell'offerta anomala; g) alla richiesta di offerta migliorativa; h) al sorteggio di cui all'articolo 21; avvengono utilizzando il domicilio digitale presente negli indici di cui agli articoli 6-bis e 6-ter del decreto legislativo n. 82/05 o, per gli operatori economici transfrontalieri, attraverso un indirizzo di servizio elettronico di recapito certificato qualificato ai sensi del Regolamento eIDAS. Se l'operatore economico non è presente nei predetti indici elegge domicilio digitale speciale presso la stessa Piattaforma e le comunicazioni di cui sopra sono effettuate utilizzando tale domicilio digitale. Salvo quanto disposto nel paragrafo "2.2 Chiarimenti" del presente Disciplinare, tutte le comunicazioni tra l'Agenzia e gli operatori economici

si intendono validamente ed efficacemente effettuate qualora rese mediante SATER all'indirizzo PEC del concorrente indicato in fase di registrazione.

Salvo quanto disposto nel paragrafo "2.2 Chiarimenti" del presente Disciplinare, tutte le comunicazioni tra l'Agenzia e gli operatori economici si intendono validamente ed efficacemente effettuate qualora rese mediante SATER all'indirizzo PEC del concorrente indicato in fase di registrazione.

Le richieste di accesso agli atti e le relative risposte sono effettuate attraverso il Sistema secondo le modalità indicate nelle guide all'utilizzo della piattaforma SATER "Richiesta di accesso agli atti" accessibili dal sito http://intercenter.regione.emilia-romagna.it/help/guide.

È onere della ditta concorrente provvedere tempestivamente a modificare i recapiti suindicati secondo le modalità esplicitate nelle guide per l'utilizzo della piattaforma "Registrazione e funzioni base" e "Gestione anagrafica" (per la modifica dei dati sensibili) accessibili dal sito http://intercenter.regione.emilia-romagna.it/help/guide.

Eventuali problemi temporanei nell'utilizzo di tali forme di comunicazione dovranno essere tempestivamente segnalati all'Agenzia; diversamente la medesima declina ogni responsabilità per il tardivo o mancato recapito delle comunicazioni.

In caso di raggruppamenti temporanei, GEIE, aggregazioni di imprese di rete o consorzi ordinari, anche se non ancora costituiti formalmente, la comunicazione recapitata al mandatario si intende validamente resa a tutti gli operatori economici raggruppati, aggregati o consorziati.

In caso di consorzi di cui all'art. 45, comma 2, lett. b) e c) del Codice, la comunicazione recapitata al consorzio si intende validamente resa a tutte le consorziate.

In caso di avvalimento, la comunicazione recapitata all'offerente si intende validamente resa a tutti gli operatori economici ausiliari.

3. OGGETTO DELL'APPALTO, IMPORTO E SUDDIVISIONE IN LOTTI

La gara è suddivisa nei seguenti lotti:

Descrizione dei lotti

Numero lotto	Oggetto del lotto	CIG	Importo
Lotto 1	**SERVIZI DI IT SYSTEM MANAGEMENT**	**97219284C8**	**€ 65.000.000,00**
Lotto 2	**SERVIZI DI SICUREZZA INFORMATICA**	**972192959B**	**€ 40.000.000,00**

Prestazioni oggetto del Lotto 1 e importo a base d'asta

n.	Descrizione servizi/beni	CPV	P *(principale)* S *(secondaria)*	Importo lotto in euro
1	**SERVIZI DI IT SYSTEM MANAGEMENT**	*72250000-2*	*P*	**65.000.000,00**
			Importo totale di gara:	**65.000.000,00**

Prestazioni oggetto del Lotto 2 e importo a base d'asta

n.	Descrizione servizi/beni	CPV	P *(principale)*	Importo lotto in euro
1	**SERVIZI DI SICUREZZA INFORMATICA**	*72250000-2*	*P*	**40.000.000,00**
			Importo totale di gara:	**40.000.000,00**

IMPORTO TOTALE LOTTI 1-2	**105.000.000,00**

Il dettaglio delle prestazioni è specificato nel Capitolato di gara e relativi allegati.

L'importo totale soggetto al ribasso è al netto di Iva e/o di altre imposte e contributi di legge, nonché degli oneri per la sicurezza dovuti a rischi da interferenze.

L'importo degli oneri per la sicurezza da interferenze è pari a € 0,00 Iva e/o altre imposte e contributi di legge esclusi e **non è soggetto a ribasso.**

Si precisa che il valore della Convenzione è frutto di una stima relativa al presumibile fabbisogno delle Amministrazioni contraenti che utilizzeranno la Convenzione stessa nell'arco temporale della sua durata. Pertanto, la predetta stima non è in alcun modo impegnativa né vincolante né per l'Agenzia né per le Amministrazioni contraenti nei confronti degli aggiudicatari.

In considerazione di quanto disposto dall'articolo 95, comma 10, del Codice, non deve essere indicata la stima dei costi della manodopera e degli oneri aziendali concernenti l'adempimento delle disposizioni in materia di salute e sicurezza sui luoghi di lavoro nel caso di servizi di natura intellettuale e di forniture senza posa in opera.

Nel caso in cui un concorrente risulti primo in graduatoria per entrambi i Lotti, al medesimo potrà essere aggiudicato solo il Lotto 1, in virtù della maggiore rilevanza economica dello stesso. Di conseguenza, per il Lotto 2, si procederà allo scorrimento della graduatoria e qualora non siano presenti altre offerte valide, il Lotto non sarà aggiudicato.

Stante quanto sopra, ai fini dell'aggiudicazione dei Lotti 1 e 2, si tiene altresì conto se gli operatori economici si trovino tra di loro in una situazione di controllo di cui all'articolo 2359 del codice civile o in una qualsiasi relazione, anche di fatto, se la situazione di controllo o la relazione comporti che le offerte sono imputabili ad un unico centro decisionale.

3.1 DURATA

La durata della Convenzione per ciascun Lotto è di **36** mesi, decorrenti dalla data di sottoscrizione della stessa.

Resta inteso che per durata della Convenzione, si intende il periodo entro il quale le Amministrazioni contraenti possono emettere Ordinativi di fornitura, vale a dire, stipulare contratti con il Fornitore.

Gli Ordinativi di fornitura emessi dalle singole Amministrazioni contraenti avranno durata minima annuale e massima di 36 mesi per i servizi a canone a far data dalla loro emissione; mentre per i servizi relativi alla richiesta di fabbisogni professionali la durata degli Ordinativi di Fornitura potrà essere variabile in relazione alla quantità di giornate richieste per le figure professionali previste.

La data di scadenza degli Ordinativi di fornitura, comunque, non potrà essere superiore alla data di scadenza, originaria o eventualmente rinnovata, della Convenzione stessa.

L'Agenzia si riserva la facoltà di risolvere la Convenzione in qualunque momento, senza ulteriori oneri per l'Agenzia medesima, qualora disposizioni legislative, regolamentari ed autorizzative non ne consentano la prosecuzione in tutto o in parte, ovvero negli altri casi stabiliti nella Convenzione medesima.

3.2 OPZIONI E RINNOVI

La Convenzione potrà essere rinnovata fino ad ulteriori **24** mesi, su comunicazione scritta dell'Agenzia, nell'ipotesi in cui alla scadenza del termine, **non** sia stato esaurito l'importo massimo spendibile, previsto per ogni singolo lotto.

La durata degli Ordinativi di fornitura in corso di esecuzione potrà essere modificata per il tempo strettamente necessario alla conclusione delle procedure necessarie per l'individuazione del nuovo contraente avviate prima della scadenza del contratto ai sensi dell'articolo 106, comma 11, del Codice dei Contratti. In tal caso il contraente è tenuto all'esecuzione delle prestazioni oggetto della Convenzione agli stessi - o più favorevoli - prezzi, patti e condizioni.

Nel caso in cui, prima del decorso del termine di durata della Convenzione, anche eventualmente rinnovato, sia esaurito l'importo massimo spendibile riferito al singolo lotto, al Fornitore potrà essere richiesto, alle stesse condizioni, di incrementare tale importo fino alla concorrenza di un quinto, ai sensi dell'articolo 106, comma 12, del Codice.

Fermo restando quanto sopra, l'Agenzia potrà altresì, nel corso dell'esecuzione, apportare variazioni secondo quanto previsto dal suddetto articolo.

4. SOGGETTI AMMESSI IN FORMA SINGOLA E ASSOCIATA E CONDIZIONI DI PARTECIPAZIONE

Gli operatori economici possono partecipare alla presente gara in forma singola o associata, purché in possesso dei requisiti prescritti dai successivi articoli.

Ai soggetti costituiti in forma associata si applicano le disposizioni di cui agli articoli 47 e 48 del Codice.

È vietato ai concorrenti di partecipare al singolo lotto in più di un raggruppamento temporaneo o consorzio ordinario di concorrenti o aggregazione di operatori economici aderenti al contratto di rete (nel prosieguo, aggregazione di retisti).

È vietato al concorrente che partecipa al singolo lotto in raggruppamento o consorzio ordinario di concorrenti, di partecipare anche in forma individuale.

È vietato al concorrente che partecipa al singolo lotto in aggregazione di imprese di rete, di partecipare anche in forma individuale. Le imprese retiste non partecipanti all'aggregazione possono presentare offerta, per il medesimo lotto, in forma singola o associata.

I consorzi di cui all'articolo 45, comma 2, lettere b) e c) del Codice sono tenuti ad indicare, in sede di offerta, per quali consorziati il consorzio concorre; a questi ultimi **è vietato** partecipare, in qualsiasi altra forma, al singolo lotto. In caso di violazione sono esclusi dalla gara sia il consorzio sia il consorziato; in caso di inosservanza di tale divieto si applica l'articolo 353 del codice penale.

In alternativa i consorzi di cui all'articolo 45 comma 2 lettera c) del Codice possono eseguire la prestazione con la propria struttura.

Nel caso di consorzi di cui all'articolo 45, comma 2, lettere b) e c) del Codice, le consorziate designate dal consorzio per l'esecuzione della Convenzione quadro non possono, a loro volta, a cascata, indicare un altro soggetto per l'esecuzione.

Qualora il consorziato designato sia, a sua volta, un consorzio di cui all'articolo 45 comma 2, lettera b) è tenuto anch'esso a indicare, in sede di offerta, i consorziati per i quali concorre; a questi ultimi è vietato partecipare, in qualsiasi altra forma, alla presente gara. In caso di violazione sono esclusi dalla gara sia il consorzio che la consorziata; in caso di inosservanza di tale divieto si applica l'articolo 353 del codice penale.

Il concorrente che intende partecipare a più lotti è tenuto a presentarsi sempre nella medesima forma (individuale o associata) ed in caso di RTI, sempre nella medesima composizione, **pena l'esclusione** del soggetto stesso e del concorrente in forma associata cui il soggetto partecipa. I consorzi di cui all'articolo 45, comma 2, lettere b) e c) del Codice possono indicare consorziati esecutori diversi, ma questi ultimi non possono partecipare in altra forma ad altri lotti pena la loro esclusione e quella del consorzio da tutti i lotti.

Fermo restando l'obbligo del RTI/Consorzio ordinario, in caso di partecipazione a più lotti, di presentarsi nella medesima composizione, le imprese potranno assumere, nei diversi lotti, ruoli diversi (mandataria/mandante) e/o una diversa percentuale di ripartizione delle quote, fatto salvo il rispetto per ogni lotto delle regole previste dal presente Disciplinare.

Le aggregazioni di retisti aderenti al contratto di rete di cui all'articolo 45, comma 2, lett. f) del Codice, rispettano la disciplina prevista per i raggruppamenti temporanei di imprese in quanto compatibile. In particolare:

a) **nel caso in cui la rete sia dotata di organo comune con potere di rappresentanza e soggettività giuridica (cd. rete - soggetto),** l'aggregazione di imprese di rete partecipa a mezzo dell'organo comune, che assumerà il ruolo della mandataria, qualora in possesso dei relativi requisiti. L'organo comune potrà indicare anche solo alcune tra le imprese retiste per la partecipazione alla gara ma dovrà obbligatoriamente far parte di queste;

b) **nel caso in cui la rete sia dotata di organo comune con potere di rappresentanza ma priva di soggettività giuridica (cd. rete-contratto),** l'aggregazione di imprese di rete partecipa a mezzo dell'organo comune, che assumerà il ruolo della mandataria, qualora in possesso dei requisiti previsti per la mandataria e qualora il contratto di rete rechi mandato allo stesso a presentare domanda di partecipazione o offerta per determinate tipologie di procedure di gara. L'organo comune potrà indicare anche solo alcune tra le imprese retiste per la partecipazione alla gara ma dovrà obbligatoriamente far parte di queste;

c) **nel caso in cui la rete sia dotata di organo comune privo di potere di rappresentanza ovvero sia sprovvista di organo comune, oppure se l'organo comune è privo dei requisiti di qualificazione**, l'aggregazione di imprese di rete partecipa nella forma del raggruppamento costituito o costituendo, con applicazione integrale delle relative regole.

Per tutte le tipologie di rete, la partecipazione congiunta alle gare deve risultare individuata nel contratto di rete come uno degli scopi strategici inclusi nel programma comune, mentre la durata dello stesso dovrà essere commisurata ai tempi di realizzazione dell'appalto.

Il ruolo di mandante/mandataria di un raggruppamento temporaneo di imprese può essere assunto anche da un consorzio di cui all'articolo 45, comma 1, lett. b), c) ovvero da una sub-associazione, nelle forme di un RTI o consorzio ordinario costituito oppure di un'aggregazione di imprese di rete.

A tal fine, se la rete è dotata di organo comune con potere di rappresentanza (con o senza soggettività giuridica), tale organo assumerà la veste di mandataria della sub-associazione; se, invece, la rete è dotata di organo comune privo del potere di rappresentanza o è sprovvista di organo comune, il ruolo di mandataria della sub-associazione è conferito dalle imprese retiste partecipanti alla gara, mediante mandato dando evidenza della ripartizione delle quote di partecipazione.

L'impresa in concordato preventivo con continuità aziendale può concorrere anche riunita in RTI purché non rivesta la qualità di mandataria e sempre che le altre imprese aderenti al RTI non siano assoggettate ad una procedura concorsuale.

Secondo quanto previsto dalla deliberazione AGCM 18/09/2013, in caso di anomalie comportamentali che possono essere indizio di fenomeni anticoncorrenziali, tra cui la partecipazione in R.T.I. di imprese in grado di partecipare alla gara singolarmente, l'Agenzia procederà a segnalare all'Autorità tali fenomeni. La delibera è consultabile all'indirizzo: http://www.agcm.it/stampa/news/6647-varato-il-vademecum-sugli-appalti.html.

5. REQUISITI GENERALI

Sono **esclusi** dalla gara gli operatori economici per i quali sussistono cause di esclusione di cui all'articolo 80 del Codice. In caso di partecipazione di consorzi di cui all'articolo 45, comma 2, lettere b) e c), del Codice la sussistenza dei requisiti di cui all'articolo 80 del Codice è attestata e verificata nei confronti del consorzio e delle consorziate indicate quali esecutrici.

Costituisce causa di esclusione degli operatori economici dalla procedura di gara il mancato rispetto, al momento della presentazione dell'offerta, degli obblighi in materia di lavoro delle persone con disabilità di cui alla legge 12 marzo 1999, n. 68, oltre che ai sensi dell'art. 80, comma 5, lettera i), del Codice.

Sono comunque **esclusi** gli operatori economici che abbiano affidato incarichi in violazione dell'articolo 53, comma 16-*ter*, del d.lgs. del 2001 n. 165 a soggetti che hanno esercitato, in qualità di dipendenti, poteri autoritativi o negoziali presso l'amministrazione affidante negli ultimi tre anni.

La mancata accettazione delle clausole contenute nell'Allegato 1b - Patto di integrità e il mancato rispetto dello stesso costituiscono **causa di esclusione** dalla gara, ai sensi dell'articolo 83 bis del D.Lgs. n. 159/2011.

Tutti i soggetti interessati a partecipare alla procedura devono **obbligatoriamente** registrarsi al sistema accedendo all'apposito link sul Portale dell'Autorità (Servizi ad accesso riservato – **FVOE**) secondo le istruzioni contenute.

La verifica del possesso dei requisiti di **carattere generale** avviene attraverso l'utilizzo della **Banca Dati ANAC** e, nello specifico, mediante il Fascicolo virtuale.

Nelle more dell'effettiva messa a regime del FVOE e qualora si riscontrassero difficoltà operative nell'utilizzo dello stesso che impediscano o ritardino le operazioni di verifica dei requisiti di partecipazione in capo agli operatori economici, l'Agenzia si riserva la facoltà di effettuare la verifica secondo le modalità preesistenti al rilascio del FVOE.

6. REQUISITI SPECIALI E MEZZI DI PROVA

I concorrenti, **a pena di esclusione**, devono essere in possesso dei requisiti previsti nei commi seguenti.

La verifica del possesso dei requisiti di carattere tecnico-organizzativo comprovabili mediante i documenti indicati di seguito avviene attraverso l'utilizzo della Banca Dati ANAC e, nello specifico, mediante il Fascicolo virtuale.

6.1 REQUISITI DI IDONEITÀ

Costituiscono requisiti di idoneità:

a) Iscrizione nel Registro delle Imprese oppure nell'Albo delle Imprese artigiane per attività coerenti con quelle oggetto della presente procedura di gara.

b) Possesso dei requisiti di idoneità tecnico professionale necessari per la corretta esecuzione del servizio, di cui all'art. 26, comma 1, lettera a), punto 2, del d.lgs. n. 81/2008 e s.m.i..

Il concorrente non stabilito in Italia ma in altro Stato Membro o in uno dei Paesi di cui all'art. 83, comma 3, del Codice, presenta dichiarazione giurata o secondo le modalità vigenti nello Stato nel quale è stabilito.

Per la comprova dei sopra indicati requisiti l'Agenzia acquisisce d'ufficio i documenti in possesso di pubbliche amministrazioni, previa indicazione, da parte dell'operatore economico, degli elementi indispensabili per il reperimento delle informazioni o dei dati richiesti.

6.2 REQUISITI DI CAPACITÀ ECONOMICA E FINANZIARIA

Non previsti.

6.3 REQUISITI DI CAPACITÀ TECNICA E PROFESSIONALE

Esecuzione di servizi analoghi.

Per il Lotto1:

a) aver eseguito o avere in corso di esecuzione, nel triennio precedente la pubblicazione del bando sulla GUUE, uno o più contratti (fino ad un massimo di dieci) per un valore complessivo non inferiore a € 10.000.000,00 (IVA esclusa) con soggetti pubblici o privati aventi ad oggetto servizi analoghi a quelli della presente procedura di gara;

oppure

(in mancanza del requisito sopra indicato per giustificati motivi quali la costituzione di nuova impresa):

aver eseguito o avere in corso di esecuzione, nell'anno precedente la pubblicazione del bando sulla GUUE, uno o più contratti (fino ad un massimo di quattro) per un valore complessivo non inferiore a € 2.500.000,00 (IVA esclusa) con soggetti pubblici o privati aventi ad oggetto servizi analoghi a quelli della presente procedura di gara.

b) Possesso di una valutazione di conformità del proprio sistema di gestione della qualità alla norma UNI EN ISO 9001:2015 nel settore IT System Management (gestione dei sistemi informativi), idonea, pertinente e proporzionata ai servizi oggetto della presente procedura di gara (Lotto 1).

Per il Lotto2:

a) aver eseguito o avere in corso di esecuzione, nel triennio precedente la pubblicazione del bando sulla GUUE, uno o più contratti (fino ad un massimo di dieci) per un valore complessivo non inferiore a € 5.000.000,00 (IVA esclusa) con soggetti pubblici o privati aventi ad oggetto servizi analoghi a quelli della presente procedura di gara (Lotto 2);

oppure

(in mancanza del requisito sopra indicato per giustificati motivi quali la costituzione di nuova impresa):

aver eseguito o avere in corso di esecuzione, nell'anno precedente la pubblicazione del bando sulla GUUE, uno o più contratti (fino ad un massimo di quattro) per un valore complessivo non inferiore a € 1.250.000,00 (IVA esclusa) con soggetti pubblici o privati aventi ad oggetto servizi analoghi a quelli della presente procedura di gara.

b) Possesso di una valutazione di conformità del proprio sistema di gestione della qualità alla norma UNI EN ISO 9001:2015 nel settore della sicurezza informatica, idonea, pertinente e proporzionata ai servizi oggetto della presente procedura di gara.

La comprova del requisito di cui al punto a) dei Lotti 1 e 2 "**Esecuzione di servizi analoghi**" è fornita mediante:

- certificati rilasciati dall'amministrazione/ente contraente, con l'indicazione dell'oggetto, dell'importo e del periodo di esecuzione;
- contratti stipulati con le amministrazioni pubbliche, completi di copia delle fatture quietanzate ovvero dei documenti bancari attestanti il pagamento delle stesse;
- attestazioni rilasciate dal committente privato con l'indicazione dell'oggetto, dell'importo e del periodo di esecuzione.

- contratti stipulati con privati, completi di copia delle fatture quietanzate ovvero dei documenti bancari attestanti il pagamento delle stesse;

La comprova del requisito di cui al punto b) dei Lotti 1 e 2 "**Certificazione ISO 9001**" è fornita mediante un **certificato** di conformità rilasciato da un organismo di certificazione accreditato ai sensi della norma UNI CEI EN ISO/IEC 17021-1 per lo specifico settore e campo di applicazione/scopo del certificato richiesto, da un Ente nazionale unico di accreditamento firmatario degli accordi EA/MLA oppure autorizzato a norma dell'articolo 5, paragrafo 2 del Regolamento (CE), n. 765/2008. L'operatore economico che non ha la possibilità di ottenere la predetta documentazione entro il termine richiesto, per una causa a sè non imputabile, può presentare altri mezzi di prova *idonei a dimostrare* che le misure di garanzia della qualità soddisfano le norme di garanzia richieste.

6.4 INDICAZIONI PER I RAGGRUPPAMENTI TEMPORANEI, CONSORZI ORDINARI, AGGREGAZIONI DI IMPRESE DI RETE, GEIE

I soggetti di cui all'articolo 45, comma 2, lett. d), e), f) e g) del Codice devono possedere i requisiti di partecipazione nei termini di seguito indicati.

Alle aggregazioni di retisti, ai consorzi ordinari ed ai GEIE si applica la disciplina prevista per i raggruppamenti temporanei di imprese. Nei consorzi ordinari la consorziata che assume la quota maggiore di attività esecutive riveste il ruolo di capofila che è assimilata alla mandataria.

Nel caso in cui la mandante/mandataria di un raggruppamento temporaneo di imprese sia una sub-associazione, nelle forme di un consorzio ordinario costituito oppure di un'aggregazione di retisti, i relativi requisiti di partecipazione sono soddisfatti secondo le medesime modalità indicate per i raggruppamenti.

Il **requisito relativo all'iscrizione** nel Registro delle Imprese oppure nell'Albo delle Imprese artigiane di cui alla lettera a) ed il requisito di cui alla lettera b) devono essere posseduti:

a. da ciascun componente del raggruppamento/consorzio/GEIE anche da costituire, nonché dal GEIE medesimo;
b. da ciascuna componente dell'aggregazione di rete nonché dall'organo comune-nel caso in cui questa abbia soggettività giuridica.

Nell'ipotesi di raggruppamento temporaneo orizzontale il requisito dell'esecuzione di servizi analoghi di cui al precedente **punto 6.3 lett. a) dei Lotti 1 e 2**, deve essere posseduto dal raggruppamento nel suo complesso.

In caso di RTI la certificazione ISO 9001 di cui al punto **6.3 lett b) dei Lotti 1 e 2** dovrà essere posseduta da ciascuno dei componenti del raggruppamento.

6.5 INDICAZIONI PER I CONSORZI DI COOPERATIVE E DI IMPRESE ARTIGIANE E I CONSORZI STABILI

I soggetti di cui all'articolo 45, comma 2, lett. b) e c) del Codice devono possedere i requisiti di partecipazione nei termini di seguito indicati.

Il **requisito relativo all'iscrizione nel Registro delle Imprese oppure nell'Albo delle Imprese artigiane** di cui al **punto 6.1 lett. a)** deve essere posseduto dal consorzio e dalle imprese consorziate indicate come esecutrici.

Il requisito dell'esecuzione di servizi analoghi di cui al precedente **punto 6.3 lett. a)**, **dei Lotti 1 e 2**, deve essere posseduto:

1. per i consorzi di cui all'articolo 45, comma 2 lettera b) del Codice, direttamente dal consorzio medesimo, salvo che quelli relativi alla disponibilità delle attrezzature e dei mezzi d'opera nonché all'organico medio annuo che sono computati cumulativamente in capo al consorzio ancorché posseduti dalle singole imprese consorziate;

2. per i consorzi di cui all'art. 45, comma 2, lett. c) del Codice, dal consorzio, che può spendere, oltre ai propri requisiti, anche quelli delle consorziate i quali vengono computati cumulativamente in capo al consorzio.

Il requisito della certificazione ISO 9001 di cui al punto 6.3, lett b), dei Lotti 1 e 2 è attestato e verificato in relazione:

a) al consorzio e alle singole imprese consorziate indicate quali esecutrici;

b) al solo consorzio il cui ambito di certificazione del sistema gestionale include la verifica che l'erogazione dei servizi o delle forniture da parte delle imprese consorziate indicate quali esecutrici rispettino i requisiti delle norme coperte da certificazione;

c) alle imprese consorziate indicate come esecutrici in caso di certificazioni specificamente correlate alla attività oggetto dell'appalto.

7. AVVALIMENTO

Il concorrente può soddisfare la richiesta dei requisiti di carattere economico -finanziario e tecnico professionale di cui al punto 6.3 anche mediante ricorso all'avvalimento.

L'avvalimento è obbligatorio per gli operatori economici che hanno depositato la domanda di concordato, qualora non sia stato ancora depositato il decreto previsto dall'articolo 163 del regio decreto 16 marzo 1942, n. 267.

Non è consentito l'avvalimento per la dimostrazione dei requisiti generali e di idoneità professionale.

Il ricorso all'avvalimento per la certificazione ISO 9001 di cui al punto **6.3, lett b), dei Lotti 1 e 2** comporta che l'ausiliaria metta a disposizione dell'ausiliata per l'esecuzione dell'appalto le proprie risorse e il proprio apparato organizzativo in tutte le parti che giustificano l'attribuzione del requisito di qualità.

L'ausiliaria deve:

a) possedere i requisiti previsti dal paragrafo 5 nonché i requisiti tecnici e le risorse oggetto di avvalimento e dichiararli presentando un proprio DGUE, da compilare nelle parti pertinenti;

b) rilasciare la dichiarazione di avvalimento contenente l'obbligo verso il concorrente e verso l'Agenzia, di mettere a disposizione, per tutta la durata dell'appalto, le risorse necessarie di cui è carente il concorrente.

Il concorrente deve allegare il contratto di avvalimento nel quale sono specificati i requisiti economico-finanziari e tecnico-organizzativi messi a disposizione e le correlate risorse strumentali e umane.

Il concorrente può avvalersi di più imprese ausiliare.

A pena di esclusione, non è consentito che l'ausiliaria presti avvalimento per più di un concorrente e che partecipino al medesimo lotto sia l'ausiliaria che l'impresa concorrente che si avvale dei requisiti.

Il concorrente e l'ausiliaria sono responsabili in solido nei confronti della Agenzia, per quanto di competenza, e delle Amministrazioni contraenti in relazione alle prestazioni oggetto della Convenzione e degli Ordinativi di fornitura

Qualora per l'ausiliaria sussistano motivi di esclusione o laddove essa non soddisfi i pertinenti criteri di selezione, il concorrente sostituisce l'impresa ausiliaria entro 7 giorni decorrenti dal ricevimento della richiesta da parte dell'Agenzia. Contestualmente il concorrente produce i documenti richiesti per l'avvalimento.

È sanabile, mediante soccorso istruttorio, la mancata produzione delle dichiarazioni dell'ausiliaria o del contratto di avvalimento, a condizione che i citati elementi siano preesistenti e comprovabili con documenti di data certa, anteriore al termine di presentazione dell'offerta.

Non è sanabile - e quindi è causa di esclusione dalla gara - la mancata indicazione dei requisiti e delle risorse messi a disposizione dall'ausiliaria in quanto causa di nullità del contratto di avvalimento.

8. SUBAPPALTO

Non può essere affidata in subappalto l'integrale esecuzione della Convenzione.

Il concorrente indica, all'atto dell'offerta, le parti del servizio/fornitura che intende subappaltare o concedere in cottimo. In caso di mancata indicazione delle parti da subappaltare il subappalto è vietato.

L'aggiudicatario e il subappaltatore sono responsabili in solido nei confronti della stazione appaltante dell'esecuzione delle prestazioni oggetto del contratto di subappalto.

9. GARANZIA PROVVISORIA

L'offerta è corredata, **a pena di esclusione**, da:

1) **una garanzia provvisoria** pari al due per cento (2%) dell'importo a base di gara del singolo lotto e precisamente di importo pari ad **€ 1.300.000,00 per il Lotto 1 e ad € 800.000,00 per il Lotto 2**.

   (Stante il vincolo di aggiudicazione previsto, per l'operatore economico che partecipa ad entrambi i Lotti il valore della garanzia definitiva sarà commisurato a quello del solo lotto aggiudicabile, ovvero il Lotto 1).

   Si applicano le riduzioni di cui all'articolo 93 comma 7 del Codice.

2) **una dichiarazione di impegno,** da parte di un istituto bancario o assicurativo o altro soggetto di cui all'articolo 93, comma 3 del Codice, anche diverso da quello che ha rilasciato la garanzia provvisoria, **a rilasciare garanzia fideiussoria definitiva** qualora il concorrente risulti affidatario. Tale dichiarazione di impegno non è richiesta alle microimprese, piccole e medie imprese e ai raggruppamenti temporanei o consorzi ordinari esclusivamente dalle medesime costituiti.

In caso di partecipazione a più lotti sono prestate tante distinte ed autonome garanzie provvisorie e impegni al rilascio della definitiva quanti sono i lotti cui si intende partecipare ovvero la concorrente può prestare un'unica cauzione cumulativa, purché nella medesima siano indicati specificatamente i lotti cui si partecipa ed i relativi importi.

La **garanzia provvisoria è costituita**, a scelta del concorrente:

a. da cauzione presso l'istituto incaricato del servizio di tesoreria Unicredit S.p.A. a titolo di pegno a favore di Intercent-ER, con bonifico bancario utilizzando le seguenti coordinate: IBAN IT 48 Z 02008 02435 000010670122 – Codice BIC Swift UNCRITM1BA2 - codice dell'Ente 3182065 - CONTO CAUZIONI Intercent-ER;

b. da fideiussione bancaria o assicurativa rilasciata da imprese bancarie o assicurative che: risponde ai requisiti di solvibilità previsti dalle leggi che ne disciplinano le rispettive attività o rilasciata da un intermediario finanziario iscritto nell'albo di cui all'articolo 106 del decreto

legislativo 1 settembre 1993, n. 385; svolge in via esclusiva o prevalente attività di rilascio di garanzie; è sottoposta a revisione contabile da parte di una società di revisione iscritta nell'albo previsto dall'articolo 161 del decreto legislativo 24 febbraio 1998, n. 58; ha i requisiti minimi di solvibilità richiesti dalla vigente normativa bancaria assicurativa rispondano ai requisiti di cui all'articolo 93, comma 3 del Codice.

Gli operatori economici, prima di procedere alla sottoscrizione della garanzia, sono tenuti a verificare che il soggetto garante sia in possesso dell'autorizzazione al rilascio di garanzie mediante accesso ai seguenti siti internet:

- http://www.bancaditalia.it/compiti/vigilanza/intermediari/index.html
- http://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/garanzie-finanziarie/
- http://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/soggetti-non-legittimati/Intermediari_non_abilitati.pdf
- http://www.ivass.it/ivass/imprese_jsp/HomePage.jsp

La **garanzia fideiussoria** deve:

1) contenere espressa menzione dell'oggetto dell'appalto e del soggetto garantito;
2) essere intestata a tutti gli operatori economici del costituito/costituendo raggruppamento temporaneo o consorzio ordinario o GEIE, ovvero a tutte le imprese retiste che partecipano alla gara ovvero, in caso di consorzi di cui all'articolo 45, comma 2, lett. b) e c) del Codice, al solo consorzio;
3) essere conforme allo schema tipo approvato con decreto del Ministro dello sviluppo economico n. 193 del 16.09.2022;
4) avere validità per almeno **240** giorni dalla data di presentazione dell'offerta;
5) prevedere espressamente:
   a. la rinuncia al beneficio della preventiva escussione del debitore principale di cui all'articolo 1944 del Codice civile;
   b. la rinuncia ad eccepire la decorrenza dei termini di cui all'articolo 1957, secondo comma, del Codice civile;
   c. la sua operatività entro quindici giorni a semplice richiesta scritta dell'Agenzia;
6) contenere l'impegno a rilasciare la garanzia definitiva, ove rilasciata dal medesimo garante;
7) essere corredata dall'impegno del garante a rinnovare la garanzia ai sensi dell'articolo 93, comma 5, del Codice, su richiesta dell'Agenzia, nel caso in cui al momento della sua scadenza non sia ancora intervenuta l'aggiudicazione.

La garanzia fideiussoria e la dichiarazione di impegno devono essere **sottoscritte** da un soggetto in possesso dei poteri necessari per impegnare il garante ed essere inserite sul SATER in una delle seguenti forme**:**

- originale informatico, ai sensi dell'articolo 1, lett. p) del D.lgs. 82/2005, sottoscritto con firma digitale dal soggetto in possesso dei poteri necessari per impegnare il garante;
- copia informatica di documento analogico (scansione di documento cartaceo) secondo le modalità previste dall'articolo 22, commi 1 e 2, del D.Lgs. 82/2005;
- In duplicato informatico dell'originale informatico conforme alle disposizioni dell'articolo 23-bis del D.Lgs. n. 82/2005.

In caso di bonifico, assegni ecc., il concorrente deve inserire su SATER il documento che attesti l'avvenuto versamento in una delle forme sopra indicate. Il documento deve indicare il nominativo dell'operatore economico che ha operato il versamento stesso.

In caso di richiesta di estensione della durata e validità dell'offerta e della garanzia fideiussoria, il concorrente potrà produrre una nuova garanzia provvisoria di altro garante, in sostituzione della precedente, a condizione che abbia espressa decorrenza dalla data di presentazione dell'offerta.

L'importo della garanzia e del suo eventuale rinnovo **è ridotto** secondo le misure e le modalità di cui all'articolo 93, comma 7, del Codice.

Per fruire di dette riduzioni il concorrente dichiara nella domanda di partecipazione il possesso dei relativi requisiti.

In caso di partecipazione in forma associata, la riduzione del 50% per il possesso della certificazione del sistema di qualità di cui all'articolo 93, comma 7, si ottiene:

a. per i soggetti di cui all'articolo 45, comma 2, lett. d), e), f), g), del Codice solo se tutte le imprese che costituiscono il raggruppamento, consorzio ordinario o GEIE, o tutte le imprese retiste che partecipano alla gara siano in possesso della predetta certificazione;
b. per i consorzi di cui all'articolo 45, comma 2, lett. b) e c) del Codice, se il Consorzio ha dichiarato in fase di offerta che intende eseguire con risorse proprie, sole se il Consorzio possiede la predetta certificazione; se il Consorzio ha indicato in fase di offerta che intende assegnare parte delle prestazioni a una o più consorziate individuate nell'offerta, solo se sia il Consorzio sia la consorziata designata posseggono la predetta certificazione, o in alternativa se il solo Consorzio possiede la predetta certificazione e l'ambito di certificazione del suo sistema gestionale include la verifica che l'erogazione della prestazione da parte della consorziata rispetti gli standard fissati dalla certificazione.

Le altre riduzioni previste dall'articolo 93, comma 7, del Codice si ottengono nel caso di possesso da parte di una sola associata oppure, per i consorzi di cui all'articolo 45, comma 2, lett. b) e c) del Codice, da parte del consorzio e/o delle consorziate.

È sanabile, mediante soccorso istruttorio, la mancata presentazione della garanzia provvisoria e/o dell'impegno a rilasciare garanzia fideiussoria definitiva solo a condizione che siano stati già costituiti nella loro integrità prima della presentazione dell'offerta.

Non è sanabile - e quindi **è causa di esclusione** - la sottoscrizione della garanzia provvisoria da parte di un soggetto non legittimato a rilasciare la garanzia o non autorizzato ad impegnare il garante.

10. SOPRALLUOGO

Non previsto.

11. PAGAMENTO DEL CONTRIBUTO A FAVORE DELL'ANAC

I concorrenti effettuano, **a pena di esclusione**, il pagamento del contributo previsto dalla legge in favore dell'Autorità Nazionale Anticorruzione secondo le modalità di cui alla delibera ANAC n. 621 del 20 Dicembre 2022 secondo le modalità indicate sul Portale dei pagamenti dell'ANAC all'indirizzo https://www.anticorruzione.it/-/portale-dei-pagamenti-di-anac.

Il contributo dovuto è pari a **€ 500,00** per ciascun lotto per il quale si presenta offerta.

Il concorrente allega copia della ricevuta di pagamento del contributo.

In caso di mancata presentazione l'Agenzia accerta il pagamento del contributo mediante consultazione del sistema FVOE.

Qualora il pagamento non risulti registrato nel sistema, la mancata presentazione della ricevuta potrà essere sanata ai sensi dell'articolo 83, comma 9, del Codice, a condizione che il pagamento sia stato già effettuato prima della scadenza del termine di presentazione dell'offerta.

In caso di mancata dimostrazione dell'avvenuto pagamento, l'Agenzia **esclude** il concorrente dal lotto per il quale non è stato versato il contributo, ai sensi dell'articolo 1, comma 67 della l. 266/2005.

12. MODALITÀ DI PRESENTAZIONE DELL'OFFERTA E SOTTOSCRIZIONE DEI DOCUMENTI DI GARA

L'offerta e la documentazione relativa alla procedura devono essere presentate esclusivamente attraverso SATER.

Non sono considerate valide le offerte presentate attraverso modalità diverse da quelle previste nel presente disciplinare. L'offerta e la documentazione devono essere sottoscritti con firma digitale.

Le dichiarazioni sostitutive si redigono ai sensi degli articoli 19, 46 e 47 del decreto del Presidente della Repubblica n.445/2000.

La documentazione presentata in copia è accompagnata da dichiarazione di conformità all'originale ai sensi del decreto legislativo n. 82/05.

L'offerta deve pervenire entro e non oltre le ore 16,00 del giorno 04/07/2023 a pena di irricevibilità.

SATER non accetta offerte presentate dopo la data e l'orario stabiliti come termine ultimo di presentazione dell'offerta.

Della data e dell'ora di arrivo dell'offerta fa fede l'orario registrato dalla piattaforma.

Le operazioni di inserimento su SATER di tutta la documentazione richiesta rimangono ad esclusivo rischio del concorrente. Si invitano pertanto i concorrenti ad avviare tali attività con *congruo anticipo* rispetto alla scadenza prevista onde evitare la non completa e quindi mancata trasmissione dell'offerta entro il termine previsto.

Qualora si verifichi un mancato funzionamento o un malfunzionamento di SATER si applica quanto previsto al paragrafo 1.1.

Ogni operatore economico per la presentazione dell'offerta ha a disposizione una capacità pari alla dimensione massima di 100 *megabyte* per singolo file o cartella compressa.

12.1 REGOLE PER LA PRESENTAZIONE DELL'OFFERTA

La presentazione dell'offerta (documentazione amministrativa, offerta tecnica e offerta economica) deve essere effettuata su SATER secondo le modalità esplicitate nelle guide per l'utilizzo della piattaforma, accessibili dal sito http://intercenter.regione.emilia-romagna.it/help/guide. **Si raccomanda di seguire pedissequamente la procedura riportata nelle guide, eseguendo le operazioni richieste nella sequenza riportata nelle stesse.**

L' **"OFFERTA"** è composta da:

A – **Documentazione amministrativa**;

B – **Offerta tecnica** (una per ogni lotto per il quale si intende partecipare);

C – **Offerta economica** (una per ogni lotto per il quale si intende partecipare).

È ammessa offerta successiva, purché entro il termine di scadenza, a sostituzione della precedente. Prima della scadenza del termine perentorio per la presentazione delle offerte, il concorrente può sottoporre una nuova offerta che all'atto dell'invio invaliderà quella precedentemente inviata. A tal proposito si precisa che qualora, alla scadenza della gara, risultino presenti su SATER più offerte dello stesso operatore economico, salvo diversa indicazione dell'operatore stesso, verrà ritenuta valida l'offerta collocata temporalmente come ultima.

Si precisa inoltre che:

- l'offerta è vincolante per il concorrente;
- con la trasmissione dell'offerta, il concorrente accetta tutta la documentazione di gara, allegati e chiarimenti inclusi.

Al momento della ricezione delle offerte, ai sensi dell'articolo 58, comma 5 del Codice, ciascun concorrente riceve notifica del corretto recepimento della documentazione inviata all'indirizzo PEC indicato in sede di registrazione.

SATER consente al concorrente di visualizzare l'avvenuta trasmissione della domanda.

Il concorrente che intenda partecipare in forma associata (per esempio raggruppamento temporaneo di imprese/Consorzi, sia costituiti che costituendi) in sede di presentazione dell'offerta indica la forma di partecipazione e indica gli operatori economici riuniti o consorziati.

Tutta la documentazione da produrre deve essere in lingua italiana.

In caso di mancanza, incompletezza o irregolarità della traduzione della documentazione amministrativa, si applica l'articolo 83, comma 9 del Codice.

L'offerta vincola il concorrente per 240 giorni dalla scadenza del termine indicato per la presentazione dell'offerta.

Nel caso in cui alla data di scadenza della validità delle offerte le operazioni di gara siano ancora in corso, sarà richiesto agli offerenti di confermare la validità dell'offerta sino alla data indicata e di produrre un apposito documento attestante la validità della garanzia prestata in sede di gara fino alla medesima data.

Il mancato riscontro alla richiesta dell'Agenzia entro il termine fissato da quest'ultima è considerato come rinuncia del concorrente alla partecipazione alla gara.

13. SOCCORSO ISTRUTTORIO

Le carenze di qualsiasi elemento formale della domanda, e in particolare, la mancanza, l'incompletezza e ogni altra irregolarità essenziale degli elementi e del DGUE, con esclusione di quelle afferenti al contenuto sostanziale dell'offerta economica e dell'offerta tecnica, possono essere sanate attraverso la procedura di soccorso istruttorio di cui all'articolo 83, comma 9, del Codice.

L'irregolarità essenziale è sanabile laddove non si accompagni ad una carenza sostanziale del requisito alla cui dimostrazione la documentazione omessa o irregolarmente prodotta era finalizzata. La successiva correzione o integrazione documentale è ammessa laddove consenta di attestare l'esistenza di circostanze preesistenti, vale a dire requisiti previsti per la partecipazione e documenti/elementi a corredo dell'offerta. Nello specifico valgono le seguenti regole:

- il mancato possesso dei prescritti requisiti di partecipazione non è sanabile mediante soccorso istruttorio ed è **causa di esclusione** dalla procedura di gara;
- l'omessa o incompleta nonché irregolare presentazione delle dichiarazioni sul possesso dei requisiti di partecipazione e ogni altra mancanza, incompletezza o irregolarità del DGUE e della domanda sono sanabili, ad eccezione delle false dichiarazioni;
- la mancata presentazione di elementi a corredo dell'offerta (es. garanzia provvisoria e impegno del fideiussore) ovvero di condizioni di partecipazione gara (es. mandato collettivo

speciale o impegno a conferire mandato collettivo), entrambi aventi rilevanza in fase di gara, sono sanabili, solo se preesistenti e comprovabili con elementi di data certa, anteriore al termine di presentazione dell'offerta;

- il difetto di sottoscrizione della domanda di partecipazione, del DGUE, delle dichiarazioni richieste e dell'offerta è sanabile.

Ai fini del soccorso istruttorio l'Agenzia assegna al concorrente un congruo termine - non superiore a **dieci** giorni - perché siano rese, integrate o regolarizzate le dichiarazioni necessarie, indicando il contenuto e i soggetti che le devono rendere e la documentazione richiesta da trasmettere tramite SATER.

Ove il concorrente produca dichiarazioni o documenti non perfettamente coerenti con la richiesta, l'Agenzia *può* chiedere ulteriori precisazioni o chiarimenti, *limitate alla documentazione presentata in fase di soccorso istruttorio*, fissando un termine **perentorio a pena di esclusione**.

In caso di inutile decorso del termine, l'Agenzia procede all'**esclusione** del concorrente dalla procedura.

14. DOMANDA DI PARTECIPAZIONE E DOCUMENTAZIONE AMMINISTRATIVA

L'operatore economico inserisce sul SATER secondo le modalità indicate nelle guide per l'utilizzo della piattaforma http://intercenter.regione.emilia-romagna.it/help/guide la seguente documentazione:

1. domanda di partecipazione ed eventuale procura/e;
2. DGUE del concorrente (se in RTI DGUE di mandataria e mandanti);
3. garanzia provvisoria e dichiarazione di impegno di un fideiussore;
4. copia informatica della ricevuta di avvenuto pagamento del contributo all'ANAC;
5. PASSOE;
6. documentazione in caso di avvalimento di cui al punto 14.4;
7. documentazione per i soggetti associati di cui al successivo punto 14.5.

14.1 DOMANDA DI PARTECIPAZIONE ED EVENTUALE PROCURA

La domanda di partecipazione è redatta secondo il modello Allegato 1a - Domanda di partecipazione.

Nella domanda di partecipazione il concorrente indica i propri dati identificativi (ragione sociale, codice fiscale, sede) la forma singola o associata con la quale partecipa al lotto e il CCNL applicato con l'indicazione del relativo codice alfanumerico unico di cui all'articolo 16 quater del D.L. n. 76/2020 (punto A.2 della Domanda di partecipazione).

Il concorrente indica nella domanda di partecipazione per quale lotto concorre.

In caso di partecipazione in RTI, consorzio ordinario, aggregazione di imprese di rete, GEIE, il concorrente fornisce i dati identificativi (ragione sociale, codice fiscale, sede) e il ruolo di ciascuna impresa (mandataria/mandante, capofila/consorziata).

Nel caso di consorzio di cooperative e imprese artigiane o di consorzio stabile di cui all'articolo 45, comma 2 lett. b) e c) del Codice, il consorzio indica il consorziato per il quale concorre alla gara; qualora il consorziato designato sia, a sua volta, un consorzio di cui all'articolo 45, comma 2, lettera b) del Codice, esso deve indicare il consorziato o i consorziati per il quale o per i quali concorre, in assenza si intende che lo stesso partecipa in nome e per conto proprio.

Nella domanda di partecipazione il concorrente dichiara:

- i dati identificativi (nome, cognome, data e luogo di nascita, codice fiscale, comune di residenza etc.) dei soggetti di cui all'articolo 80, comma 3 del Codice, ovvero indica la banca dati ufficiale o il pubblico registro da cui i medesimi possono essere ricavati in modo aggiornato alla data di presentazione dell'offerta;
- di non partecipare alla medesima gara in altra forma singola o associata, né come ausiliaria per altro concorrente;
- di accettare, senza condizione o riserva alcuna, tutte le norme e disposizioni contenute nella documentazione gara,
- di essere edotto degli obblighi derivanti dal Codice di comportamento adottato dalla Regione Emilia-Romagna con Delibera di Giunta n. 905/2018, reperibile sul sito della Agenzia, e di impegnarsi, in caso di aggiudicazione, ad osservare e a far osservare ai propri dipendenti e collaboratori, per quanto applicabile, il suddetto codice, pena la risoluzione del contratto;
- di accettare il patto di integrità approvato dalla Regione Emilia-Romagna con Delibera della Giunta del 13 aprile 2022 n. 565 allegato alla documentazione di gara. La mancata accettazione delle clausole contenute nel patto di integrità costituisce causa di esclusione dalla gara, ai sensi dell'articolo 83-bis, del decreto legislativo 159/2011;
- [*NEL CASO DI OPERATORI ECONOMICI NON RESIDENTI E PRIVI DI STABILE ORGANIZZAZIONE IN ITALIA*] l'impegno ad uniformarsi, in caso di aggiudicazione, alla disciplina di cui agli articoli 17, comma 2, e 53, comma 3 del decreto del Presidente della Repubblica 633/72 e a comunicare alla Agenzia la nomina del proprio rappresentante fiscale, nelle forme di legge;
- [*NEL CASO DI OPERATORI ECONOMICI NON RESIDENTI E PRIVI DI STABILE ORGANIZZAZIONE IN ITALIA*] il domicilio fiscale …, il codice fiscale …, la partita IVA …, l'indirizzo di posta elettronica certificata o strumento analogo negli altri Stati Membri, ai fini delle comunicazioni di cui all'articolo 76, comma 5 del Codice;
- di aver preso visione e di accettare il trattamento dei dati personali di cui al punto 27.

In caso di incorporazione, fusione societaria o cessione o affitto d'azienda, le dichiarazioni di cui all'articolo 80, commi 1, 2 e 5, lettera l) del Codice, devono riferirsi anche ai soggetti di cui all'articolo

80 comma 3 del Codice che hanno operato presso la società incorporata, che si è fusa o che ha ceduto o dato in affitto l'azienda nell'anno antecedente la data di pubblicazione del bando di gara.
Rispetto al socio unico ed al socio di maggioranza, in caso di società con numero di soci pari o inferiore a quattro, assumono rilevanza sia il socio persona fisica che il socio persona giuridica, pertanto, la ditta concorrente (e/o l'eventuale subappaltatore e/o ausiliaria) deve rendere le dichiarazioni relative all'assenza delle cause di esclusione di cui all'articolo 80, commi 1 e 2, del Codice anche con riferimento ai soggetti sopraindicati.

La domanda e le relative dichiarazioni sono sottoscritte ai sensi del D. Lgs. n.82/2005:

- dal concorrente che partecipa in forma singola;
- nel caso di raggruppamento temporaneo, consorzio ordinario o GEIE costituiti, dalla mandataria/capofila;
- nel caso di raggruppamento temporaneo, consorzio ordinario o GEIE non ancora costituiti, da tutti i soggetti che costituiranno il raggruppamento o consorzio;
- nel caso di aggregazioni di retisti:
  a. **se la rete è dotata di un organo comune con potere di rappresentanza e con soggettività giuridica**, ai sensi dell'articolo 3, comma 4-*quater*, del D.L. 10 febbraio 2009, n. 5, la domanda di partecipazione deve essere sottoscritta dal solo operatore economico che riveste la funzione di organo comune;
  b. **se la rete è dotata di un organo comune con potere di rappresentanza ma è priva di soggettività giuridica**, ai sensi dell'articolo 3, comma 4-*quater*, del D.L. 10 febbraio 2009, n. 5, la domanda di partecipazione deve essere sottoscritta dall'impresa che riveste le funzioni di organo comune nonché da ognuna delle imprese aderenti al contratto di rete che partecipano alla gara;
  c. **se la rete è dotata di un organo comune privo del potere di rappresentanza o se la rete è sprovvista di organo comune, oppure se l'organo comune è privo dei requisiti di qualificazione richiesti per assumere la veste di mandataria**, la domanda di partecipazione deve essere sottoscritta dall'impresa aderente alla rete che riveste la qualifica di mandataria, ovvero, in caso di partecipazione nelle forme del raggruppamento da costituirsi, da ognuna delle imprese aderenti al contratto di rete che partecipa alla gara.
- Nel caso di consorzio di cooperative e imprese artigiane o di consorzio stabile di cui all'articolo 45, comma 2 lett. b) e c) del Codice, la domanda è sottoscritta digitalmente dal consorzio medesimo.

La domanda e le relative dichiarazioni sono firmate dal legale rappresentante del concorrente o da un suo procuratore munito della relativa procura. In tal caso, il concorrente allega alla domanda copia conforme all'originale della procura oppure nel solo caso in cui dalla visura camerale del concorrente risulti l'indicazione espressa dei poteri rappresentativi conferiti con la procura, la

dichiarazione sostitutiva resa dal procuratore attestante la sussistenza dei poteri rappresentativi risultanti dalla visura.

La domanda di partecipazione deve essere presentata nel rispetto di quanto stabilito dal Decreto del Presidente della Repubblica n. 642/72 in ordine all'assolvimento dell'imposta di bollo.

Si precisa che il bollo è dovuto:

- in caso di RTI e consorzi ordinari costituiti/costituendi solo dalla mandataria capogruppo;

- nel caso di consorzi stabili di cui all'art. 45, comma 2 lett. b) e c) del Codice, dal consorzio medesimo;

- nel caso di Aggregazioni di rete dall'organo comune/mandataria.

Il pagamento della suddetta imposta del valore di € **16,00** può essere assolto mediante una delle seguenti modalità:

- applicazione del contrassegno telematico sul Modulo per l'attestazione del Pagamento del bollo, allegato alla documentazione di gara (Allegato 7), avendo cura di indicare, in particolare, il numero identificativo e la data dello stesso;
- virtualmente, previa autorizzazione rilasciata dall'Agenzia delle Entrate al soggetto che ne ha fatto richiesta, avendone i requisiti, ai sensi dell'articolo 15 del DPR 642/72.

I contribuenti non residenti in Italia e non titolari di conti correnti presso banche convenzionate con l'Agenzia delle Entrate e che non possono assolvere l'imposta di bollo utilizzando una delle modalità tradizionali, possono eseguire il versamento mediante bonifico, avendo cura di specificare nella causale il proprio codice fiscale (in mancanza, la denominazione) e gli estremi dell'atto a cui si riferisce l'imposta, seguendo le indicazioni riportate nella risposta a interpello n. 322/2020 dell'Agenzia Entrate, disponibile al seguente link: Schede - Pagamento delle imposte dall'estero - Che cos'è - Agenzia delle Entrate (agenziaentrate.gov.it) Si precisa che, in questo caso, l'operatore economico dovrà allegare alla documentazione la quietanza del bonifico effettuato.

14.2 DOCUMENTO DI GARA UNICO EUROPEO

Il concorrente compila il DGUE presente a sistema su SATER.

Presenta inoltre il DGUE per ciascuna ausiliaria, dal quale risulti il possesso dei requisiti di cui al. paragrafo 6 e compilato per le parti relative ai requisiti oggetto di avvalimento.

Il DGUE presente sul SATER, una volta compilato, dovrà essere scaricato, firmato digitalmente e allegato all'interno della busta "Documentazione amministrativa".

Il DGUE deve essere presentato:

- nel caso di raggruppamenti temporanei, consorzi ordinari, GEIE, da tutti gli operatori economici che partecipano alla procedura in forma congiunta;

- nel caso di aggregazioni di imprese di rete da ognuna delle imprese retiste, se l'intera rete partecipa, ovvero dall'organo comune e dalle singole imprese retiste indicate;
- nel caso di consorzi cooperativi, di consorzi artigiani e di consorzi stabili, dal consorzio e dai consorziati per conto dei quali il consorzio concorre.

14.3 PER GLI OPERATORI ECONOMICI AMMESSI AL CONCORDATO PREVENTIVO CON CONTINUITÀ AZIENDALE DI CUI ALL'ARTICOLO 186 BIS DEL R.D. 16 MARZO 1942, N. 267

Il concorrente, utilizzando il modello Allegato 2a - Schema dichiarazioni concordato preventivo, dichiara, inoltre, ai sensi degli articoli 46 e 47 del decreto del Presidente della Repubblica n. 445/2000 gli estremi del provvedimento di ammissione al concordato e del provvedimento di autorizzazione a partecipare alle gare nonché dichiara di non partecipare alla gara quale mandataria di un raggruppamento temporaneo di imprese e che le altre imprese aderenti al raggruppamento non sono assoggettate ad una procedura concorsuale ai sensi dell'articolo 186 bis, comma 6 del R.D. 16 marzo 1942, n. 267. Il concorrente presenta una relazione di un professionista in possesso dei requisiti di cui all'articolo 67, terzo comma, lettera d), del Regio Decreto 16 marzo 1942, n. 267, che attesta la conformità al piano e la ragionevole capacità di adempimento della Convenzione.

14.4 DOCUMENTAZIONE IN CASO DI AVVALIMENTO

Il concorrente, per ciascuna ausiliaria, allega:

1) il DGUE a firma dell'ausiliaria;

2) la dichiarazione di avvalimento;

3) il contratto di avvalimento;

4) il PASSOE dell'ausiliaria.

14.5 DOCUMENTAZIONE ULTERIORE PER I SOGGETTI ASSOCIATI

Per i raggruppamenti temporanei <u>già</u> costituiti

- copia del mandato collettivo irrevocabile con rappresentanza conferito alla mandataria per atto pubblico o scrittura privata autenticata.
- dichiarazione delle parti del servizio/fornitura, ovvero la percentuale in caso di servizio/forniture indivisibili, che saranno eseguite dai singoli operatori economici riuniti o consorziati.

Per i consorzi ordinari o GEIE già costituiti

- copia dell'atto costitutivo e dello statuto del consorzio o GEIE con indicazione del soggetto designato quale capofila.

- dichiarazione sottoscritta delle parti del servizio/fornitura ovvero la percentuale in caso di servizio/forniture indivisibili, che saranno eseguite dai singoli operatori economici consorziati.

Per i raggruppamenti temporanei o consorzi ordinari o GEIE non ancora costituiti

- dichiarazione resa da ciascun concorrente attestante:
  a. l'operatore economico al quale, in caso di aggiudicazione, sarà conferito mandato speciale con rappresentanza o funzioni di capogruppo;
  b. l'impegno, in caso di aggiudicazione, ad uniformarsi alla disciplina vigente con riguardo ai raggruppamenti temporanei o consorzi o GEIE ai sensi dell'articolo 48, comma 8, del Codice conferendo mandato collettivo speciale con rappresentanza all'impresa qualificata come mandataria che stipulerà la Convenzione in nome e per conto delle mandanti/consorziate;
  c. le parti del servizio/fornitura, ovvero la percentuale in caso di servizio/forniture indivisibili, che saranno eseguite dai singoli operatori economici riuniti o consorziati.

Per le aggregazioni di imprese aderenti al contratto di rete: se la rete è dotata di un organo comune con potere di rappresentanza e soggettività giuridica

- copia del contratto di rete con indicazione dell'organo comune che agisce in rappresentanza della rete;
- dichiarazione che indichi per quali imprese la rete concorre;
- dichiarazione sottoscritta con firma digitale che indichi le parti del servizio o della fornitura, ovvero la percentuale in caso di servizio/forniture indivisibili, che saranno eseguite dai singoli operatori economici aggregati in rete.

Per le aggregazioni di imprese aderenti al contratto di rete: se la rete è dotata di un organo comune con potere di rappresentanza ma è priva di soggettività giuridica

- copia del contratto di rete;
- copia del mandato collettivo irrevocabile con rappresentanza conferito all'organo comune;
- dichiarazione che indichi le parti del servizio o della fornitura, ovvero la percentuale in caso di servizio/forniture indivisibili, che saranno eseguite dai singoli operatori economici aggregati in rete.

Per le aggregazioni di imprese aderenti al contratto di rete: se la rete è dotata di un organo comune privo del potere di rappresentanza o se la rete è sprovvista di organo comune, ovvero, se l'organo comune è privo dei requisiti di qualificazione richiesti, partecipa nelle forme del RTI costituito o costituendo:

in caso di RTI costituito

- copia del contratto di rete;
- copia del mandato collettivo irrevocabile con rappresentanza conferito alla mandataria;

- dichiarazione delle parti del servizio o della fornitura, ovvero la percentuale in caso di servizio/forniture indivisibili, che saranno eseguite dai singoli operatori economici aggregati in rete.

in caso di RTI costituendo:

- copia del contratto di rete;
- dichiarazioni, rese da ciascun concorrente aderente all'aggregazione di rete, attestanti:
  a. a quale concorrente, in caso di aggiudicazione, sarà conferito mandato speciale con rappresentanza o funzioni di capogruppo;
  b. l'impegno, in caso di aggiudicazione, ad uniformarsi alla disciplina vigente in materia di raggruppamenti temporanei;
  c. le parti del servizio o della fornitura, ovvero la percentuale in caso di servizio/forniture indivisibili, che saranno eseguite dai singoli operatori economici aggregati in rete.

15. CONTENUTO DELLA BUSTA "OFFERTA TECNICA"

La busta "Offerta tecnica" contiene, **a pena di esclusione**, per ciascun lotto, i seguenti documenti, da allegare su SATER secondo le modalità esplicitate nelle guide per l'utilizzo della piattaforma SATER accessibili dal sito http://intercenter.regione.emilia-romagna.it/help/guide:

a) **Relazione tecnica dei servizi offerti** (vedi lo "Schema di offerta tecnica", per il Lotto 1 l'all. 4a e per il Lotto 2 l'all.4b);

b) Compilazione esclusivamente sul sistema SATER dei valori offerti per i **criteri di valutazione tabellari "T"**, più precisamente per i criteri di valutazione riferiti agli SLA migliorativi nn. 9,10,11, 12 e 13 del Lotto 1 e per i criteri di valutazione nn.11, 12 e 13 del Lotto 2, selezionando per ciascun criterio, nella rispettiva colonna uno tra i valori presenti nel relativo menù a tendina.

c) Eventuali Segreti tecnici e commerciali come esplicitato nel paragrafo seguente.

All'offerta deve essere allegato un indice riepilogativo degli elaborati.

La Relazione contiene una proposta tecnico-organizzativa che illustra, con particolare riferimento ai criteri di valutazione indicati nella tabella di cui al successivo punto 17.1, tutti gli elementi evidenziati nel relativo Schema di offerta tecnica (Allegati 4a e 4b), cui si rinvia.

L'offerta tecnica deve rispettare le caratteristiche minime stabilite nel Progetto e nella documentazione di gara, **pena l'esclusione** dalla procedura di gara, nel rispetto del principio di equivalenza di cui all'articolo 68 del Codice.

La commissione giudicatrice potrà invitare i concorrenti a fornire chiarimenti/integrazioni in ordine ai documenti e alle dichiarazioni presentate nell'ambito della documentazione tecnica. La carenza

sostanziale della documentazione tecnica complessivamente presentata dalle concorrenti, tale da non consentire la valutazione di quanto offerto da parte della commissione giudicatrice, comporta l'esclusione dalla gara.

La documentazione tecnica deve essere priva, a pena di esclusione, di qualsivoglia indicazione (diretta e/o indiretta) all'offerta economica.

15.1 SEGRETI TECNICI E COMMERCIALI

Il concorrente deve dichiarare quali informazioni fornite, inerenti l'offerta presentata, costituiscano segreti tecnici e commerciali, pertanto coperte da riservatezza.

In base a quanto disposto dall'articolo 53, comma 5, del Codice, il diritto di accesso agli atti e ogni forma di divulgazione sono esclusi in relazione alle informazioni fornite dai concorrenti nell'ambito delle offerte che costituiscono, secondo motivata e comprovata dichiarazione del concorrente, segreti tecnici e commerciali.

A tal proposito si chiarisce che i segreti industriali e commerciali non devono essere semplicemente asseriti, ma devono essere effettivamente sussistenti e di ciò deve essere dato un principio di prova da parte del concorrente.

La ditta concorrente deve quindi allegare su SATER una dichiarazione in formato elettronico, firmata digitalmente e denominata "Segreti tecnici e commerciali", nella sezione "Offerta tecnica", contenente i dettagli dell'offerta coperti da riservatezza, accompagnata da idonea documentazione che:

- argomenti in modo approfondito e congruo le ragioni per le quali eventuali parti dell'offerta sono da segretare;
- fornisca un "principio di prova" atto a dimostrare la tangibile sussistenza di eventuali segreti tecnici e commerciali.

L'Agenzia si riserva comunque di valutare la compatibilità dell'istanza di riservatezza con il diritto di accesso dei soggetti interessati.

L'Agenzia di riserva di imporre alle ditte concorrenti condizioni intese a proteggere il carattere di riservatezza delle informazioni rese disponibili.

Si precisa che l'Agenzia non effettuerà ulteriori informative e procederà, su richiesta scritta del concorrente entro 15 (quindici) giorni a comunicare quanto previsto dall'articolo 76, comma 2, del Codice (fermo restando quanto previsto dal comma 4 del medesimo articolo).

16. CONTENUTO DELLA BUSTA "OFFERTA ECONOMICA"

La busta "Offerta economica" contiene l'offerta economica, ed è predisposta su SATER secondo le modalità esplicitate nelle guide per l'utilizzo della piattaforma SATER accessibili dal sito http://intercenter.regione.emilia-romagna.it/help/guide.

L'offerta economica, firmata secondo le modalità di cui al precedente paragrafo 12 deve indicare **a pena di esclusione** i seguenti elementi:

a) **Il corrispettivo/prezzo unitario offerto** per l'unità di misura indicata (**prezzo offerto per UM, IVA esclusa**) al netto di Iva e/o di altre imposte e contributi di legge nonché degli oneri per la sicurezza dovuti a rischi da interferenze.

Verranno prese in considerazione fino a 2 (due) cifre decimali.

Ciascun concorrente visualizzerà tante righe quanti sono i servizi a canone o le figure professionali a giornata/uomo cui deve obbligatoriamente associare un valore (prezzo unitario offerto per UM, IVA esclusa) a fronte dei quantitativi specificati.

Il Valore complessivo dell'offerta è calcolato automaticamente dal SATER moltiplicando i ("P") (prezzi offerti per UM, IVA esclusa) per le Quantità (Q) indicate a sistema **(PXQ)**; esso sarà espresso con un numero di decimali non superiore a due (2) e non potrà superare il valore a base d'asta, **pena l'esclusione.**

La ditta concorrente deve compilare *on line* l'offerta economica per il Lotto a cui partecipa sul sistema SATER.

Le offerte sono sintetizzate nelle seguenti tabelle, rispettivamente per il Lotto 1 ed il Lotto 2 e riportate integralmente per entrambi i lotti nell'allegato 5:

Lotto 1

Macro Categoria	Modalità di erogazione/remunerazione	Il canone annuo corrisponde al prezzo per
Servizio di monitoraggio NOC	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi e Apparati di rete;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi mail server;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi DB server;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi Web server;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi Back office;	Canone annuo	Server/Appliance (virtuale o fisico)

Sistemi Storage backup;	Canone annuo	Server/Appliance (virtuale o fisico)
Figure Professionali:		
TEM - ICT Operation Manager;	GG/uomo	
CET - Enterprise Architect;	GG/uomo	
SPP - System Architect;	GG/uomo	
SIS - System Administrator Senior;	GG/uomo	
SIM - System Administrator Middle;	GG/uomo	
SIJ - System Administrator Junior;	GG/uomo	
DBS - Database Administrator Senior;	GG/uomo	
DBJ - Database Administrator Junior;	GG/uomo	
SRS - Network Specialist Senior;	GG/uomo	
SRJ - Network Specialist Junior.	GG/uomo	

Lotto 2

Macro Categoria	Modalità di erogazione/remunerazione	Il canone annuo corrisponde al prezzo per
Servizio di monitoraggio SOC	Canone annuo	FASCIA DI EPS
Sistemi Firewall, IDS,IPS	Canone annuo	PIATTAFORMA
Sistemi Antivirus e di telemetria xDR/EDR/NDR	Canone annuo	PIATTAFORMA
Sistemi WAF,	Canone annuo	PIATTAFORMA
Sistemi SIEM, SOAR,	Canone annuo	PIATTAFORMA
Servizio di Incident response & remediation		ENTE
Servizio di threat intelligence / APT-feed / asset tracker & data leak	Canone annuo	DOMINIO
Servizio di User and entity behavior analytics (UEBA)	Canone annuo	UTENTE
Servizio di host hardening	Canone annuo	DEVICE MODEL
Servizio di security awareness	Canone annuo	UTENTE
Servizio di Vulnerability Management	Canone annuo	IP
Servizio di Application Security Testing	Canone annuo	APPLICAZIONE
Figure Professionali:		
Security Project Manager	GG/uomo	
Governance & risk compliance (GRC) consultant	GG/uomo	
Security architect & engineer	GG/uomo	
Security Advisor senior	GG/uomo	
Security Advisor junior	GG/uomo	

Security specialist	GG/uomo	
Security specialist con reperibilità H24	GG/uomo	
Security Analyst senior	GG/uomo	
Security Analyst junior	GG/uomo	
Vulnerability researcher / Ethical Hacker senior	GG/uomo	
Vulnerability researcher / Ethical Hacker junior	GG/uomo	
Incident handler / response senior	GG/uomo	
Incident handler / response junior	GG/uomo	
Digital forensic	GG/uomo	
CyberSecurity & Privacy Legal Advisor	GG/uomo	

L'offerta economica viene poi perfezionata scaricando il documento generato da SATER che dovrà essere firmato digitalmente dal legale rappresentante e ricaricato a Sistema (come indicato nelle guide per l'utilizzo della piattaforma di cui sopra).

Si precisa che:

- Il prezzo unitario offerto non può essere pari a 0 (zero);
- Il valore complessivo offerto per ciascun lotto di partecipazione è calcolato automaticamente da SATER;
- I quantitativi triennali (Q) indicati nell'offerta economica (vedi all.5) hanno valore indicativo e concorrono unicamente alla determinazione del valore complessivo dell'offerta.

Sono inammissibili le offerte economiche che superino l'importo a base d'asta per ciascun lotto.

Con la presentazione dell'offerta, in caso di aggiudicazione, il concorrente si obbliga irrevocabilmente nei confronti del committente ad eseguire i servizi in conformità a quanto indicato nell'Offerta tecnica e nell'Offerta economica. Gli oneri fiscali sono in conformità alle leggi vigenti.

17. CRITERIO DI AGGIUDICAZIONE

L'appalto è aggiudicato in base al criterio dell'offerta economicamente più vantaggiosa individuata sulla base del miglior rapporto qualità/prezzo, ai sensi dell'articolo 95, comma 2, del Codice.

La valutazione dell'offerta tecnica e dell'offerta economica sarà effettuata in base ai seguenti punteggi.

	PUNTEGGIO MASSIMO
Offerta tecnica	*80*
Offerta economica	*20*
TOTALE	**100**

17.1 CRITERI DI VALUTAZIONE DELL'OFFERTA TECNICA

Il punteggio dell'offerta tecnica è attribuito sulla base dei criteri di valutazione elencati nella sottostante tabella con la relativa ripartizione dei punteggi.

Nella colonna identificata con la lettera **D** vengono indicati i "Punteggi discrezionali", vale a dire i punteggi il cui coefficiente è attribuito in ragione dell'esercizio della discrezionalità spettante alla commissione giudicatrice.

Nella colonna identificata dalla lettera **T** vengono indicati i "Punteggi tabellari", vale a dire i punteggi fissi e predefiniti che saranno attribuiti o non attribuiti in ragione dell'offerta o mancata offerta di quanto specificamente richiesto.

Tabella dei criteri discrezionali (D) e tabellari (T) di valutazione dell'offerta tecnica

LOTTO 1

N°	CRITERI DI VALUTAZIONE	MODALITA' DI ATTRIBUZIONE DEL PUNTEGGIO	PUNTI **D** MAX	PUNTI **T** MAX
1	Organizzazione e suddivisione attività.	Vedi tabella riportata al par.17.2	8	
2	Gestione dell'infrastruttura NOC.	Vedi tabella riportata al par.17.2	6	
3	Flessibilità.	Vedi tabella riportata al par.17.2	6	
4	Metodologia e modalità operative adottate.	Vedi tabella riportata al par.17.2	6	
5	Protezione dei servizi IT, salvaguardia dati/informazioni, ottimizzazione dei processi critici.	Vedi tabella riportata al par.17.2	6	
6	Gestione delle chiamate di supporto.	Vedi tabella riportata al par.17.2	6	
7	Centri di competenza offerti.	Vedi tabella riportata al par.17.2	6	
8	Formazione risorse professionali impiegate	Vedi tabella riportata al par.17.2	6	
9	Migliorie degli SLA -Gestione Sistemi, Rete e NOC: Tempo di presa in carico	Saranno attribuiti due punti fino ad un max di 6 per la riduzione delle tempistiche di risoluzione richieste in Capitolato (Tabelle 2 e 3 del Capitolato) rispetto a tutti e		6

N°	CRITERI DI VALUTAZIONE	MODALITA' DI ATTRIBUZIONE DEL PUNTEGGIO	PUNTI **D** MAX	PUNTI **T** MAX
		tre i livelli di criticità, come segue: • meno 10%: 2 punti • meno 20%: 4 punti • meno 30%: 6 punti		
10	Migliorie degli SLA -Gestione Sistemi, Rete: Tempo di risoluzione Malfunzionamento	SLA migliorativo: Saranno attribuiti due punti fino ad un max di 6 per la riduzione delle tempistiche di risoluzione richieste in Capitolato (Tabella 2 del Capitolato) rispetto a tutti e tre i livelli di criticità, come segue: • meno 10%: 2 punti • meno 20%: 4 punti • meno 30%: 6 punti		6
11	Migliorie degli SLA - NOC: Tempo di risoluzione del malfunzionamento	Saranno attribuiti due punti fino ad un max di 6 per la riduzione delle tempistiche di risoluzione richieste in Capitolato (Tabella 3 del Capitolato) rispetto a tutti e tre i livelli di criticità, come segue: • meno 10%: 2 punti • meno 20%: 4 punti • meno 30%: 6 punti		6
12	Migliorie degli SLA -Richieste al Service Desk sistemistico: Tempo di gestione richieste service desk	Saranno attribuiti due punti fino ad un max di 6 per la riduzione delle tempistiche di risoluzione richieste in Capitolato (Tabella 4 del Capitolato) rispetto a tutti e tre i livelli di criticità, come segue: • meno 10%: 2 punti • meno 20%: 4 punti • meno 30%: 6 punti		6
13	Migliorie degli SLA - Richieste al Service Desk sistemistico: Tasso di risoluzione ticket al service desk	SLA migliorativo: Saranno attribuiti due punti fino ad un max di 6 per l'aumento del tasso di risoluzione del ticket come richiesto in Capitolato (Tabella 4 del Capitolato) rispetto a tutti e tre i livelli di criticità, come segue: • aumento dal 50% al 60%: 2 punti		6

N°	CRITERI DI VALUTAZIONE	MODALITA' DI ATTRIBUZIONE DEL PUNTEGGIO	PUNTI **D** MAX	PUNTI **T** MAX
		• aumento dal 60% al 70%: 4 punti • aumento dal 70% all'80%: 6 punti		
	Totale per tipo di criterio		**50**	**30**
Totale complessivo (D+T) = 80 punti				

LOTTO 2

N°	CRITERI DI VALUTAZIONE	MODALITA' DI ATTRIBUZIONE DEL PUNTEGGIO	PUNTI **D** MAX	PUNTI **T** MAX
1	Organizzazione e suddivisione attività.	Vedi tabella riportata al par.17.2	8	
2	Servizi di monitoraggio della sicurezza - SOC	Vedi tabella riportata al par.17.2	8	
3	Conduzione Operativa e ServiceDesk Sistemistico di Sicurezza Informatica	Vedi tabella riportata al par.17.2	8	
4	Modalità di pianificazione ed erogazione dei Servizi di VA periodico e continuativo	Vedi tabella riportata al par.17.2	6	
5	Penetration test (PT) e Controllo del codice (AST)	Vedi tabella riportata al par.17.2	6	
6	Threat Intelligence e Security Advisory	Vedi tabella riportata al par.17.2	6	
7	Servizio UEBA	Vedi tabella riportata al par.17.2	4	
8	Servizi di Incident Response & Remediation, Digital Forensic	Vedi tabella riportata al par.17.2	8	
9	Progetto di sistema specialistico in merito alla Security Awareness	Vedi tabella riportata al par.17.2	4	
10	Figure professionali, disponibilità e aggiornamento delle risorse	Vedi tabella riportata al par.17.2	4	
11	Migliorie degli SLA -Servizi di Gestione Sistemi e apparati di sicurezza, SOC e Incident Response: Presa in carico di un alert	Sarà attribuito un punto fino ad un max di 6 per la riduzione delle tempistiche di risoluzione richieste in Capitolato (Tabelle SLA 5, 6 e 7) rispetto a tutti e tre i livelli di severità, come segue: • meno 10%: 2 punto • meno 20%: 4 punti • meno 30%: 6 punti		6

N°	CRITERI DI VALUTAZIONE	MODALITA' DI ATTRIBUZIONE DEL PUNTEGGIO	PUNTI **D** MAX	PUNTI **T** MAX
12	Migliorie degli SLA - Gestione Apparati e Sistemi di Sicurezza: Tempistiche di risoluzione del malfunzionamento	Sarà attribuito un punto fino ad un max di 6 per la riduzione delle tempistiche di risoluzione richieste in Capitolato (Tabella 5) rispetto a tutti e tre i livelli di severità, come segue: • meno 10%: 2 punto • meno 20%: 4 punti • meno 30%: 6 punti		6
13	Migliorie SLA - Servizi SOC e di Incident Response & Remediation: Azioni da intraprendere, convalida e risoluzione	Sarà attribuito un punto fino ad un max di 6 per la riduzione delle tempistiche di risoluzione richieste in Capitolato (Tabelle 6 e 7) rispetto a tutti e tre i livelli di severità, come segue: • meno 10%: 2 punti • meno 20%: 4 punti • meno 30%: 6 punti		6
	Totale per tipo di criterio		**62**	**18**
Totale complessivo (D+T) = 80 punti				

17.2 METODO DI ATTRIBUZIONE DEL COEFFICIENTE PER IL CALCOLO DEL PUNTEGGIO DELL'OFFERTA TECNICA

A ciascuno degli elementi qualitativi cui è assegnato un punteggio discrezionale nella colonna "D" della tabella, per la determinazione del coefficiente Cai variabile da zero a uno, la commissione calcola la media aritmetica dei coefficienti attribuiti dai singoli commissari a ciascun elemento qualitativo dell'offerta secondo la seguente scala:

Giudizio	**Ottimo**	**Più che adeguato**	**Adeguato**	**Parzialmente adeguato**	**Scarsamente adeguato**	**Non adeguato**
Coefficiente Cai assegnato	1,00	0,80	0,60	0,40	0,20	0,00

Il punteggio assegnato agli elementi indicati come tabellari "T" viene attribuito automaticamente in valore assoluto, sulla base della presenza o assenza nell'offerta, dell'elemento richiesto o della sua differente valorizzazione.

Si precisa che sia per i criteri nn. 9, 10, 11, 12 e 13 della colonna "T" del Lotto 1, che per i criteri nn. 11, 12 e 13 della colonna "T" del Lotto 2, l'operatore economico deve valorizzare i relativi campi sulla piattaforma SATER.

17.3 METODO DI ATTRIBUZIONE DEL COEFFICIENTE PER IL CALCOLO DEL PUNTEGGIO DELL'OFFERTA ECONOMICA

Quanto all'offerta economica, è attribuito all'elemento economico un coefficiente, variabile da zero ad uno, calcolato tramite la seguente formula*:*

Formula del "ribasso massimo non lineare"

$$C_i = (R_a/R_{max})^{\alpha}$$

dove:

C_i *= coefficiente attribuito al concorrente i-esimo;*

R_a *= ribasso dell'offerta del concorrente i-esimo;*

R_{max} *= ribasso dell'offerta più conveniente.*

$\alpha = 0{,}50$

17.4 METODO PER IL CALCOLO DEI PUNTEGGI

La commissione, terminata l'attribuzione dei coefficienti agli elementi qualitativi e quantitativi, procederà, in relazione a ciascuna offerta, all'attribuzione dei punteggi per ogni singolo criterio secondo il metodo aggregativo compensatore.

Il punteggio è dato dalla seguente formula:

$$P_i = C_{ai} \times P_a + C_{bi} \times P_b + \ldots\ldots C_{ni} \times P_n$$

dove

Pi = *punteggio concorrente i;*

Cai = *coefficiente criterio di valutazione a, del concorrente i;*

Cbi = *coefficiente criterio di valutazione b, del concorrente i;*

.....

Cni = *coefficiente criterio di valutazione n, del concorrente i;*

Pa = *peso criterio di valutazione a;*

Pb = *peso criterio di valutazione b;*

.....

Pn = *peso criterio di valutazione n.*

Al risultato della suddetta operazione verranno sommati eventuali punteggi tabellari, già espressi in valore assoluto, ottenuti dall'offerta del singolo concorrente.

18. COMMISSIONE GIUDICATRICE

La commissione giudicatrice è nominata dopo la scadenza del termine per la presentazione delle offerte ed è composta da un numero dispari pari a n. 3 membri, esperti nello specifico settore cui si riferisce l'oggetto della Convenzione. In capo ai commissari non devono sussistere cause ostative alla nomina ai sensi dell'articolo 77, comma 4,5 e 6 del Codice. A tal fine i medesimi rilasciano prima del conferimento dell'incarico apposita dichiarazione all'Agenzia.

La commissione giudicatrice è responsabile della valutazione delle offerte tecniche ed economiche dei concorrenti e, di regola, lavora a distanza con procedure telematiche che salvaguardino la riservatezza delle comunicazioni.

L'Agenzia pubblica, sul profilo di committente, nella pagina informativa dedicata alla presente procedura, e nella sezione Amministrazione trasparente, la composizione della commissione giudicatrice e i curricula dei componenti.

Il RUP si avvale dell'ausilio della commissione giudicatrice ai fini della verifica dell'anomalia delle offerte.

19. SVOLGIMENTO OPERAZIONI DI GARA

La prima seduta avrà luogo il giorno **05/07/2023**, alle ore **10:00.**

La presente vale quindi anche come convocazione a detta seduta che avverrà esclusivamente in modalità telematica e alla quale le ditte interessate potranno partecipare collegandosi a SATER nelle modalità di cui sopra.

Tale seduta, se necessario, sarà aggiornata ad altra ora o a giorni successivi, nella data e negli orari che saranno comunicati ai concorrenti tramite SATER.

Parimenti le successive sedute saranno comunicate ai concorrenti mediante SATER almeno **2** giorni prima della data fissata.

La piattaforma SATER consente la pubblicità delle sedute di gara preordinate all'apertura:

- della documentazione amministrativa;
- delle offerte tecniche;
- delle offerte economiche;

e la riservatezza delle sedute che non sono pubbliche. La pubblicità delle sedute è garantita mediante collegamento dei concorrenti da remoto per consentire a ciascun soggetto interessato di visualizzare le operazioni della seduta, secondo le modalità esplicitate nelle guide per l'utilizzo della piattaforma SATER, accessibili dal sito http://intercenter.regione.emilia-romagna.it/help/guide/.

20. VERIFICA DOCUMENTAZIONE AMMINISTRATIVA

Nella prima seduta il seggio di gara accede alla documentazione amministrativa di ciascun concorrente, mentre l'offerta tecnica e l'offerta economica restano, chiuse, segrete e bloccate dal sistema, e procede a:

a) controllare la completezza della documentazione amministrativa presentata;
b) verificare la conformità della documentazione amministrativa a quanto richiesto nel presente disciplinare;
c) redigere apposito verbale relativo alle attività svolte;

Ad esito delle verifiche di cui sopra il RUP provvede a:

a) attivare la procedura di soccorso istruttorio di cui al precedente punto 13
b) redigere e adottare il provvedimento che determina le esclusioni e le ammissioni dalla procedura di gara, laddove necessario, provvedendo altresì alla sua pubblicazione sul sito della Agenzia, nella pagina informativa dedicata alla presente procedura, e nella sezione Amministrazione trasparente e alla sua comunicazione ai concorrenti immediata e comunque entro un termine non superiore a cinque giorni, a mezzo PEC all'indirizzo comunicato in fase di registrazione al SATER.

L'Agenzia si riserva di chiedere agli offerenti, in qualsiasi momento nel corso della procedura, di presentare tutti i documenti complementari o parte di essi, qualora questo sia necessario per assicurare il corretto svolgimento della procedura.

La prosecuzione della procedura è limitata ai soli concorrenti ammessi.

21. APERTURA E VALUTAZIONE DELLE OFFERTE TECNICHE ED ECONOMICHE

La data e l'ora della seduta pubblica in cui si procede all'apertura delle offerte tecniche sono comunicate tramite SATER ai concorrenti ammessi ai sensi dell'articolo 20.

La commissione giudicatrice procede [all'apertura, esame e valutazione delle offerte presentate dai predetti concorrenti e all'assegnazione dei relativi punteggi applicando i criteri e le formule indicati nel bando e nel presente Disciplinare. Gli esiti della valutazione sono registrati da SATER.

La commissione giudicatrice rende visibile ai concorrenti, con le modalità di cui all'articolo 19:

a) i punteggi tecnici attribuiti alle singole offerte tecniche;

b) le eventuali esclusioni dalla gara dei concorrenti.

SATER consente la prosecuzione della procedura ai soli concorrenti ammessi alla valutazione delle offerte economiche.

La commissione giudicatrice all'apertura delle offerte economiche e, quindi, alla valutazione delle offerte economiche, secondo i criteri e le modalità descritte al punto 17 e successivamente

all'individuazione dell'unico parametro numerico finale per la formulazione della graduatoria.

Nel caso in cui le offerte di due o più concorrenti ottengano lo stesso punteggio complessivo, ma punteggi differenti per il prezzo e per tutti gli altri elementi di valutazione è collocato primo in graduatoria il concorrente che ha ottenuto il miglior punteggio sull' offerta tecnica.

Nel caso in cui le offerte di due o più concorrenti ottengano lo stesso punteggio complessivo e gli stessi punteggi parziali per il prezzo e per l'offerta tecnica, i predetti concorrenti, su richiesta dell'Agenzia, presentano un'offerta migliorativa sul prezzo entro **dieci giorni** dall'invito. La richiesta è effettuata secondo le modalità previste all'articolo 2.3. È collocato primo in graduatoria il concorrente che ha presentato la migliore offerta. Ove permanga l'*ex aequo* la commissione procede mediante sorteggio ad individuare il concorrente che verrà collocato primo nella graduatoria. L'Agenzia comunica il giorno e l'ora del sorteggio, secondo le modalità previste all'articolo 2.3.

La Commissione giudicatrice rende visibile ai concorrenti, con le modalità di cui all'articolo 19 i prezzi offerti.

All'esito delle operazioni di cui sopra, la commissione, redige la graduatoria e comunica la proposta di aggiudicazione al RUP.

Qualora individui offerte che superano la soglia di anomalia di cui all'articolo 97, comma 3 del Codice, e in ogni altro caso in cui, in base a elementi specifici, l'offerta appaia anormalmente bassa, la commissione, chiude la seduta dando comunicazione al RUP, che procede alla verifica dell'anomalia.

In qualsiasi fase delle operazioni di valutazione delle offerte tecniche ed economiche, la commissione provvede a comunicare, tempestivamente al RUP i casi di esclusione da disporre per:

- mancata separazione dell'offerta economica dall'offerta tecnica, ovvero inserimento di elementi concernenti il prezzo nella documentazione amministrativa o nell'offerta tecnica;
- presentazione di offerte parziali, plurime, condizionate, alternative oppure irregolari in quanto non rispettano i documenti di gara, ivi comprese le specifiche tecniche, o anormalmente basse;
- presentazione di offerte inammissibili in quanto la commissione giudicatrice ha ritenuto sussistenti gli estremi per l'informativa alla Procura della Repubblica per reati di corruzione o fenomeni collusivi o ha verificato essere in aumento rispetto all'importo a base di gara;

22. VERIFICA DI ANOMALIA DELLE OFFERTE

Al ricorrere dei presupposti di cui all'articolo 97, comma 3, del Codice, e in ogni altro caso in cui, in base a elementi specifici, l'offerta appaia anormalmente bassa, il RUP [avvalendosi della commissione giudicatrice, se ritenuto necessario] valuta la congruità, serietà, sostenibilità e realizzabilità delle offerte che appaiono anormalmente basse.

Si procede a verificare la prima migliore offerta anormalmente bassa. Qualora tale offerta risulti anomala, si procede con le stesse modalità nei confronti delle successive offerte, fino ad individuare la migliore offerta ritenuta non anomala.

Il RUP richiede per iscritto al concorrente la presentazione, per iscritto, delle spiegazioni, se del caso indicando le componenti specifiche dell'offerta ritenute anomale.

A tal fine, assegna un termine non inferiore a quindici giorni dal ricevimento della richiesta.

Il RUP esaminate le spiegazioni fornite dall'offerente e, ove le ritenga non sufficienti ad escludere l'anomalia, può chiedere, anche mediante audizione orale, ulteriori chiarimenti, assegnando un termine perentorio per il riscontro.

Il RUP esclude le offerte che, in base all'esame degli elementi forniti con le spiegazioni risultino, nel complesso, inaffidabili.

23. AGGIUDICAZIONE E STIPULA DELLA CONVENZIONE

La commissione invia al RUP la proposta di aggiudicazione in favore del concorrente che ha presentato la migliore offerta.

Qualora vi sia stata verifica di congruità delle offerte anomale la proposta di aggiudicazione è formulata dal RUP al termine del relativo procedimento.

Qualora nessuna offerta risulti conveniente o idonea in relazione all'oggetto della Convenzione quadro, l'Agenzia si riserva la facoltà di non procedere all'aggiudicazione.

L'aggiudicazione diventa efficace all'esito positivo della verifica del possesso dei requisiti prescritti dal presente Disciplinare.

In caso di esito negativo delle verifiche, l'Agenzia procederà alla revoca dell'aggiudicazione, alla segnalazione all'ANAC nonché all'incameramento della garanzia provvisoria. L'Agenzia aggiudicherà, quindi, al secondo graduato procedendo altresì, alle verifiche nei termini sopra indicati.

Nell'ipotesi in cui la Convenzione quadro non possa essere aggiudicata neppure a favore del concorrente collocato al secondo posto nella graduatoria, la Convenzione verrà aggiudicata, nei termini sopra detti, scorrendo la graduatoria.

Qualora l'Agenzia autorizzi l'esecuzione della Convenzione/Accordo in via d'urgenza ai sensi dell'articolo 32, comma 8, del Codice, l'aggiudicatario/i si impegna/no a darne esecuzione nelle more delle verifiche di legge e degli adempimenti finalizzati alla stipula.

La comunicazione di avvenuta stipulazione della Convenzione si intende attuata, ad ogni effetto di legge, con la pubblicazione della medesima sul sito http://intercenter.regione.emilia-romagna.it/.

La stipula avrà luogo entro **60** giorni dall'intervenuta efficacia dell'aggiudicazione salvo il differimento espressamente concordato con l'aggiudicatario.

A seguito di richiesta motivata proveniente dall'aggiudicatario la data di stipula del contratto può essere differita purché ritenuta compatibile con la sollecita esecuzione del contratto stesso.

La garanzia provvisoria verrà svincolata all'aggiudicatario automaticamente al momento della stipula della Convenzione; agli altri concorrenti verrà svincolata tempestivamente e comunque entro trenta giorni dalla comunicazione dell'avvenuta aggiudicazione.

La Convenzione non potrà essere stipulata prima di **35** giorni dall'invio dell'ultima delle comunicazioni del provvedimento di aggiudicazione.

All'atto della stipulazione della Convenzione, l'aggiudicatario deve presentare la garanzia definitiva da calcolare sull'importo contrattuale, secondo le misure e le modalità previste dall'articolo 103 del Codice.

Il mancato invio/la mancata presentazione di quanto necessario ai fini della stipula sarà causa di revoca dell'aggiudicazione.

La Convenzione sarà stipulata in modalità elettronica, mediante scrittura privata.

La Convenzione è soggetta agli obblighi in tema di tracciabilità dei flussi finanziari di cui alla l. 13 agosto 2010, n. 136.

L'esito positivo degli accertamenti d'ufficio nonché la ricezione della documentazione richiesta nel termine fissato è condizione essenziale per la stipula della Convenzione. Nei casi di cui all'articolo 110, comma 1, del Codice l'Agenzia interpella progressivamente i soggetti che hanno partecipato alla procedura di gara, risultanti dalla relativa graduatoria, al fine di stipulare una nuova Convenzione quadro per l'affidamento dell'esecuzione o del completamento del servizio.

Le spese relative alla pubblicazione del bando e dell'avviso sui risultati della procedura di affidamento sono a carico dell'aggiudicatario e dovranno essere rimborsate all'Agenzia entro il termine di sessanta giorni dall'aggiudicazione.

L'importo presunto delle spese di pubblicazione è pari a € 6.500,00. L'Agenzia comunicherà all'aggiudicatario l'importo effettivo delle suddette spese, nonché le relative modalità di pagamento.

L'importo verrà pubblicato altresì sul sito http://intercenter.regione.emilia-romagna.it/, nella pagina informativa dedicata alla presente procedura.

Sono a carico dell'aggiudicatario anche tutte le spese contrattuali, gli oneri fiscali quali imposte e tasse - ivi comprese quelle di registro ove dovute - relative alla stipulazione della Convenzione.

L'affidatario, almeno venti giorni prima dell'inizio dell'esecuzione delle attività, deve depositare presso l'Agenzia il contratto di subappalto, inviandone copia anche alla Amministrazione contraente. Ai sensi dell'articolo 105, comma 2, del Codice l'affidatario comunica alla Agenzia e, per conoscenza, all'Amministrazione contraente, per ogni sub-contratto che non costituisce subappalto, l'importo e l'oggetto del medesimo, nonché il nome del sub-contraente, prima dell'inizio della prestazione.

L'affidatario deposita, prima o contestualmente alla sottoscrizione della Convenzione, i contratti continuativi di cooperazione, servizio e/o fornitura di cui all'articolo 105, comma 3, lett. c-bis) del Codice.

L'aggiudicatario è altresì tenuto ad effettuare tutte le operazioni necessarie, ad esso richieste dall'Agenzia, al fine della predisposizione del negozio elettronico, attraverso il quale le Amministrazioni contraenti procederanno ad emettere gli Ordinativi di fornitura.

24. CODICE DI COMPORTAMENTO

Nello svolgimento delle attività oggetto della Convenzione, l'aggiudicatario di ciascun lotto deve uniformarsi ai principi e, per quanto compatibili, ai doveri di condotta richiamati nel Decreto del Presidente della Repubblica 16 aprile 2013 n. 62, e nel codice di comportamento della Regione Emilia-Romagna approvato con Delibera di Giunta n. 905/2018 nel Piano Triennale di Prevenzione della Corruzione e della Trasparenza.

In seguito alla comunicazione di aggiudicazione e prima della stipula della Convenzione, l'aggiudicatario ha l'onere di prendere visione dei documenti pubblicati sul sito dell'Agenzia al link: https://intercenter.regione.emilia-romagna.it/agenzia/prevenzione-della-corruzione.

25. FORMAZIONE

Entro il medesimo termine previsto per la sottoscrizione della Convenzione, l'aggiudicatario di ciascun lotto è tenuto a formarsi adeguatamente attraverso gli strumenti messi a disposizione dall'Agenzia, tra cui sessioni frontali, streaming, specifici manuali pubblicati sul sito e call center, al fine di conoscere gli elementi necessari per l'utilizzo corretto del SATER per quanto attiene alle specifiche funzionalità di pertinenza: stipula della Convenzione, compilazione listini, gestioni ordinativi, etc.

26. DEFINIZIONE DELLE CONTROVERSIE

Per le controversie derivanti dalla Convenzione è competente il Foro di Bologna, rimanendo espressamente esclusa la compromissione in arbitri.

27. TRATTAMENTO DEI DATI PERSONALI

I dati raccolti sono trattati e conservati ai sensi del Regolamento UE n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, del decreto legislativo 30 giugno 2003, n.196 recante il "Codice in materia di

protezione dei dati personali" e ss mm e ii, del decreto della Presidenza del Consiglio dei Ministri n. 148/21 e dei relativi atti di attuazione.

L'Agenzia Intercent-ER, per le finalità successivamente descritte, raccoglie e tratta le seguenti tipologie di dati:

(*i*) Dati 'personali' (es. dati anagrafici, indirizzi di contatto, ecc.);

(*ii*) Dati 'giudiziari', di cui all'articolo 10 del Regolamento UE, relativi a condanne penali o a reati, il cui trattamento è effettuato esclusivamente per valutare il possesso dei requisiti e delle qualità previsti dalla vigente normativa per permettere la partecipazione alla procedura di gara e l'eventuale aggiudicazione. Il trattamento dei dati giudiziari avviene sulla base dell'Autorizzazione al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici, rilasciata dal Garante per la protezione dei dati personali.

Il trattamento dei dati personali conferiti nell'ambito della procedura di acquisizione di beni o servizi, o comunque raccolti dall'Agenzia a tale scopo, è finalizzato unicamente all'espletamento della predetta procedura, nonché delle attività ad essa correlate e conseguenti.

In relazione alle descritte finalità, il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici, con logiche strettamente correlate alle finalità predette e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi.

I dati potranno essere trattati anche in base ai criteri qualitativi, quantitativi e temporali di volta in volta individuati.

Il conferimento dei dati richiesti dall'Agenzia Intercent-ER è necessario, in base alla normativa in materia di appalti e contrattualistica pubblica, per valutare il possesso dei requisiti e delle qualità richiesti per la partecipazione alla procedura nel cui ambito i dati stessi sono acquisiti; pertanto, la loro mancata indicazione può precludere l'effettuazione della relativa istruttoria.

Il concorrente è consapevole che, in caso di aggiudicazione della gara, i dati forniti all'Agenzia Intercent-ER saranno comunicati alle Amministrazioni/Aziende Sanitarie aderenti alla Convenzione per le finalità relative alla sottoscrizione degli Ordinativi di Fornitura e per i relativi adempimenti di legge.

Potranno venire a conoscenza dei suddetti dati personali gli operatori dell'Agenzia individuati quali Incaricati del trattamento, a cui sono impartite idonee istruzioni in ordine a misure, accorgimenti, modus operandi, tutti volti alla concreta tutela dei dati personali.

I dati raccolti potranno altresì essere conosciuti da:

- Soggetti esterni, i cui nominativi sono a disposizione degli interessati, facenti parte della Commissione;

- Soggetti terzi fornitori di servizi per l'Agenzia, o comunque ad essa legati da rapporto contrattuale, unicamente per le finalità sopra descritte, previa designazione in qualità di Responsabili del trattamento e comunque garantendo il medesimo livello di protezione;
- Altre Amministrazioni pubbliche, cui i dati potranno essere comunicati per adempimenti procedimentali;
- Altri concorrenti che facciano richiesta di accesso ai documenti di gara, secondo le modalità e nei limiti di quanto previsto dalla vigente normativa in materia;
- Legali incaricati per la tutela dell'Agenzia in sede giudiziaria.

In ogni caso, operazioni di comunicazione e diffusione di dati personali, diversi da quelli sensibili e giudiziari, potranno essere effettuate dall'Agenzia nel rispetto di quanto previsto Regolamento UE/2016/679 (GDPR).

I dati relativi al concorrente aggiudicatario della gara ed il prezzo di aggiudicazione dell'appalto saranno diffusi tramite il sito internet www.intercenter.regione.emilia-romagna.it.

In adempimento agli obblighi di legge in materia di trasparenza amministrativa, il concorrente prende atto ed acconsente a che i dati e la documentazione che la legge impone di pubblicare siano pubblicati e diffusi tramite il sito internet www.intercenter.regione.emilia-romagna.it, sezione Amministrazione Trasparente.

I dati personali non saranno trasferiti al di fuori dell'Unione Europea.

I dati verranno conservati per un arco di tempo non superiore a quello necessario al raggiungimento delle finalità per i quali essi sono trattati.

Il periodo di conservazione dei dati è di 10 anni dall'aggiudicazione definitiva per la stazione appaltante e dalla conclusione dell'esecuzione del contratto per l'Azienda Sanitaria/Amministrazione contraente e comunque per un arco di tempo non superiore a quello necessario all'adempimento degli obblighi normativi.

A tal fine, anche mediante controlli periodici, verrà verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al perseguimento delle finalità sopra descritte. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non saranno utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

Nell'ambito della presente gara non è previsto alcun tipo di processo decisionale automatizzato.

In qualunque momento l'interessato può esercitare i diritti previsti dagli artt. 7 e da 15 a 22 del Regolamento UE/2016/679. In particolare, l'interessato ha il diritto di ottenere la conferma dell'esistenza o meno dei propri dati e di conoscerne il contenuto, l'origine e le finalità del trattamento, di verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettifica, i destinatari cui i dati saranno comunicati, il periodo di conservazione degli stessi; ha altresì

il diritto di chiedere la cancellazione o la limitazione al trattamento, 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 ovvero revocare il trattamento. La relativa richiesta va rivolta alla Regione Emilia-Romagna, Ufficio per le relazioni con il pubblico (Urp), per iscritto o recandosi direttamente presso lo sportello URP in Viale Aldo Moro 52, 40127 Bologna (Italia): tel. 800 662200, fax 051 4689664, e-mail: accesso@regione.emilia-romagna.it, PEC urp@postacert.regione.emilia-romagna.it.

L'interessato ha altresì il diritto di proporre reclamo all'autorità Garante per la protezione dei Dati personali (www.garanteprivacy.it).

Titolare del trattamento dei dati personali di cui alla presente informativa è l'Agenzia Intercent-ER, con sede in Bologna, Via dei Mille 21, CAP 40121.

L'elenco aggiornato dei responsabili del trattamento designati dall'Agenzia è disponibile, su espressa richiesta, da inoltrare ai seguenti recapiti: Agenzia Intercent-ER, Via dei Mille 21, 40121 Bologna (Italia), tel. 051 527.3081 – 527.3082, fax 051 527.3084, e-mail: intercenter@regione.emilia-romagna.it.

Il Responsabile della protezione dei dati designato è contattabile all'indirizzo mail dpo@regione.emilia-romagna.it o presso la sede della Regione Emilia-Romagna di Viale Aldo Moro n. 30.

ALLEGATI

Sono parte integrante del presente disciplinare di gara i seguenti documenti:

1) Progetto ai sensi dell'articolo 23, commi 14 e 15, del Codice;
2) Bando di gara;
3) Disciplinare di gara;
4) Allegato 1 – DGUE (Deve essere compilato su SATER dall'operatore economico e dall'eventuale ausiliaria. In caso di RTI dovranno compilarlo sia la mandataria che le mandanti)
5) Allegato 1a – Domanda di partecipazione;
6) Allegato 1b - Patto di integrità, approvato dalla Regione Emilia-Romagna con delibera della giunta del 13 aprile 2022 n. 565*;*
7) Allegato 2a – Schema dichiarazioni concordato preventivo;
8) Allegato 2b – Schema Avvalimento;
9) Allegato 3 – Capitolato tecnico;
10) Allegato 3.A – Profili Professionali
11) Allegato 4a – Schema di offerta tecnica Lotto 1;
12) Allegato 4b – Schema di offerta tecnica Lotto 2;
13) Allegato 5 – Schema di offerta economica Lotti 1 e 2;
14) Allegato 6 – Schema di Convenzione Lotti 1 e 2;
15) Allegato 7 – Modulo per attestazione pagamento imposta di bollo

***

PROCEDURA APERTA PER L'ACQUISIZIONE DI SERVIZI DI IT SYSTEM MANAGEMENT E SICUREZZA INFORMATICA 2

CAPITOLATO TECNICO

LOTTI 1 e 2

ALLEGATO 3

(RETTIFICATO)

INDICE

1. PREMESSA

Il presente Capitolato Tecnico disciplina gli aspetti tecnici della Convenzione per la fornitura di servizi relativi all'IT System Management e alla Sicurezza Informatica per le Pubbliche Amministrazioni della Regione Emilia-Romagna (seconda edizione).

2. OGGETTO DELL'ACQUISIZIONE

L'oggetto della fornitura si compone di due lotti: il Lotto 1 riguarda i servizi di gestione, manutenzione, sviluppo delle architetture informatiche e supporto specialistico per le infrastrutture hardware e software di base utilizzati dalle Amministrazioni della Regione Emilia-Romagna a supporto delle proprie attività informatizzate (IT System Management); il Lotto 2 riguarda i servizi necessari e funzionali a garantire adeguati livelli di sicurezza dei sistemi IT nel loro complesso, dei dati trattati e in generale delle informazioni (Sicurezza Informatica).

Il complesso dei servizi e delle attività ricomprese nei due lotti è quindi volto a garantire la piena operatività delle infrastrutture tecnologiche, a mantenerne la perfetta efficienza, a garantire agli utenti la disponibilità e le prestazioni delle applicazioni su di esse installate, l'integrità e confidenzialità dei relativi dati, nonché a fornire il supporto necessario per garantirne il costante allineamento con l'evoluzione tecnologica del mercato ICT e delle soluzioni e servizi di Sicurezza Informatica e a definirne la crescita in coerenza con gli obiettivi strategici delle Amministrazioni stesse.

Si sottolinea che i contesti tecnologici e le architetture applicative sono da intendersi come una fotografia di un panorama tecnologico che è in continua e rapida evoluzione. Pertanto, le Ditte concorrenti dovranno sapersi adeguare in modo flessibile al mutare del contesto di riferimento e dovranno cogliere le opportunità fornite dall'evoluzione tecnologica per proporle ed implementarle, ove necessario, nel sistema informatico delle Amministrazioni.

Oltre al contesto tecnologico si deve tenere conto anche dell'evoluzione normativa nazionale ed europea in materia di Data Protection e Cybersecurity.

Sempre più importante è la costante formazione del personale e delle terze parti delle Amministrazioni, la conoscenza e il know-how tecnico aziendale sul tema della sicurezza informatica, Security Awareness and Training, in aderenza agli standard ISO/IEC 27001, ai Framework nazionale e internazionale (NIST) per la Cybersecurity e la Data Protection e in coerenza con il GDPR (Regolamento europeo 679/2016).

Di seguito si descrivono le caratteristiche tecniche dei servizi richiesti.

3. CONTESTO TECNOLOGICO DELLA FORNITURA

L'ambito tecnologico nel quale dovranno essere erogati i servizi previsti comprende le principali tecnologie presenti nel mercato dell'ICT e della Sicurezza Informatica, ampiamente utilizzate dalle Pubbliche Amministrazioni. Di seguito viene fornita, a titolo puramente indicativo e non esaustivo, una panoramica degli ambiti tecnologici in questione.

3.1 Distribuzione delle infrastrutture

Le infrastrutture hardware e software di base utilizzate da ciascuna Amministrazione possono essere concentrate in un'unica sede o possono essere suddivise su più sedi distribuite sul territorio.

In linea generale, ove il sistema informativo abbia una struttura distribuita su più sedi, i diversi datacenter sono collegati tra loro mediante rete geografica; inoltre, il sistema informativo nel suo complesso dispone tipicamente di collegamenti alla rete internet e al Sistema Pubblico di Connettività (SPC).

Sono da tenere presenti gli sviluppi normativi nazionali per cui la distribuzione potrebbe evolvere secondo quanto previsto per il Polo Strategico Nazionale (PSN), con le conseguenti attività di adeguamento.

3.2 Tipologie hardware e software

Ciascuna Amministrazione può disporre di apparecchiature hardware e prodotti software di base e specifici di varia tipologia, specializzati per diversi ambiti progettuali e funzionali. Nella tabella seguente si riporta una sintesi delle varie tecnologie e dei principali produttori/prodotti presenti sul mercato ICT. Si sottolinea che tale elenco è fornito a puro titolo indicativo e non esaustivo.

Il Fornitore prende atto che le Amministrazioni possono introdurre variazioni dell'ambito tecnologico a fronte di specifiche esigenze delle Amministrazioni stesse, o per le naturali evoluzioni dei sistemi ICT e necessità di adeguamento dei livelli di sicurezza e si impegna ad erogare i servizi di system management o sicurezza informatica adeguando le conoscenze del personale impiegato o inserendo nei gruppi di lavoro risorse con skill adeguato, senza alcun onere aggiuntivo per le Amministrazioni.

Sistemi Operativi e Tecnologie di Virtualizzazione	
Sistemi Operativi	Linux (Red Hat, CentOS, Ubuntu, FreeBSD, Debian, Suse, Oracle), Windows, Apple Mac OSX
Software di virtualizzazione	VMware, Hyper-V, Citrix, RHeV
Software di Infrastruttura	

Storage management	SAN management software, HSM (Brocade DCFM, CA Technologies SRM, EMC Ionix ECC, Hitachi Storage Command Suite, HP Storage Essentials, IBM TPC, NetApp OnCommand)
Backup & recovery	CA Technologies ArcServer, CommVault Simpana, EMC Data protection suite, HP DataProtector, IBM TSM, Symantec Netbackup
Application integration & middleware software	integration middleware (web services, ESB, message-oriented middleware) (IBM Websphere MQ, Oracle Fusion middleware, RedHat Jboss ESB, Software AG WebMethods, Tibco)
	application server & transaction processing (Apache Tomcat, IBM Websphere, Microsoft .NET framework, Oracle Weblogic, RedHat Jboss)
	portals and web infrastructure (IBM Websphere portal, Microsoft Sharepoint, OpenText, Oracle Webcenter portal, RedHat Jboss EPP, Docker e Kubernetes)
Data management and integration	database management systems and tools (administration, utilities, monitoring) (DB2, Oracle, SQL Server, MySQL, PostGresSQL, MongoDB)
	data integration (ETL, quality, metadata) (IBM Infosphere, Informatica Powercenter, Microsoft SSIS, Oracle, SAP, SAS Dataflux)
Enterprise content management	Document management, Workflow/Business Process Management, Web content management (Alfresco, Microsoft Sharepoint, IBM FileNet e Webcontent manager, Oracle Webcenter, OpenCMS, OpenText)
IT operations management software	System monitoring (Microsoft Operations Manager, Oracle Enterprise Manager, IBM Tivoli, BMC, CA, HP)
	Security agent (antivirus, activity monitor & audit solution, logging)
	Application performance monitoring (BMC, CA, Compuware, HP, Oracle, Quest Software)
	IT service management (service desk, asset, change, configuration management) (BMC Remedy, CA Service Desk Manager, IBM Smartcloud Control Desk) workload automation (BMC Control M, CA workload automation, IBM Tivoli workload scheduler)
Identity & data management software	Identity and access management (single sign-on), Data access management (FAM), Privileged access management (PAM)
Enterprise Software	
Business Intelligence	IBM Cognos, Microstrategy, Oracle BIEE, Pentaho, Qlicktech, SAP BusinessObjects e BW
Customer Relationship Management	Oracle Siebel, SAP Customer Service
Enterprise Resource Planning	SAP/R3, SAP HANA, SAP BPC, SAP HR ed eRecruiting, Oracle JD

	Edwards EnterpriseOne, SAGE ERP X3
Api Management	Kong API Gateway and Service Connectivity Platform, Wso2
Software Client	
Client software	sistemi operativi client e dispositivi mobili (Windows, Apple, Android)
	prodotti software di informatica individuale (MS Office, MS SharePoint, OpenOffice)
	web browser (MS Edge, Firefox, Chrome, Safari)
	antivirus (MCAfee, Norton, Trend Micro ecc.), data leak prevention ed encryption
	Sistemi di virtualizzazione (XenApp, XenDesktop)
	software distribution e remote desktop control
Tecnologie Hardware	
Server	server entry-level, midrange o enterprise, configurazioni standalone, rack o blade, architettura x86 o RISC
Storage	SAN, NAS, protocolli fiber channel, fiber channel-over-Ethernet, iSCSI, Infiniband, tape library e virtual tape library, object storage
Network & security	Protocolli di rete e di routing per reti locali, cablaggio strutturato, sistemi wireless, apparati (switch, router, firewall, load balancer, wifi access points), network solutions (Alcatel-Lucent, Avaya, Brocade, Check Point software, Cisco, Extreme Networks, Fortinet, HP)
Tecnologie Data Analytics	
Big data/Data Analytics	Apache Spark, Kafka, Hadoop, Ambari, Redash e Azure Synapse
Tecnologie Cloud	
Public Cloud	Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)
Tecnologie Sicurezza	
Security software, technology and service	Data security (encryption), endpoint, server e email security (antivirus, antimalware, anti-ransomware), xDR Detection and Response, network security (firewall, VPN, IDS/IPS) e Network Access Control (Forescout, Fortinac), Data Loss Prevention (DLP), Zero Trust Architecture, Penetration Test e Vulnerability assessment su sistemi e reti (LAN e Wifi), Vulnerability management e Web Application Scan, DAST, SAST, SCA: verifica del codice dinamico e statico per applicazioni sicure nell'intero ciclo di vita (SDLC a garanzia del principio generale di "sicurezza e privacy by design e by default"). Risk management.
Monitoring and orchestrator	Security information and event management – SIEM e Security Orchestration, Automation and Response - SOAR (Microsoft Sentinel

	IBM, MICROFOCUS, Splunk, ecc…) UEBA (User and Entity Behavior Analytics)
Threat intelligence and information sharing	External Attack Surface Management (EASM), Threat Intelligence service e Commercial Digital Risk Protection, MISP Threat Sharing
Security Awareness	Piattaforme specialistiche di ambito E-Learning training and gaming

4. CARATTERISTICHE, MODALITA' E SPECIFICHE DEI SERVIZI

Di seguito sono descritti in dettaglio i servizi richiesti per il Lotto 1 "IT System Management" e il Lotto 2 "Sicurezza Informatica" oggetto della Convenzione.

4.1 Lotto 1 – IT System Management

Il presente Lotto 1 annovera al suo interno un insieme di servizi e attività che in virtù della loro complessità e soprattutto criticità devono essere svolti in piena e stretta sinergia con le figure professionali dell'IT, interno all'Ente, del Fornitore dei servizi di Sicurezza Informatica o di eventuali altre figure professionali che operano per conto dell'Amministrazione. Per questo è richiesta la massima collaborazione fra le parti, in accordo con l'Amministrazione committente.

Di seguito l'elenco dei Servizi inerenti al presente Lotto.

4.1.1 Servizi di Monitoraggio Sistemi e Reti

Il "Servizio di Monitoraggio Sistemi e Reti" comprende al suo interno il servizio di monitoraggio operato sullo strato network dell'architettura, erogato dal **NOC – Network Operation Center.**

In particolare, il sottoservizio **NOC** si occuperà della rilevazione di malfunzionamenti hardware e/o software tali da rendere irraggiungibili od inutilizzabili i servizi effettuando gli interventi di primo livello e le attività di escalation verso i livelli superiori a seguito di procedure schedulate.

Pertanto, il Fornitore deve disporre all'interno del proprio Centro Servizi per l'Operatività da Remoto del servizio NOC da mettere a disposizione delle Amministrazioni che facciano richiesta di servizi da erogare mediante tale modalità operativa.

La lingua di riferimento per l'erogazione dei servizi deve essere l'italiano.

Da tale Centro, attraverso l'utilizzo degli opportuni strumenti e mediante l'impiego di personale specializzato, il Fornitore dovrà avere la possibilità di operare in collegamento con i sistemi dell'Amministrazione per effettuare tutte le attività di gestione che non richiedono necessariamente la presenza di personale in loco, ad esempio:

- monitoraggio dei sistemi, delle reti, delle applicazioni e dei database;
- gestione dei processi di service management;

- esecuzione dei processi di change semplici e proceduralizzati (definizione utenze, reset password, ecc.);
- attività di Gestione Operativa remotizzabili (riavvio application server, ecc..).

Compreso inoltre:

- controllare costantemente (sulla base delle finestre di erogazione del Servizio concordate con l'Amministrazione) il sistema di "monitoraggio ed allarmistica" per poter intervenire proattivamente e/o tempestivamente in caso di attivazione di regole di allarme o superamento di soglie critiche preimpostate su tutti i componenti della rete compresi tutti i server dell'infrastruttura;
- ricevere, qualificare e gestire fino a chiusura le richieste di assistenza che potranno generarsi da tale sistema di monitoraggio o tramite chiamata sia di personale dell'Amministrazione, sia di Help-desk di società terze che forniscono servizi di manutenzione su sistemi hardware e software utilizzati dall'Amministrazione stessa;
- gestire in autonomia la gestione degli allarmi, contattando servizi di Help-Desk di fornitori terzi (quali provider di connettività, manutentori di sistemi hardware e software, etc.), contattando il personale tecnico dell'Amministrazione qualora ve ne sia la necessità; l'Amministrazione fornirà al Fornitore l'elenco dei numeri utili ed i relativi codici di accesso per i vari Helpdesk qualora presenti.
- essere un single point of contact attivo e raggiungibile (sulla base delle finestre di erogazione del Servizio concordate con l'Amministrazione) tramite numero di telefono ed e-mail;
- coordinare gli interventi on-site di fornitori terzi e se necessario prendere i relativi accordi logistici con le strutture presso le quali gli apparati sono installati. La Ditta dovrà collaborare con il fornitore terzo fino al completo ripristino della configurazione e la ripresa delle complete funzionalità;
- provvedere ad inviare periodicamente (con cadenza concordata con il personale dell'Amministrazione), tramite comunicazione e-mail, un riepilogo degli allarmi attivi e di tutte le criticità in atto;
- informare il personale dell'Amministrazione di eventuali anomalie/guasti, all'insorgere dell'allarme;
- generare report relativi a target monitorati; periodicità e tipologia dei report generati verranno concordati con l'Amministrazione.

Da parte del NOC dovrà essere realizzato un accesso ridondato al sistema di monitoraggio installato presso l'Amministrazione, in modo da garantirne l'utilizzo anche in caso di fault del collegamento primario.

Tutto il personale del NOC deve essere in grado di prendere in carico tutte le attività relative all'infrastruttura dell'Amministrazione, al fine di garantire una continuità di servizio al Committente; a tal fine, pertanto, il Fornitore deve adeguatamente formare ed istruire il personale del NOC, relativamente all'infrastruttura ICT dell'Amministrazione stessa.

Il NOC del Fornitore deve rispettare inoltre le seguenti regole:

- la connessione telematica tra il Centro Servizi e le sedi dell'Amministrazione deve essere realizzata attraverso canale dedicato punto-punto a costo del Fornitore. Nessun onere potrà essere ascritto all'Amministrazione. Si intende ricompresa nella connessione anche la dotazione degli apparati di networking ed ogni altra dotazione necessaria, inclusi i cablaggi dalla terminazione di rete del Provider del collegamento ai locali CED dell'Amministrazione. La soluzione deve garantire adeguate prestazioni e affidabilità in caso di malfunzionamento di uno dei componenti dell'infrastruttura;
- il Fornitore deve predisporre presso il proprio Centro servizi una soluzione tecnologica, avente prestazioni e affidabilità adeguate anche in caso di malfunzionamento di uno dei componenti dell'infrastruttura, atta a garantire ai gruppi impegnati nell'erogazione dei servizi;
- In particolare:

  a) **Un punto di accesso alla rete dell'Amministrazione** ed eventualmente, su richiesta, anche un punto di accesso dedicato al sito di Disaster Recovery. In particolare, il Fornitore dovrà garantire che gli accessi alla rete ed ai sistemi dell'Amministrazione avvengano esclusivamente dal personale identificato mediante utenze nominative autorizzate dal proprio sistema di gestione degli accessi. Per quanto riguarda l'accesso ai sistemi di proprietà dell'Amministrazione, il Fornitore dovrà utilizzare utenze nominative nelle modalità concordate con l'Amministrazione, compatibilmente alle specifiche tecnologie e sempre in conformità con quanto previsto dal provvedimento del Garante in materia di accesso degli amministratori di sistema. Non è richiesta la realizzazione di un sistema di Single Sign On che consenta l'uso delle medesime credenziali nei due domini (Sistemi del Centro servizi e Sistemi dell'Amministrazione);

b) **Autenticazione e profilazione delle utenze**. Il processo di autenticazione e profilazione delle utenze è riferito al punto di accesso alla rete dell'Amministrazione;

c) **Tracciatura degli accessi ai sistemi** (login, ssh, desktop remoto, ecc.). In ottemperanza al provvedimento del Garante per la protezione dei dati personali, in materia di accessi degli amministratori di sistema, dovrà essere possibile registrare gli accessi e le attività eseguite dagli amministratori, sul sistema per la gestione degli accessi del Centro Servizi. Per quanto riguarda la registrazione degli accessi e delle attività degli Amministratori su ciascun sistema di proprietà dell'Amministrazione, le modalità saranno concordate con l'Amministrazione;

d) **Conservazione dei Log**. È richiesta la conservazione per almeno un anno dei log del sistema di gestione degli accessi, utilizzato per l'accesso alla rete ed ai sistemi dell'Amministrazione, utilizzando strumenti di conservazione e di gestione dei log predisposti dal Centro servizi del Fornitore. L'Amministrazione si riserva di richiedere tali log con frequenza periodica in base alle procedure concordate con il Fornitore stesso.

- il Fornitore deve garantire la sicurezza del collegamento e la riservatezza dei sistemi e delle informazioni attraverso la formalizzazione e l'applicazione di procedure e politiche di sicurezza da adottare al proprio interno, adeguate ai requisiti stabiliti. Infatti, è responsabilità del Fornitore assicurare che il Centro Servizi, le infrastrutture in esso ospitate, le informazioni gestite e le transazioni da e verso la rete dell'Amministrazione siano protette mediante l'adozione di adeguati sistemi e metodologie definite utilizzando come riferimento le norme della serie ISO/IEC 27001. In particolare, nell'esecuzione dei servizi, il Fornitore deve garantire l'evoluzione, la manutenzione e l'adeguamento tecnologico dei sistemi, delle reti e di tutti gli strumenti impiegati presso il Centro servizi che si rendano necessarie a soddisfare i requisiti di sicurezza stabiliti, nonché l'aggiornamento delle politiche di sicurezza e delle contromisure attuate e la risoluzione reattiva o proattiva di incidenti di sicurezza.

In considerazione dell'esigenza di garantire il massimo grado di copertura di tutti gli aspetti di sicurezza, si richiede la redazione di un Piano della Sicurezza, in conformità a best practice e/o a standard internazionali, secondo quanto concordato con l'Amministrazione.

Nel seguito si riportano alcuni requisiti da intendersi come minimi.

Categoria	Requisiti minimi

Sicurezza delle reti	Il punto di accesso alla rete dell'Amministrazione deve essere adeguatamente protetto mediante sistemi firewall che operino secondo modalità note come "Stateful inspection". Devono essere utilizzati sistemi/meccanismi di intrusion detection e prevention che analizzino il traffico in entrata ed in uscita dalla rete dell'Amministrazione.
Riservatezza dei dati e delle trasmissioni	Deve essere garantita la riservatezza di tutti i dati gestiti.
Integrità dei dati	Devono essere adottati antivirus centralizzati ad aggiornamento periodico, che analizzino e bonifichino gli eventuali codici malevoli. Devono essere adottati antivirus su tutte le postazioni utilizzate dal personale del Fornitore e collegate con la rete dell'Amministrazione. Tali postazioni devono soddisfare lo standard per le postazioni di lavoro previste per l'Amministrazione
Auditing e vulnerability assessment	Devono essere registrati tutti gli eventi telematici che hanno impatto sui sistemi, effettuati dal Centro servizi del Fornitore, permettendo la ricostruzione di comportamenti insidiosi e l'individuazione di possibili responsabilità penali e civili conseguenti condotte illecite. Tali registrazioni dovranno essere effettuate e conservate sui sistemi del centro servizi che consentiranno l'accesso alla rete dell'Amministrazione, ovvero sui sistemi dell'Amministrazione, secondo le modalità concordate con l'Amministrazione.
Amministrazione accessi	Devono essere adottati adeguati processi di Amministrazione degli accessi (fisici e logici) effettuati nel Centro servizi che prevedano l'identificazione delle diverse categorie di utenti, la definizione dei corrispondenti profili di autorizzazione e delle modalità di rilascio dell'accesso.

Il Fornitore deve garantire la continuità dei servizi anche in caso di evento disastroso e/o di interruzione della connessione tra il Centro servizi e la rete dell'Amministrazione.

In particolare, il Fornitore deve implementare una soluzione, tecnica ed organizzativa, che consenta di garantire il ripristino delle funzionalità al fine di garantire l'erogazione dei servizi ed il rispetto dei requisiti di qualità contrattuali.

Il Fornitore, se richiesto dall'Amministrazione, dovrà mettere a disposizione una piattaforma di Monitoraggio dei sistemi e delle applicazioni (diversamente utilizzerà la piattaforma già in essere presso l'Amministrazione committente).

La piattaforma di monitoraggio dovrà consentire di tenere sotto controllo lo stato operativo dei sistemi e delle relative componenti e degli apparati di rete, rilevando automaticamente informazioni quali a titolo esemplificativo, ma non esaustivo, le seguenti:

- Stato dei diversi sistemi, sottosistemi, servizi ed apparati;
- Parametri critici per la funzionalità dei diversi sistemi, sottosistemi, servizi ed apparati, definendo dei valori di soglia che denuncino la prossimità di situazioni critiche. Ad esempio, per i server tali parametri potranno riguardare: Spazio Disco, Utilizzo memoria, utilizzo CPU, utilizzo schede di rete;
- Stato dei processi applicativi che siano di particolare rilevanza per la funzionalità dei servizi erogati.

Gli eventi generati dalla piattaforma di monitoraggio dovranno essere collezionati in appositi Log. La piattaforma dovrà inoltre essere configurata in modo da intraprendere eventuali azioni correttive in maniera automatica.

Nell'ambito della piattaforma di monitoraggio, il Fornitore dovrà prevedere una soluzione per il monitoraggio end-to-end dei servizi applicativi erogati agli utenti finali, in modo da poterne facilmente verificare lo stato operativo e prestazionale.

Correlando tutte le informazioni provenienti dai vari sistemi che costituiscono l'ambiente di esercizio con quelle relative alle transazioni applicative, la soluzione dovrà dare evidenza dello stato operativo dei servizi applicativi erogati ed essere così di supporto alla rapida risoluzione dei problemi.

In particolare, dovrà consentire di identificare automaticamente le componenti da controllare lungo la catena applicativa in caso di errore.

Oltre a monitorare la disponibilità dei servizi applicativi e ad essere di supporto nella risoluzione dei problemi, la soluzione dovrà consentire di verificare e controllare le performance dei servizi erogati per verificarne l'aderenza ai livelli di servizio attesi.

Il software di monitoraggio fornito dal Fornitore (se richiesto dall'Amministrazione) dovrà essere installato su server di proprietà dell'Amministrazione stessa.

Compito del Fornitore sarà in particolare di:

- installare la piattaforma di monitoring e tutti i software necessari al suo corretto funzionamento sui server dell'Amministrazione; tutti i software necessari al funzionamento del monitoraggio non dovranno avere alcun costo di licenza aggiuntivo (compreso il sistema

operativo dei server);

- provvedere alla configurazione di target monitorabili tramite SNMP, script sviluppati su misura, verifica di URL, query sui principali DB (Oracle, MySQL, SQLServer, ecc…), verifiche su file di log, sviluppo di moduli aggiuntivi per soddisfare le esigenze puntuali;
- assistere il personale dell'Amministrazione nella definizione ed ottimizzazione dei target da monitorare;
- permettere l'accesso al portale WEB di monitoraggio tramite autenticazione Active Directory o LDAP (diversi domini di autenticazione potranno esistere contemporaneamente);
- profilare gli accessi al sistema di monitoraggio.

4.1.2 Servizi di Conduzione Operativa Sistemi

La "Conduzione Operativa Sistemi" comprende sia i servizi base di gestione continuativa (sottoservizio "**Server logici e fisici"**) sia i servizi di gestione delle piattaforme di memorizzazione e archiviazione (sottoservizio "**Storage/Backup"**). La conduzione dei sistemi "**Server logici e fisici"** prevede quindi la manutenzione attiva dei sistemi, la gestione dei software di base e d'ambiente, le basi dati, la gestione sicurezza logica di base e la gestione della configurazione nonché delle variazioni dovute a normale conduzione degli apparati precedentemente citati. È compito del servizio di conduzione dei server, secondo le specifiche dell'apparato in oggetto (mail server, DB server, etc.) predisporre, governare e presidiare la corretta esecuzione dei piani di backup in aderenza a quanto previsto dal piano dedicato. Per quanto attiene la gestione dei sistemi di storage e backup, attività erogata nel sottoservizio dedicato, sono comprese nel servizio la gestione delle LUN, la modifica/creazione di nuovi segmenti e aree di archiviazione, la gestione delle autorizzazioni ed abilitazioni all'accesso delle stesse aree di memorizzazione. Relativamente alla gestione dei backup rientra all'interno dei compiti del servizio la verifica della funzionalità degli apparati dedicati, il check sul corretto stato di servizio dei supporti di memorizzazione (siano essi magnetici a cassetta o HDD). Sarà compito del servizio anche la segnalazione di eventuali malfunzionamenti e/o deterioramenti degli apparati laddove tali danni dovessero compromettere la funzionalità degli apparati e di conseguenza inficiare il buon esito delle politiche di backup. Si evidenzia che, gli apparati switch fibre channel, per le loro peculiari caratteristiche, risultano amministrati in questo servizio e non nella macrocategoria "Conduzione Operativa Reti".

Pertanto, per Conduzione Operativa si intende il complesso delle attività riconducibili all'ordinaria gestione e manutenzione dell'infrastruttura IT garantendone il funzionamento e l'efficienza.

Gli obiettivi della conduzione operativa sono:

- garantire la disponibilità dei sistemi e l'esecuzione delle attività schedulate;

- assicurare un continuo controllo sullo stato dei sistemi e dei collegamenti, individuare criticità o malfunzionamenti ed intraprendere le azioni necessarie;
- prevenire, gestire e risolvere tutti i problemi che comportano interruzione o degrado del servizio all'utenza;
- ottimizzare l'utilizzo dello storage in termini di razionalizzazione degli accessi e garantire la disponibilità, la salvaguardia e l'integrità dei dati;
- garantire l'efficienza dei sistemi rispetto all'utilizzo delle risorse hardware e software;
- controllare l'impatto sulla tecnologia esistente e garantire l'adeguamento degli ambienti elaborativi a fronte dell'immissione in esercizio di modifiche correttive e/o evolutive di applicazioni esistenti;
- monitorare e verificare i consumi effettivi delle eventuali infrastrutture e servizi in cloud.

Nella conduzione operativa sistemi sono incluse, a titolo indicativo, le attività descritte nei paragrafi di seguito.

4.1.2.1 Presa in carico di nuovi Servizi e Tecnologie

L'attività è finalizzata alla presa in carico di nuovi servizi, sistemi, procedure operative e di tutti gli elementi base oggetto dei servizi di gestione (sistemi, apparati HW, prodotti SW e firmware).
Il Fornitore è responsabile di effettuare tutte le attività necessarie per l'avviamento e per la presa in carico sia nei casi in cui le attività realizzative siano state effettuate dal Fornitore stesso sia nei casi in cui le attività realizzative siano state effettuate da terze parti (es. vendor).
Il Fornitore è responsabile:

- di eseguire le procedure definite dall'Amministrazione per la messa in produzione delle infrastrutture;
- di eseguire le procedure definite all'interno del processo di "Service Asset & Configuration Management" per l'identificazione dei nuovi Elementi di Configurazione;
- dell'implementazione e gestione delle politiche di software Distribution relativamente al parco tecnologico dell'Amministrazione della verifica, valutazione ed eventuale integrazione della documentazione prevista dall'Amministrazione.

4.1.2.2 Gestione Piattaforme Elaborative

Le attività sono volte a mantenere un ambiente di elaborazione stabile e tale da garantire il soddisfacimento dei requisiti operativi. Più in dettaglio, le attività consistono nell'integrazione dei prodotti di terze parti con le componenti del sistema operativo, comprendendo le attività di aggiornamento, test di funzionalità e distribuzione del software utilizzato, nel rispetto dell'evoluzione

tecnologica dei sistemi, degli standard di mercato e dei livelli di servizio contrattuali. La gestione degli ambienti elaborativi prevede in particolare:

- l'installazione, personalizzazione, distribuzione, manutenzione e test del sistema operativo, dei sottosistemi e dei prodotti del middleware (Web Server, Application Server, Data Server, ecc.);
- la definizione ed attuazione delle procedure di automazione operativa (script di avvio/arresto, controllo dei servizi, trasferimento automatico di dati, ecc.);
- le configurazioni necessarie all'integrazione di prodotti software (configurazioni dei prodotti relativi all'ambiente, alla sicurezza, alla connettività, all'autenticazione attraverso servizi di gestione centralizzata delle utenze, alla comunicazione tra diversi layer tecnologici, ad es. Application server e Data Base server);
- coordinamento degli interventi di manutenzione HW;
- verifica periodica delle fonti di pubblicazione dei bollettini di sicurezza per le tecnologie in uso presso l'Amministrazione ed esecuzione periodica dell'aggiornamento dei sistemi per la rimozione delle vulnerabilità di sicurezza (installazione patch, windows update, modifiche alla configurazione dei servizi, ecc.) in accordo con le misure di prevenzione degli incidenti definite dal committente. A tal proposito, si precisa che l'Amministrazione consentirà l'utilizzo delle utenze di accesso ai network dei vendor di cui è in possesso, con cui il Fornitore potrà consultare informazioni relative alla sicurezza. Tuttavia, il Fornitore dovrà accedere a bollettini pubblici e/o informazioni ottenute attraverso propri canali, a complemento della citata attività;
- coordinamento ed esecuzione di tutte le attività legate alla conduzione dei siti di disaster recovery/business continuity sia nella normale conduzione (compreso l'allineamento dei dati fra i vari siti ove richiesto), sia a fronte dei test periodici e a fronte di dichiarazioni di disastro da parte dell'Amministrazione. L'Amministrazione si riserva di effettuare test di DR ogni qualvolta l'evidenza della situazione, variazioni significative dell'infrastruttura, obblighi normativi o procedure di qualificazione per i servizi IT che l'Amministrazione dovrà o vorrà osservare, lo richiedano.

In generale, il Fornitore è tenuto farsi parte proattiva nel proporre e analizzare modifiche agli apparati gestiti, al fine di mantenerli allineati alle ultime fix, release e versioni del software installato.

4.1.2.3 Gestione delle Procedure Batch

Le procedure batch si articolano in:

- batch applicativo, schedulato a seguito di richiesta effettuata dalle varie aree applicative;
- batch tecnico, che riguarda essenzialmente il salvataggio dei dati e la memorizzazione dei dati di sistema, utilizzati per la produzione di report statistici mensili.

Il Fornitore ha la responsabilità del buon esito del batch tecnico per tutti i prodotti installati, compresi quelli di automazione. Inoltre, il Fornitore ha la responsabilità, a fronte di errori di esecuzione del batch applicativo, di fornire il supporto per verificare eventuali cause riconducibili all'infrastruttura. Il Fornitore si impegna ad utilizzare i prodotti messi a disposizione dall'Amministrazione per l'automazione delle attività di IT Operations in ambienti open.

4.1.2.4 Gestione Alta Affidabilità

Per tutti i sistemi per i quali sia stato configurato un meccanismo di alta affidabilità (per esempio cluster Microsoft, cluster Linux, Oracle RAC, ridondanza di connessioni fisiche), sulla base della periodicità concordata o a fronte di un change complesso su uno specifico sistema, il Fornitore deve produrre un piano che descriva le modalità di test, i risultati attesi, ed eseguire il test secondo la tempistica concordata con l'Amministrazione.

4.1.2.5 Gestione dello Storage

L'attività si sostanzia principalmente nel:

- controllare l'utilizzo dei dischi e delle Virtual Tape Library (VTL), per assicurare la disponibilità di spazio;
- gestire lo spazio sui dischi e le VTL;
- riorganizzare gli archivi, per assicurarne la massima efficienza;
- creare, gestire e ripristinare i cataloghi utente;
- classificare i tipi di dati e le applicazioni che li utilizzano;
- ottimizzare l'utilizzo dello storage;
- definire le politiche di gestione VTL4;
- l'analisi conoscitiva dell'utilizzo dello storage e produzione costante di reportistica;
- bonificare i dati obsoleti;
- la configurazione degli switch per le necessità di nuovi collegamenti (zoning, ecc.) e inizializzazione dei dischi.

Le politiche di backup da adottare sono definite dall'Amministrazione; per politiche di gestione delle VTL si intende la realizzazione delle suddette politiche di backup tramite l'implementazione e la

gestione sulle VTL, di procedure operative, configurazioni e automazioni e quant'altro il fornitore ritenga necessario.

Le politiche di backup definiscono Retention prestabilite per classi di dati e servizi; pertanto, per bonifica dei dati si intende il recupero degli spazi di archiviazione della VTL a scadenza delle singole Retention.

4.1.2.6 Backup e Restore Management

L'esecuzione delle operazioni di backup e restore è basata sui prodotti in uso presso l'Amministrazione che si interfacciano con i vari tool disponibili per ciascuna tipologia di Piattaforma/Database.

Il Fornitore deve garantire la continuità dei servizi e/o il recupero dei dati (dati di sistema e delle applicazioni) in tutti i casi in cui si renda necessario, comprendendo l'ultima transazione eseguita con successo.

Sulla base delle politiche definite dall'Amministrazione, è responsabilità del Fornitore definire la pianificazione delle attività di backup, al fine di ottimizzare la finestra temporale a disposizione.

4.1.2.7 Gestione Database

Il Fornitore deve effettuare l'amministrazione, ottimizzazione e installazione dei database ospitati dai sistemi gestiti. Le attività da svolgere nell'ambito di tale servizio sono, ad esempio, le seguenti: installazione e upgrade dei prodotti, configurazione ed amministrazione dei database, riorganizzazione dei dati.

A titolo esemplificativo ma non esaustivo si prevedono le seguenti attività:

- installazione e configurazione del database;
- DB Administration (creazione tabelle, caricamento dati, ripristino degli indici, ottimizzazione dei DB, ecc.);
- aggiornamento dati statistici del catalogo del database;
- soluzione delle anomalie;
- installazione delle fix correttive e di sicurezza;
- installazione nuovi release;
- reporting periodico per evidenziare le frammentazioni dei database;
- analisi delle prestazioni delle singole sessioni applicative ed individuazione di possibili ottimizzazioni del codice.

4.1.2.8 Gestione Dominio

Il Fornitore deve effettuare la gestione del dominio secondo le politiche definite dall'Amministrazione, in particolare per ciò che concerne la sicurezza.

Le principali attività svolte nell'ambito dell'erogazione del servizio sono le seguenti:

- gestione sistemistica dell'AD: attività di conduzione funzionale dell'Active Directory, quali il monitoraggio, il backup, il patch management (limitatamente ai domain controller) e la gestione log (raccolta ed archiviazione) per tutti i Domain Controller;
- gestione degli account utente su AD
- gestione del dominio: gestione delle policy, dei computer in dominio, della propagazione delle policy sui singoli computer, gestione del servizio DNS.

Il Fornitore deve provvedere alla sospensione/cancellazione di tutte le utenze riconducibili al Fornitore uscente, dando evidenza dell'operazione all'Amministrazione tramite elenchi ordinati per server (ordinati per dominio nel caso di utenze di dominio), entro il termine massimo concordato con l'Amministrazione in fase di subentro. Inoltre, entro tale medesimo termine, il Fornitore deve provvedere alla modifica delle password per tutte le utenze di tipo Amministrazione o Super User, secondo le politiche in essere.

4.1.2.9 Gestione Middleware

Le principali attività da svolgere nell'ambito dell'Amministrazione di tali prodotti sono:

- installazione e configurazione dei prodotti e loro evoluzione e manutenzione;
- deploy delle applicazioni e/o degli oggetti applicativi (applicazioni, report, siti, folder, ecc.);
- implementazione di configurazioni di scalabilità orizzontale o verticale (configurazione dei domini, dei cluster, dei cloni, ecc.) a seconda delle necessità;
- configurazione delle integrazioni tra i servizi (Enterprise Service Bus, Single Sign On, ecc.);
- configurazione delle code, degli End Point, ecc…;
- configurazione delle utenze e dei relativi privilegi;
- analisi dei log e delle eccezioni applicative o sistemistiche;
- analisi delle prestazioni degli specifici ambiti di installazione applicativa (ad es. Java Virtual Machine, Microsoft IIS) utilizzando gli strumenti propri di ogni singolo midlleware (Oracle Enterprise Manager, ecc.);
- correzione delle anomalie e manutenzione periodica per l'allineamento del livello di patch necessario alla rimozione dei bug e delle vulnerabilità dei prodotti;
- predisposizione di script gestionali per l'avviamento e l'arresto delle singole applicazioni o di

specifici processi/componenti;

- gestione dei componenti/device periferici (libreria ottica, stampanti di sistema, ecc.);
- predisposizione degli agent di test e di profilazione delle applicazioni e supporto all'analisi dei dati raccolti.

In considerazione della rapida evoluzione di queste tecnologie e delle frequenti opportunità di variazione del contesto tecnologico dell'Amministrazione, soprattutto per l'adozione di nuove piattaforme middleware, il Fornitore deve garantire un adeguato rinnovamento delle competenze.

4.1.2.10 Definizione delle Procedure Operative

È richiesto che il Fornitore effettui la definizione delle procedure operative a supporto della standardizzazione delle attività tecniche afferenti i servizi di Conduzione Operativa dei Sistemi dell'infrastruttura e ne produca la documentazione di dettaglio.

Inoltre, è responsabilità del Fornitore predisporre e mantenere aggiornate procedure automatiche (script, procedure, ecc.) a supporto delle attività di conduzione. Ciascuna procedura automatica è accompagnata dalla documentazione concordata, da sottoporre all'approvazione dell'Amministrazione, necessaria all'eventuale presa in carico e manutenzione della procedura stessa da parte dell'Amministrazione o da terzi da essa designati. Il formato ed i contenuti di tale documentazione sono concordati nel corso degli incontri tecnici.

Nell'eventualità in cui l'Amministrazione si avvalga di terzi per la predisposizione di procedure automatiche, il Fornitore ha la responsabilità di prendere in carico le stesse nonché di effettuarne la gestione e gli eventuali successivi adeguamenti.

L'Amministrazione si riserva la facoltà di sottoporre a verifica e/o accettazione le procedure realizzate e/o modificate dal Fornitore.

4.1.2.11 Gestione Piattaforme di Posta Elettronica

Il servizio di Conduzione Operativa Sistemi deve comprendere anche il servizio di gestione della posta elettronica che prevede: la gestione e l'aggiornamento periodico dei sistemi di posta elettronica in uso presso l'Amministrazione; la gestione dei backup, del monitoraggio degli stessi e dell'eventuale recovery dell'intero sistema server e/o della singola casella e-mail.

Obiettivo della fornitura del servizio di gestione della posta elettronica è permettere il regolare funzionamento 24h x 365 giorni/anno, salvo brevi periodi di manutenzione, della posta elettronica in ingresso ed in uscita, mediante le attività necessarie, quali (a titolo esemplificativo e non esaustivo) quelle di seguito definite:

- gestire il servizio di posta elettronica dei domini di posta, assicurando la manutenzione e il

corretto funzionamento del servizio;

- dare il necessario supporto alla corretta gestione/creazione/eliminazione degli indirizzi di posta elettronica o alias, assegnati a ciascun utente o a liste di distribuzione;
- effettuare il controllo antivirus ed anti-spamming sui sistemi coinvolti ed attivare, le eventuali azioni di contrasto;
- effettuare periodicamente il controllo del corretto funzionamento ed aggiornamento del sistema antivirus sui sistemi di posta;
- garantire adeguate misure di sicurezza al fine di evitare usi impropri dei Server che fanno parte del Sistema preposto al servizio di posta elettronica;
- garantire un efficace livello di performance del servizio ed azioni in direzione del miglioramento delle stesse;
- garantire tempi rapidi di ripristino del servizio o di ogni sua parte componente in caso di disservizio;
- apportare modifiche alle configurazioni dei sistemi di posta per allinearli con le esigenze che possono emergere;
- implementare e manutenere i meccanismi di aggiornamento/creazione automatica delle caselle di posta e di ogni altro elemento del sistema (realizzati tramite scripting per es.).

Tutte le attività di gestione ordinaria/straordinaria del sistema di posta elettronica dovranno essere preventivamente concordate con il personale dell'Amministrazione.

4.1.3 Servizi di Conduzione Operativa Reti

La **"Conduzione Operativa Reti"** prevede la manutenzione attiva dei sistemi di rete, la gestione delle regole di routing e di sezionamento delle reti (VLan). E' compresa la copia e backup delle configurazioni degli apparati in aderenza a quanto previsto dall'apposito piano, qualora esistente.

Il servizio ha la finalità di garantire il corretto funzionamento dell'infrastruttura attiva di rete LAN attraverso il suo continuo monitoraggio e l'interazione con i fornitori titolari dei contratti di manutenzione delle apparecchiature di rete, siano esse parte del cablaggio o wireless, inclusi i dispositivi operanti come firewall, utilizzati dall'Amministrazione, nonché di monitorare l'infrastruttura della rete geografica dell'Amministrazione (WAN) attraverso l'utilizzo degli strumenti messi a disposizione dal fornitore assegnatario dei servizi di connettività in rete geografica.

Tale servizio dovrà essere realizzato con adeguato personale tecnico, che garantisca il corretto e completo funzionamento di tutti gli aspetti di configurazione dei vari apparati costituenti il sistema e l'integrazione con tutti i sistemi appartenenti alla infrastruttura di rete.

La Ditta avrà anche il compito di supportare il personale tecnico dell'Amministrazione, per le problematiche di rete e nella fase di troubleshooting.

Il Fornitore deve garantire la continuità di esercizio delle reti anche a fronte di problemi particolarmente complessi.

In particolare, il servizio:

- gestisce l'indirizzamento IP secondo gli standard concordati con l'Amministrazione, la nomenclatura/indirizzamento dei server e dei posti di lavoro, nonché i parametri di configurazione e di QoS;
- prevede la razionalizzazione dell'infrastruttura di rete attiva e passiva, sulla base di quanto concordato con l'Amministrazione;
- prevede l'implementazione e la gestione dei sistemi di problem determination e di analisi degli output a supporto delle applicazioni che utilizzino l'infrastruttura di rete (es. sniffer, sonde);
- effettua configurazione VPN;
- effettua configurazioni VLAN e link aggregation;
- effettua il monitoraggio costante dei parametri significativi della qualità e delle prestazioni della rete;
- coordina ed assicura gli interventi volti al ripristino delle funzionalità del servizio di rete e/o apparati TLC, mediante l'attivazione, a fronte di malfunzionamenti, dei fornitori della manutenzione contrattualizzati dall'Amministrazione;
- modifica regole di instradamento;
- assicura l'effettuazione degli interventi periodici programmati per garantire il buon funzionamento dei sistemi;
- prevede attività di Site Survey per implementazione di nuovi Access Point e verifica di copertura Wi-Fi;
- effettua l'attivazione logica di nuove prese di rete;
- prevede la collaborazione nelle fasi realizzative dei progetti infrastrutturali e/o applicativi che utilizzano l'infrastruttura di rete;
- fornisce un sistema di rendicontazione dei livelli di servizio.

Il servizio comprende anche modifiche di configurazione da apportare agli apparati di rete in quantità massiva, secondo interventi preventivamente concordati.

4.1.4 Servizi di Sviluppo e Integrazione Architetture e Sistemi

Per **Servizi di Sviluppo e Integrazione Architetture e Sistemi** si intende il complesso delle attività operative necessarie alla messa in produzione di nuovi apparati, sistemi e/o ambienti elaborativi e alla loro integrazione nell'Infrastruttura ICT ovvero ad apportare cambiamenti dell'Infrastruttura non riconducibili ad attività di ordinaria gestione e manutenzione. In particolare, il servizio è deputato alle operazioni di improvement dell'architettura dei sistemi, alle attività di assessment, alla migrazione di apparati obsoleti, consolidamento di architetture, virtualizzazione di apparati fisici (e operazioni inverse).

L'infrastruttura può comprendere server distribuiti, il software di base, middleware, DBMS, application server, gli apparati di rete, i dispositivi di storage e backup e comunque tutte le apparecchiature necessarie al corretto funzionamento dei servizi ovunque disposte nell'infrastruttura di proprietà dell'Amministrazione negli stabili di sua proprietà o di terzi ovvero noleggiata da terzi anche in cloud.

Finalità del servizio è la realizzazione, ovvero installazione, test ed avviamento dell'infrastruttura tecnologica, sulla base di Specifiche Tecniche e/o Funzionali prodotte e/o approvate dall'Amministrazione.

Tra le varie attività da eseguire sono compresi:

- il disegno dei sistemi ed il loro dimensionamento;
- l'installazione e l'interconnessione degli apparati di rete, l'integrazione tra i diversi componenti dell'infrastruttura, con contestuale configurazione;
- l'installazione e la configurazione dei sistemi, del firmware, del software di base e del middleware e l'integrazione tra i diversi componenti della fornitura;
- la migrazione di prodotti SW già presenti nel contesto tecnologico dell'Amministrazione ovvero l'aggiornamento alle versioni di recente rilascio di prodotti di mercato;
- la migrazione dei Sistemi Operativi, del middleware, dei server e dei client, per il mantenimento delle versioni ufficialmente supportate e per l'adeguamento dei sistemi alle esigenze di integrazione ed alle compatibilità applicative;
- la dismissione dei vecchi apparati comprensiva delle attività legate alla rottamazione (trasporto compreso) e cancellazione/distruzione dei dati.
- fornire un supporto progettuale e tecnologico centralizzato a tutte le strutture, le piattaforme applicative e tecnologiche dell'Amministrazione;
- incrementare la qualità di erogazione dei servizi forniti dai sistemi dipartimentali tramite la progettazione, l'implementazione e il collaudo di nuove procedure e nuove infrastrutture

tecnologiche;

- progettare, implementare e collaudare nuove soluzioni in ambito infrastruttura, software di base e middleware applicativo, per piattaforme di sviluppo, test e produzione;
- redigere e aggiornare la documentazione specialistica connessa alle attività oggetto della fornitura (sia per attività tecniche di supporto specialistico sia per attività progettuali e di nuova implementazione);
- affiancare e addestrare il Team dedicato alla Conduzione Operativa alla presa in carico delle nuove soluzioni ed architetture implementate per l'Amministrazione;
- predisporre e manutenere i piani di test per tutti i processi di migrazione di servizi su nuove architetture.

Fanno inoltre parte dell'evoluzione dei sistemi le seguenti attività:

- il supporto al capacity management delle infrastrutture informatiche;
- il supporto alla definizione di piani di disponibilità e continuità operativa delle infrastrutture;
- il supporto alla definizione dei processi di service management;
- il supporto alla gestione sistemi per attività che richiedano competenze specifiche;
- il supporto specialistico per gli aspetti tecnologici relativi allo sviluppo applicativo.
- progettare, implementare e collaudare l'evoluzione dell'infrastruttura SAN (predisposizione del piano di deploy della nuova architettura, del piano migrazione e di test, ecc.);
- progettare, implementare e collaudare l'evoluzione delle soluzioni inerenti l'ambiente di posta;
- progettare, implementare e collaudare l'evoluzione dei sistemi di monitoraggio e dei sistemi di reportistica e di datawarehouse per offrire indicatori quantitativi e qualitativi sull'erogazione dei servizi IT;
- progettare, implementare e collaudare l'evoluzione degli application server;
- progettare, implementare e collaudare l'evoluzione dei database server e sistemi software enterprise (ERP, datawarehousing, ecc.);
- progettare, implementare e collaudare l'evoluzione dei sistemi di bilanciamento e dei reverse proxy;
- progettare, implementare e collaudare l'evoluzione dei sistemi di backup/restore dei servizi IT;
- progettare, implementare e collaudare i sistemi e i piani di Business continuity e/o disaster recovery ove richiesto.

Fanno inoltre parte dello sviluppo sistemi le seguenti attività:

- analisi dell'impatto implementativo;
- analisi del rischio;
- analisi dei costi e dei benefici;
- definizione delle modalità di realizzazione;
- definizione dei metodi di collaudo;
- definizione dei metodi di installazione;
- documentazione funzionale;
- procedure operative;
- rilascio della soluzione implementata alla gestione (esercizio).

Al Fornitore può essere richiesta la predisposizione di ambienti prototipali da rendere disponibili per "proof of concept" (POC) o piccole sperimentazioni, con cui verificare le caratteristiche principali della soluzione prima del suo inserimento nell'ambiente operativo, sull'Infrastruttura dell'Amministrazione. Dopo la verifica delle funzionalità del prototipo si eseguono le installazioni nell'ambiente di destinazione finale.

Tutte le attività sopra descritte prevedono l'aggiornamento e/o la predisposizione della documentazione a supporto (dettaglio dell'installazione, delle configurazioni e delle procedure di gestione, di salvataggio della configurazione, script di start/stop dei prodotti, dipendenze con altri server ecc.).

4.1.5 Servizi di Rete: progettazione e sviluppo

I "Servizi di Rete, Progettazione e Sviluppo" sono servizi deputati alle operazioni di improvement dell'architettura di rete, nonché delle attività di verifica ed eliminazione delle obsolescenze eventualmente in essere.

In particolare, il servizio in oggetto:

- Effettua la migrazione degli apparati obsoleti verso nuove architetture, previa collaborazione nell'analisi con i servizi di cybersecurity;
- Si occupa della sostituzione di apparati riportando puntualmente la configurazione esistente sugli apparati di nuova immissione garantendo, quindi, la continuità del servizio;
- Effettua la progettazione di nuove sezioni/sottoreti;
- Effettua la verifica dei carichi di rete eventualmente procedendo alla rimodulazione degli stessi mediante suddivisioni e/o applicando politiche di QoS;
- Provvede all'efficientamento dei percorsi di routing allo scopo di ridurre i tempi di latenza incrementando quindi la velocità di scambio dati ovvero progetta "rotte" alternative al fine di poter garantire la continuità operativa sebbene attraverso instradamenti meno efficienti;

- Supporta l'identificazione delle possibilità di comunicazioni non cablata (wireless) quali punto-punto, WLAN, satellite, identificando le diverse caratteristiche e l'applicabilità a diverse necessità aziendali di trasmissione;
- Progetta collegamenti non cablati punto-punto, in termini di pianificazione geografica, calcolo di perdita del percorso, verifica delle ellissi di Fresnel e predisponendo i test da effettuare per valutare il percorso;
- Supporta l'identificazione di collegamenti basati su satellite, verificando diversi parametri e pianificando il tipo di trasferimento dati che può utilizzare tali collegamenti sia di norma sia come soluzione di ripiego;
- Pianifica, supervisiona la realizzazione ed effettua i test dei collegamenti digitali a infrarossi tra reti diverse;
- Supporta la pianificazione di diverse implementazioni della 'convergenza digitale', dal "data streaming" (sia voce che video), al VoIP (non solo a due vie ma anche conferenze audio-video), proponendo architetture, protocolli e schemi differenti;
- Supporta la pianificazione, supervisiona la realizzazione ed effettua i test di accettazione dei sistemi digitali di trasmissione, sotto forma di nuova "Radio digitale" e "TV digitale" (DRM, DAB);
- Raccoglie dati campione e li utilizza per costruire un modello pilota significativo del nuovo sistema. Rende più solido il modello generale tramite diverse sessioni di simulazione in cui i responsabili aziendali, i responsabili di processo e gli utenti operativi del sistema informativo possono comprendere e approvare pienamente le modalità di esercizio del sistema finale addivenendo quindi ad una progettazione esecutiva;
- Produce documenti e rapporti scritti di alta qualità, in cui vengono descritti argomenti organizzativi e/o tecnici con uno stile chiaro e conciso;
- Collabora con il personale IT dell'Amministrazione sia per il collaudo (nuovo modulo singolo o intero sistema) che per l'estrazione, la trasformazione e il caricamento dei dati;
- Conduce le simulazioni finali con dati reali e i test di accettazione, anche per conto dell'Amministrazione se supportato da opportuna delega;
- In conformità agli accordi presi supporta l'azienda cliente durante la fase iniziale di utilizzo del nuovo sistema e nella misurazione dei suoi vantaggi attraverso eventuali revisioni post-implementazione;

4.1.6 Servizi di Service e Performance Management

È compito del Fornitore assicurare che i servizi di gestione IT siano organizzati e strutturati secondo un approccio process-driven, in cui la complessa struttura organizzativa/operativa dei servizi sia scomposta in una serie di processi integrati e correlati tra loro in accordo con le best practices ITIL, con l'obiettivo di:

- migliorare la qualità dei servizi IT;
- ridurre i costi di erogazione dei servizi;
- allineare i servizi IT con i bisogni correnti e futuri del business e dei clienti.

Nel caso in cui l'Amministrazione abbia già definito a priori la strutturazione dei processi di gestione secondo le best practices ITIL, il Fornitore dovrà erogare i servizi adottando i processi già definiti; nel caso in cui, invece, l'Amministrazione non abbia definito, in tutto o in parte, la strutturazione dei processi di gestione, il Fornitore dovrà, su richiesta e in accordo con l'Amministrazione, proporre e adottare un'adeguata strutturazione dei processi previsti.

Si ritiene utile sottolineare, in maniera più puntuale, il valore aggiunto atteso dall'operatività del Fornitore nell'ambito di alcuni tra i processi più significativi per l'evoluzione del modello di erogazione dei servizi.

Si precisa che non tutti i processi per cui ci si attende un impegno dal Fornitore sono di seguito elencati, fermo restando che il Fornitore deve supportare l'Amministrazione effettuando tutte le attività di competenza, sulla base di quanto stabilito nelle procedure operative che saranno rese disponibili o implementate nel corso della gestione contrattuale.

4.1.6.1 Gestione delle Richieste e delle Segnalazioni

In coerenza con i processi in uso presso l'Amministrazione, è richiesto che il Fornitore utilizzi gli strumenti resi disponibili dall'Amministrazione per tracciare le attività a carattere operativo nonché le richieste di informazioni e di segnalazione di disservizio.

In particolare, il Fornitore stesso deve:

- alimentare gli strumenti di tracciatura;
- effettuare la ricezione e la presa in carico delle richieste nei tempi concordati;
- aggiornare le informazioni di ciascun ticket con l'effettivo stato/andamento delle attività;
- fornire una stima dei tempi di esecuzione e una diagnosi relativa all'intervento da effettuare;
- effettuare la chiusura dei ticket;
- gestire, per quanto di competenza, gli interventi dei fornitori terzi.

4.1.6.2 Supporto al Processo di Incident e Problem Management

Al fine di garantire la corretta fruizione dei servizi da parte dell'utenza di riferimento, il Fornitore è responsabile della gestione di tutti i casi in cui sia rilevabile una interruzione o un degrado nella fruizione del servizio. Tale responsabilità è indipendente dalla causa dell'interruzione/degrado, che può essere legato al software, all'hardware e relativo firmware sistemi e/o apparati di rete.

Il Fornitore è tenuto ad effettuare le attività necessarie al ripristino del servizio all'utenza di riferimento entro i tempi massimi prefissati, anche attraverso l'attivazione delle procedure di escalation concordate.

Tali procedure tengono conto del livello di gravità del malfunzionamento e dell'impatto dello stesso sull'operatività dell'utenza.

L'attività di gestione dei malfunzionamenti deve essere sia proattiva, ossia rivolta alla prevenzione, sia reattiva, ossia rivolta alla gestione ed infine alla risoluzione di tutti gli eventi che comportano l'interruzione o il degrado nella fruizione del servizio.

Pertanto, tra le attività richieste si includono:

- l'identificazione del malfunzionamento, la sua documentazione, la gestione delle comunicazioni e dell'escalation e la sua risoluzione, anche attraverso l'attività di terze parti;
- l'analisi del verificarsi di problemi ripetitivi. I risultati dell'analisi sono inseriti nella knowledge base e sugli elementi interessati sono eseguiti controlli approfonditi atti ad individuare e risolvere problemi di tipo strutturale, secondo quanto concordato con la l'Amministrazione nell'ambito del processo di Problem management;
- l'analisi delle informazioni derivanti dall'esecuzione delle attività di verifica di performance dei sistemi, tenendo conto delle informazioni provenienti dai sistemi di monitoraggio.

In ultimo, è responsabilità del Fornitore il salvataggio dei dati ai fini dell'analisi di incidenti di sicurezza. Il Fornitore deve assicurarsi che i sistemi, anche non direttamente gestiti, inviino al sistema di Log Management le informazioni utili alle attività di analisi, attivando - in caso negativo - le procedure concordate con l'Amministrazione.

È richiesto, infatti, che sia effettuata la conservazione di tutti i log di auditing relativi a web server, application server, apparati di sicurezza e quanto altro possa essere necessario alla ricostruzione di comportamenti insidiosi e per l'individuazione di possibili responsabilità penali e civili conseguenti a condotte illecite. Tali log devono essere mantenuti in linea per il periodo concordato con l'Amministrazione. Su tali log l'Amministrazione si riserva di richiedere al team di effettuare ricerche ed elaborazioni statistiche puntuali.

Si precisa che i dati da raccogliere e da salvare ai fini dell'indagine sugli incidenti di sicurezza saranno concordati successivamente all'avvio della fornitura.

4.1.6.3 Supporto al Processo di Change e Release & Deployment Management

Al fine di garantire il corretto funzionamento, lo sviluppo e l'evoluzione dell'infrastruttura ICT dell'Amministrazione, il Fornitore è responsabile della pianificazione, dell'attuazione, del tracciamento e della verifica dei cambiamenti dell'hardware, del firmware, dell'evoluzione dei sistemi operativi, dei prodotti programma/middleware, dei prodotti applicativi e delle relative correzioni coerentemente con i processi di Change Management e Release & Deployment Management.

4.1.6.4 Supporto al Processo di Service Asset & Configuration Management

Il Fornitore deve garantire il costante, accurato e continuo allineamento delle basi dati del CMDB; nel caso in cui tali aggiornamenti non possano essere eseguiti automaticamente, il Fornitore deve procedere con l'aggiornamento manuale. Si precisa che l'aggiornamento del CMDB è prevalentemente effettuato in automatico attraverso prodotti di scansione le cui politiche sono definite dall'Amministrazione e sono supportati da script/procedure automatiche che potrebbero essere realizzate da terzi.

Si precisa che i processi e le procedure operative sono oggetto di revisione e miglioramento continuo, pertanto, nel periodo contrattuale, le modalità indicate potrebbero variare. In ogni caso i fornitori sono obbligati a seguire qualsiasi variazione dei processi e delle procedure operative che l'Amministrazione indicherà.

L'aggiornamento costante e accurato della baseline, in particolare del CMDB, è ritenuto il nucleo fondamentale sui cui si fondano:

- i processi già in uso nonché i processi che potrebbero essere eventualmente adottati ed implementati nel corso della durata contrattuale;
- il patrimonio informativo relativo alla consistenza e alla configurazione dell'infrastruttura ICT dell'Amministrazione;
- la valutazione di eventuali impatti per i servizi di business dell'Amministrazione a fronte di evoluzioni, cambiamenti di carattere infrastrutturale;
- le analisi volte all'integrazione e/o all'introduzione di nuovi servizi a supporto dell'attività istituzionale dell'Amministrazione;
- la rilevazione e la misurazione della qualità del servizio all'utenza di riferimento.

Si ritiene utile precisare che, alla data di inizio attività, il CMDB potrebbe non essere completo di tutte le informazioni previste sia in termini di CI che di attributi previsti.
Ad inizio fornitura, è richiesto al Fornitore un assessment sulla consistenza e coerenza dei dati di Asset & Configuration e delle relazioni tra gli stessi.

4.1.6.5 Supporto al Processo Capacity Management

Il Fornitore è responsabile dell'esecuzione delle attività operative a supporto del processo di Capacity Management. Pertanto, è responsabile della raccolta dei dati, dell'analisi periodica dello stato di salute dell'Infrastruttura ICT affidata in gestione, dell'analisi dei trend di carico e della produzione di reportistica che mostri la situazione riassuntiva di ciascun sistema e che ne evidenzi eventuali criticità o necessità di evoluzione.
Si precisa che l'Amministrazione si riserva di richiedere la produzione di ulteriore reportistica il cui contenuto, formato e periodicità è concordato ad inizio fornitura ed eventualmente rivisto, nel corso della durata dei servizi, ai fini della predisposizione del Piano della Capacità.
Il Fornitore, nell'erogazione del servizio, può utilizzare gli strumenti e i prodotti resi disponibili dall'Amministrazione ovvero può utilizzare script e/o le funzionalità native del software di sistema.

4.1.6.6 ServiceDesk Sistemistico

Nell'ambito dei processi strutturati di Service Management, il Fornitore deve prevedere (se richiesto dall'Amministrazione) una funzione di Service Desk Sistemistico, che agisca come punto di contatto tra i referenti informatici dell'Amministrazione e l'IT Service Management, per gestire incidenti e richieste degli utenti e fornire un'interfaccia per gli altri processi, quali Change, Problem, Configuration, Release, ecc., gestendo tutto il ciclo di vita dell'incidente o della service request.
Gli elementi distintivi della funzione di Service Desk Sistemistico sono:

- prima diagnosi e tentativo di risoluzione delle segnalazioni/richieste al primo livello, anche attraverso l'utilizzo delle informazioni presenti nella Knowledge base;
- classificazione degli incidenti o richieste, attraverso modalità obiettive per classificare gli incidenti in modo che siano assegnati opportunamente;
- assegnazione della priorità, attraverso modalità obiettive per l'assegnamento della priorità di un incidente (ad esempio attraverso una matrice di impatto/urgenza);
- assegnazione degli incidenti/richieste, automatizzando il più possibile il routing dei casi in base al workload e alle competenze di ogni tecnico, in modo da ottimizzare le risorse;
- assegnazione a gruppi esterni, attraverso accordi con Fornitori terzi responsabili di specifiche attività.

La funzione di service desk sistemistico è relativa alle problematiche di system management descritte nel presente Capitolato Tecnico e ha come principale utenza di riferimento i referenti informatici dell'Amministrazione. Non è compresa l'assistenza agli utenti per problematiche che esulano dal contesto suddetto, quali ad esempio supporto alla gestione delle postazioni di lavoro o supporto all'utilizzo delle funzioni applicative.

4.2 Lotto 2 – Sicurezza Informatica

Il Lotto 2 annovera al suo interno un insieme di servizi e attività inerenti alla sicurezza informatica, inclusi i servizi di monitoraggio in tempo reale di eventi di sicurezza, la progettazione e lo sviluppo di soluzioni atte a garantire il livello adeguato di sicurezza rispetto al contesto IT aziendale, incluso il governo degli aspetti di sicurezza informatica nel loro complesso. Considerata la complessità e soprattutto la criticità dei servizi e delle attività ricomprese nel presente Lotto, in stretta sinergia con quelle di ambito più prettamente sistemistico e infrastrutturale, è necessario e fondamentale precisare che deve essere garantita la massima disponibilità al fine di una piena e stretta collaborazione con le figure professionali dell'IT, interno all'Ente, del Fornitore dei servizi di System Management o di eventuali altre figure professionali che operano per conto dell'Amministrazione.
Di seguito l'elenco dei Servizi inerenti il presente Lotto.

4.2.1 Servizio di Monitoraggio in tempo reale di eventi di sicurezza (SOC)

Il **"Servizio di Monitoraggio in tempo reale di eventi di sicurezza**" comprende tutte le attività di monitoraggio dell'infrastruttura IT dell'Amministrazione al fine di rilevare e gestire in tempo reale gli eventi relativi alla sicurezza informatica. Il servizio è erogato dal **SOC – Security Operation Center.**

In particolare, il SOC effettua il monitoraggio degli eventi dell'insieme delle risorse IT dell'organizzazione: server, endpoint, reti ed apparati di rete, software di sistema, applicazioni, utenze, ecc… al fine di rilevare falle di sicurezza, tentativi di intrusione o di attacco ed ogni altra tipologia di attività sospetta, quale a puro titolo esemplificativo e non esaustivo: attività compiuta da malware, sfruttamento di vulnerabilità anche di tipo Zero-Day, Targeted and Advanced Persistent Threat (APT), Privilege Escalation, movimenti laterali, attacchi ad applicazioni, frodi informatiche, Denial of Service (DDos, DoS), ecc…

Pertanto, il Fornitore deve disporre del servizio SOC all'interno del proprio Centro Servizi per l'Operatività da Remoto, da mettere a disposizione delle Amministrazioni che facciano richiesta di servizi da erogare mediante tale modalità operativa.

La lingua di riferimento per l'erogazione dei servizi deve essere l'italiano.

Da tale Centro, attraverso l'utilizzo degli opportuni strumenti e mediante l'impiego di personale specializzato, il Fornitore dovrà avere la possibilità di operare in collegamento con i sistemi dell'Amministrazione per effettuare tutte le attività previste dal servizio, ad esempio:

- controllare costantemente (sulla base delle finestre di erogazione del Servizio concordate con l'Amministrazione) il sistema di monitoraggio per poter intervenire immediatamente in caso di attivazione di allarmi;

- investigare e definire la natura delle anomalie rilevate e attribuirle ad eventuali minacce e problemi di sicurezza;
- svolgere un primo livello tecnico in ambito sicurezza rilevando, investigando e assegnando priorità alle minacce, identificando gli eventuali sistemi ed utenti impattati, mettendo in atto azioni ed attività al fine di mitigare o annullare l'impatto di minacce o incidenti;
- ricevere, qualificare e gestire richieste di assistenza che potranno generarsi dal sistema di monitoraggio o tramite chiamata sia di personale dell'Amministrazione, sia di Help-desk di società terze che forniscono servizi di manutenzione su sistemi hardware e software utilizzati dall'Amministrazione stessa;
- collaborare in sinergia con il NOC ed il personale IT dell'Amministrazione;
- contattare ed informare costantemente il personale dell'Amministrazione qualora ve ne sia la necessità (sulla base di procedure concordate con l'Amministrazione);
- gestire in autonomia gli allarmi, contattando eventualmente il personale di fornitori terzi (sulla base di procedure concordate con l'Amministrazione);
- effettuare gestione, verifica, analisi, correlazione, storicizzazione e conservazione a norma delle informazioni raccolte nei file di log delle infrastrutture di sicurezza e di rete e degli allarmi generati;
- essere un single point of contact attivo e raggiungibile (sulla base delle finestre di erogazione del Servizio concordate con l'Amministrazione) tramite numero di telefono ed e-mail;
- provvedere ad inviare periodicamente (con cadenza concordata con il personale dell'Amministrazione), tramite comunicazione e-mail, un riepilogo degli allarmi attivati e risolti e di eventuali criticità in atto;
- generare Report di Sicurezza con i dati collegati alle attività di gestione della sicurezza; periodicità e tipologia dei report generati verranno concordati con l'Amministrazione.
-

Tutto il personale del SOC deve essere in grado di prendere in carico tutte le attività relative all'infrastruttura dell'Amministrazione, al fine di garantire una continuità di servizio al Committente; a tal fine, pertanto, il Fornitore deve adeguatamente formare ed istruire il personale del SOC relativamente all'infrastruttura ICT dell'Amministrazione stessa.

Il SOC del Fornitore deve rispettare inoltre le seguenti regole:

- la connessione telematica tra il Centro Servizi e le sedi dell'Amministrazione deve essere realizzata attraverso canale dedicato punto-punto a costo del Fornitore. Nessun onere potrà essere ascritto all'Amministrazione. Si intende ricompresa nella

connessione anche la dotazione degli apparati di networking ed ogni altra dotazione necessaria, inclusi i cablaggi dalla terminazione di rete del Provider del collegamento ai locali CED dell'Amministrazione qualora se ne presentasse la necessità. La soluzione deve garantire adeguate prestazioni e affidabilità in caso di malfunzionamento di uno dei componenti dell'infrastruttura;

- il Fornitore deve predisporre presso il proprio Centro Servizi una soluzione tecnologica avente prestazioni e affidabilità adeguate anche in caso di malfunzionamento di uno dei componenti dell'infrastruttura, tale in sostanza a garantire connettività ed operatività ai gruppi impegnati nell'erogazione dei servizi.

  In particolare:

  a) **Un punto di accesso alla rete dell'Amministrazione**. In particolare, il Fornitore dovrà garantire che gli accessi alla rete ed ai sistemi dell'Amministrazione avvengano esclusivamente dal personale identificato mediante **utenze nominative** autorizzate dal proprio sistema di gestione degli accessi. Per quanto riguarda l'accesso ai sistemi di proprietà dell'Amministrazione, il Fornitore dovrà utilizzare utenze nominative nelle modalità concordate con l'Amministrazione, compatibilmente alle specifiche tecnologie e sempre in conformità con quanto previsto dal provvedimento del Garante in materia di accesso degli amministratori di sistema. Non è richiesta la realizzazione di un sistema di Single Sign On che consenta l'uso delle medesime credenziali nei due domini (Sistemi del Centro servizi e Sistemi dell'Amministrazione);

  b) **Autenticazione e profilazione delle utenze.** Il processo di autenticazione e profilazione dell'utente è riferito al punto di accesso alla rete dell'Amministrazione;

  c) **Tracciatura degli accessi ai sistemi**. In ottemperanza al provvedimento del Garante per la protezione dei dati personali, in materia di accessi degli amministratori di sistema, dovrà essere possibile registrare gli accessi e le attività eseguite dal personale del SOC sul sistema per la gestione degli accessi del Centro Servizi, ad es. login, ssh, desktop remoto. Per quanto riguarda la registrazione degli accessi e delle attività degli Amministratori su ciascun sistema di proprietà dell'Amministrazione, le modalità saranno concordate con l'Amministrazione stessa;

d) **Conservazione dei Log**. È richiesta la conservazione per almeno un anno dei log del sistema di gestione degli accessi, utilizzato per l'accesso alla rete ed ai sistemi dell'Amministrazione. Lo strumento di conservazione e di gestione dei log deve essere predisposto dal Centro servizi del Fornitore, senza alcun onere per l'Amministrazione, che si riserva di richiedere tali log con frequenza periodica in base alle procedure concordate con il Fornitore stesso.

- il Fornitore deve garantire la sicurezza del collegamento e la riservatezza dei sistemi e delle informazioni attraverso la formalizzazione e l'applicazione di procedure e politiche di sicurezza da adottare al proprio interno, adeguate ai requisiti stabiliti. Infatti, è responsabilità del Fornitore assicurare che il Centro Servizi, le infrastrutture in esso ospitate, le informazioni gestite e le transazioni da e verso la rete dell'Amministrazione siano protette mediante l'adozione di adeguati sistemi e metodologie definite utilizzando come riferimento le norme della serie ISO/IEC 27001. In particolare, nell'esecuzione dei servizi, il Fornitore deve garantire l'evoluzione, la manutenzione e l'adeguamento tecnologico dei sistemi, delle reti e di tutti gli strumenti impiegati presso il Centro Servizi che si rendano necessarie a soddisfare i requisiti di sicurezza stabiliti, nonché l'aggiornamento delle politiche di sicurezza e delle contromisure attuate e la risoluzione reattiva o proattiva di incidenti di sicurezza.

In considerazione dell'esigenza di garantire il massimo grado di copertura di tutti gli aspetti di sicurezza, si richiede la redazione di un Piano della Sicurezza in conformità a best practice e/o a standard internazionali, secondo quanto concordato con l'Amministrazione.

Nella tabella seguente si riportano alcuni requisiti da intendersi come minimi e imprescindibili:

Categoria	Requisiti Minimi
Sicurezza delle reti	Il punto di accesso alla rete dell'Amministrazione deve essere adeguatamente protetto mediante sistemi firewall che operino secondo modalità note come "Stateful Inspection". Devono essere utilizzati sistemi/meccanismi di "Intrusion Detection and Prevention" che analizzino il traffico in entrata ed in uscita dalla rete dell'Amministrazione.
Riservatezza dei dati e delle trasmissioni	Deve essere garantita la riservatezza di tutti i dati gestiti.

Categoria	Requisiti Minimi
Integrità dei dati	Devono essere adottati antivirus centralizzati ad aggiornamento periodico, che analizzino e bonifichino gli eventuali codici malevoli. Devono essere adottati antivirus su tutte le postazioni utilizzate dal personale del Fornitore e collegate con la rete dell'Amministrazione. Tali postazioni devono soddisfare lo standard per le postazioni di lavoro previste per l'Amministrazione
Auditing e vulnerability assessment	Devono essere registrati tutti gli eventi telematici che hanno impatto sui sistemi, effettuati dal Centro servizi del Fornitore, permettendo la ricostruzione di comportamenti insidiosi e/o malevoli e l'individuazione di possibili responsabilità penali e civili conseguenti condotte illecite. Tali registrazioni dovranno essere effettuate e conservate sui sistemi del centro servizi che consentiranno l'accesso alla rete dell'Amministrazione, ovvero sui sistemi dell'Amministrazione, secondo le modalità concordate con l'Amministrazione.
Amministrazione accessi	Devono essere adottati adeguati processi di Amministrazione degli accessi (fisici e logici) effettuati nel Centro servizi che prevedano l'identificazione delle diverse categorie di utenti, la definizione dei corrispondenti profili di autorizzazione e delle modalità di rilascio dell'accesso.

Il Fornitore deve adottare una soluzione tecnico-organizzativa atta a garantire la continuità dell'erogazione dei servizi anche in caso di evento disastroso e/o di interruzione della connessione tra il Centro Servizi e la rete dell'Amministrazione, e il rispetto dei requisiti di qualità contrattuali.
Il Fornitore deve erogare il servizio secondo una delle due seguenti modalità, a discrezione dall'Amministrazione sulla base delle proprie caratteristiche e risorse:

- mettendo a disposizione una propria piattaforma di monitoraggio degli eventi di sicurezza dotata di appositi moduli di detection, agenti o dispositivi da installare presso i sistemi dell'Amministrazione, in grado di raccogliere le informazioni atte ad individuare gli scenari di rischio ed attacco come sopra indicati;
- utilizzando le piattaforme già eventualmente in utilizzo presso l'Amministrazione committente comprese quelle di asset management, CMDB, e di ticketing per tracciare le attività a carattere operativo nonché le richieste di informazioni e di segnalazione di incidente.

Nella prima modalità, il Fornitore dovrà mettere a disposizione una piattaforma web che permetta all'Amministrazione di accedere ad apposite dashboard configurate opportunamente per consentire la consultazione delle anomalie rilevate, degli allarmi attivati e lo storico degli stessi, l'accesso a tutte

le informazioni inerenti le diverse fasi di gestione degli incidenti ed alle informazioni generate dai moduli di detection.

Gli eventi generati dalla piattaforma di monitoraggio e dai moduli di detection dovranno essere collezionati in appositi log e messi a disposizione dell'Amministrazione, su richiesta.

La raccolta e la cifratura dei log effettuata dalla piattaforma di monitoraggio deve garantire la catena di custodia, l'apposizione dei time stamp di ricezione da parte di ogni componente, il formato non modificabile del log con o senza la conservazione del raw event, l'hashing effettuato nel database per impedire la cancellazione selettiva dei log, la presenza di audit log di accesso alla piattaforma, nonché la compressione e la cifratura degli archivi.

All'attivazione del contratto saranno definiti e formalizzati i processi da applicare alla gestione degli allarmi e degli incidenti di sicurezza con specifico riferimento agli aspetti di comunicazione, responsabilità ed escalation tra il Fornitore, l'Amministrazione ed eventuali altri terzi coinvolti nella reazione e gestione (es. fornitori applicativi).

Sarà altresì compito del servizio **SOC** la rilevazione dei livelli di sicurezza (antivirus e allineamento delle configurazioni alle policy di sicurezza dei sistemi dell'Amministrazione). Il servizio è anche deputato all'analisi e verifica dei livelli di sicurezza complessiva dell'architettura e della valutazione di eventuali azioni di perfezionamento della security stessa.

Può essere coinvolto fattivamente anche nella progettazione di contromisure ad attacchi e tentativi di intrusione, inserimento e progettazione di nuove e più efficaci regole di protezione nonché l'esecuzione di test e simulazioni di attacco ed intrusione (VA/PT), necessari anche a valutare le corrette configurazioni e correlazioni oltre ai tempi di risposta.

In particolare, il servizio in oggetto ha in carico le seguenti attività:

- collabora col personale dell'Amministrazione e del NOC per fornire informazioni di dettaglio su aspetti di sicurezza per apparati di rete e sistemi obsoleti e per le nuove architetture (patching, hardening, protocolli da disattivare, etc);
- verifica i connettori per la raccolta dei log e delle correlazioni per generare allarmi, controllando il corretto funzionamento e le corrette informazioni a fronte dell'introduzione di nuovi servizi e architetture;
- effettua le attività di assessment degli apparati di monitoraggio per garantire che la raccolta delle informazioni sia sempre attiva ed efficace a garanzia di allarmi in real-time.

4.2.2 Servizio di Conduzione Operativa di Apparati e Sistemi di Sicurezza

È richiesto al Fornitore di erogare servizi di sicurezza in una modalità atta a gestire apparati di sicurezza informatica in produzione presso l'Amministrazione.

In particolare, i servizi previsti, a titolo esemplificativo e non esaustivo, sono:

- Servizio di gestione dei dispositivi di sicurezza perimetrale: il servizio consente di attuare la politica per la sicurezza sui dispositivi di difesa perimetrale dell'Amministrazione (per es. Firewall, VPN);
- Servizi di Next Generation firewall;
- Servizi di Web Application firewall;
- Servizio di Content Filtering. Il servizio permette di ottimizzare l'uso delle risorse infrastrutturali, quali la capacità di banda verso Internet od il sistema di posta elettronica, controllando l'ammissibilità dei contenuti in transito rispetto alle politiche di sicurezza definite;
- Servizio di Content Security (antivirus, antimalware, anti-ransomware). Il servizio provvede ad una gestione efficace delle contromisure atte a contrastare la diffusione dei codici malevoli, quali virus o worm su sistemi sia client (postazione di lavoro) che server;
- Servizio IDS (Intrusion Detection System) / IPS (Intrusion Prevention System): il servizio fornisce la valutazione di eventi, situazioni anomale od allarmi che possono rappresentare una minaccia per la sicurezza dell'infrastruttura attraverso opportuni strumenti di rilevazione;
- Servizio SIEM: il servizio fornisce un raggruppamento di vari sistemi di sicurezza (log collection, analisi dei log, correlazione di eventi, funzionalità di alerting e di archivio) in un ambiente unitario al fine di valutare le minacce e di gestire i rischi di sicurezza;
- Servizio SOAR - Security Orchestration, Automation, and Response: il servizio fornisce un insieme di soluzioni software che permettono di gestire in modo coordinato i processi di gestione delle vulnerabilità, di risposta agli incidenti e di automazione delle attività di sicurezza;
- Servizio di telemetria, xDR/EDR/NDR: server, mail, endpoint, reti detection and response;
- Servizio di Threat Sharing per la gestione degli Indici di Compromissione (IoC) e per la condivisione degli stessi con il Fornitore e con altre Organizzazioni; all'integrazione con i sistemi di sicurezza dell'amministrazione.

Per **"Conduzione Operativa Apparati e Sistemi di Sicurezza"** si intende il complesso delle attività riconducibili all'ordinaria gestione e manutenzione dell'infrastruttura di sicurezza informatica garantendone il funzionamento e l'efficienza, la copia e backup delle configurazioni degli apparati in aderenza a quanto previsto dall'apposito piano, qualora esistente. Il Fornitore deve garantire la continuità di esercizio degli apparati e sistemi di sicurezza anche a fronte di problemi particolarmente complessi.

Gli obiettivi della conduzione operativa sono:

- garantire la disponibilità dei sistemi e l'esecuzione delle attività schedulate;
- assicurare un continuo controllo sullo stato dei sistemi e dei collegamenti, individuare criticità o malfunzionamenti ed intraprendere le azioni necessarie;
- garantire l'efficienza dei sistemi rispetto all'utilizzo delle risorse hardware e software;
- controllare l'impatto sulla tecnologia esistente e garantire l'adeguamento degli ambienti elaborativi a fronte dell'immissione in esercizio di modifiche correttive e/o evolutive di applicazioni e sistemi esistenti;
- monitorare e verificare i consumi effettivi degli eventuali servizi in cloud.

4.2.3 Servizio di Vulnerability Assessment

È richiesto al Fornitore la pianificazione e l'esecuzione dei test di vulnerabilità concordati con l'Amministrazione e da essa supervisionati. I test verranno effettuati con cadenza periodica al fine di verificare il livello di efficacia delle Politiche di Sicurezza. In tale ambito sarà richiesto al Fornitore di contribuire fattivamente all'implementazione delle eventuali azioni correttive per la rimozione delle criticità individuate, in collaborazione coi tecnici del IT dell'Amministrazione, sia per la parte di controllo e revisione delle politiche di configurazione, sia per interventi specifici di host hardening sui sistemi server e storage.

Nelle variazioni delle Politiche di Sicurezza, i nuovi requisiti o le modifiche dei requisiti esistenti saranno implementati mediante un processo specifico che prevede la progettazione, l'implementazione e messa in esercizio da parte del Fornitore dei cambiamenti alle infrastrutture tecnologiche e/o alle modalità di erogazione dei servizi che si rendessero necessarie.

Il Fornitore si impegna a supportare l'Amministrazione o terzi da essa designati ad implementare le politiche di sicurezza.

4.2.4 Servizio di Vulnerability Management

Il Fornitore deve erogare, per le Amministrazioni che necessitano di un monitoraggio continuo, il servizio di Vulnerability Management le cui modalità di erogazione sono da concordare con le medesime.

Per l'Amministrazione già dotata di un sistema di Vulnerability Management che scansiona sistemi (server, apparati di rete, ecc…), applicazioni, oltre alle infrastrutture containerizzate, si richiede al Fornitore il supporto per la gestione della piattaforma e la predisposizione della reportistica con cadenza periodica sia di alto livello (Executive Summary) che di quella tecnica in cui si evidenzi le eventuali azioni correttive e la rimozione delle criticità da inoltrare alle strutture interne di

competenza, individuate assieme all'amministrazione coinvolta.

Differentemente l'Amministrazione può richiedere al Fornitore la fornitura di una piattaforma "as a service" dotata di appositi moduli di detection, agenti o dispositivi da installare presso i sistemi dell'Amministrazione, con la collaborazione del Fornitore, in grado di raccogliere le informazioni e consentire la produzione dei report nelle stesse modalità sopra riportate.

4.2.5 Attività di Penetration Test

È richiesto al Fornitore di eseguire attività di penetration testing (PT) al fine di rilevare possibili vulnerabilità di tutte le componenti di un sistema informatico dell'Amministrazione e procedere conseguentemente con una pianificazione dei rimedi e relativo innalzamento del livello di sicurezza.

Si riportano alcuni esempi di penetration test, a puro titolo esemplificativo e non esaustivo, che potranno essere richiesti: penetration test esterni, penetration test interni, penetration test mirati, penetration test delle applicazioni web, penetration test VPN, penetration test reti WiFi.

Le modalità dei PT richiesti seguono la classica categorizzazione di black-box, gray-box, white-box in cui al pen-tester viene concessa la minima conoscenza dei sistemi, reti e applicazioni di destinazione fino ad un alto livello di conoscenza che comprende tutta la documentazione che descrive un'applicazione ed il suo ciclo di vita oltre all'accesso con profili diversificati ove presenti.

Per le Amministrazioni in cui sono applicate politiche sullo sviluppo sicuro delle applicazioni, i test dovranno verificare che quanto indicato nella checklist e dichiarato dalla struttura che ha in carico l'applicazione corrisponda a quanto realmente riscontrato.

A fronte di PT negativi sono previsti i relativi re-check.

4.2.6 Servizi di Application Security Testing

Per le applicazioni di un'Amministrazione nell'intero ciclo di vita, SDLC (Software Development Life Cycle), e a garanzia del principio generale di "sicurezza e privacy by design e by default", si rende necessario il test del codice di tipo DAST (Dynamic Application Security Test) e SAST (Static Application Security Test), nonché SCA (Software Composition Analysis) per testare applicativi legacy che utilizzano codici open source o di terze parti.

Tale servizio è generalmente demandato a un fornitore terzo a cui sono state commissionate le applicazioni con il rilascio di specifici report da analizzare e verificare con il supporto dei servizi inclusi in questo capitolato.

Le Amministrazioni potranno richiedere al Fornitore un servizio di analisi del codice sia di applicazioni web-based che mobile, applicazioni Agile e "containerizzate" il cui software (o parte di esso) è di loro proprietà o in riuso, collocate on-premise o in cloud.

4.2.7 Servizi di Incident Response and Remediation

Il Fornitore deve erogare servizi di risposta e remediation degli incidenti di sicurezza.

Questo servizio ha lo scopo di:

- valutare e gestire il rischio associato alle minacce di tipo informatico;
- utilizzare strumenti tecnologici e competenze per affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza.

Il personale deputato al servizio di Incident Response, il secondo livello tecnico in ambito sicurezza informatica, di concerto al team IT (system e/o client), eseguono le necessarie attività per la risoluzione delle anomalie e nell'esecuzione di tutte le azioni necessarie al contenimento degli eventi riferiti dall'incidente nel più breve tempo possibile onde evitare la diffusione su altri sistemi, oltre al supporto e alla verifica per il ripristino degli eventuali servizi compromessi.

Tra le azioni di competenza del Team figurano a puro titolo esemplificativo e non esaustivo:

- identificazione dei sistemi compromessi;
- analisi delle minacce e classificazione del livello di impatto;
- identificazione dei soggetti da coinvolgere ed eventuale apertura di uno specifico ticket o chiamata diretta a soggetti terzi, secondo le modalità concordate con l'organizzazione;
- definire e adottare contromisure al fine di mitigare le conseguenze dell'incidente, neutralizzare le minacce, prevenire ulteriori accessi o danni in modo concordato con l'Amministrazione e coinvolgendo gli altri soggetti deputati alla gestione dell'incidente;
- definire e adottare contromisure di protezione della rete per prevenire ulteriore diffusione di malware in modo concordato con l'Amministrazione e coinvolgendo gli altri soggetti deputati alla gestione dell'incidente;
- isolare i sistemi compromessi (ad esempio da malware) con gli opportuni strumenti e garantire la gestione corretta dell'analisi forense.

Inoltre, dovrà svolgere un'attività di supporto ai processi di gestione dell'incidente da parte dell'Amministrazione, come ad esempio supporto alla redazione dell'incident report e all'enforcement tecnologico in funzione delle informazioni acquisite durante tutte le fasi di gestione dell'incidente.

4.2.8 Servizio di User and entity behavior analytics (UEBA)

Il Fornitore deve erogare il Servizio di User and Entity Behavior Analytics (UEBA), che consiste nell'utilizzo di piattaforme ed algoritmi, nonché di intelligenza artificiale, al fine di identificare in

modo automatico schemi di comportamento anomalo di utenti o di altre componenti dell'infrastruttura IT. Gli algoritmi a disposizione della piattaforma vengono addestrati a riconoscere gli schemi di comportamento abitualmente adottati dagli utenti e da altre entità in modo tale da riconoscere attività anomale e potenziali malintenzionati.

4.2.9 Reportistica

Il Fornitore predispone Report Tecnici periodici che indichino lo stato generale in ambito sicurezza dell'infrastruttura dell'organizzazione che lo ha richiesto.

Sono altresì richiesti Executive Report (Executive Summary) per fornire informazioni di tipo statistico da presentare ai vertici dell'organizzazione con periodicità concordata. Tali report considerano rischi, incidenti, malware, ed altro, rilevati in un certo periodo, prendendo in considerazione i KPI (Key Performance Indicator) definiti dall'Amministrazione e necessari al monitoraggio della sicurezza informatica.

4.2.10 Servizio di Digital Forensic

Il Fornitore fornisce figure professionali certificate e competenti per l'implementazione dei processi che consentano all'Amministrazione di organizzare e trattare in modo opportuno le informazioni presenti nei diversi dispositivi aziendali per la propria tutela a fronte di una richiesta di presentazione di prove in tribunale o funzionali a diverse tipologie di indagini specifiche. Oltre ai servizi di Analisi Forense eseguiti per motivi legali su copie dei dati e dei sistemi. L'Analisi delle prove deve essere effettuata con i software più utilizzati dalle forze dell'ordine e dalle agenzie di intelligence. Viene emesso un report finale che evidenzia tutte le attività di indagine effettuate, i risultati rilevati e le eventuali estrazioni di file di prova con allegata la relativa compilazione della catena di custodia, a fini investigativi anche da parte delle Autorità competenti.

4.2.11 Servizio di threat intelligence

Il Fornitore eroga servizi di Threat Intelligence per il monitoraggio delle più recenti informazioni relative a minacce, vulnerabilità ed exploit di sicurezza garantendo: accuratezza, affidabilità, chiarezza e completezza.

All'interno di tali servizi possono essere richiesti a titolo puramente indicativo e non esaustivo:

- APT feed: fornitura dei dati relativi ai più recenti IoCs (indicatori di compromissione);
- Threat sharing automatizzata;
- Asset tracker & data leak: rilevare fughe di dati di proprietà dell'Amministrazione in Internet, anche nel c.d. "dark web".

Le informazioni di maggior impatto devono essere comunicate tempestivamente al personale che effettua il monitoraggio, in tempo reale, dell'infrastruttura di sicurezza e ai referenti dell'organizzazione che ha richiesto il servizio.

- Il Fornitore dovrà mettere a disposizione una piattaforma web che permetta all'Amministrazione di accedere alle apposite dashboard che rendono disponibili le informazioni (Knowledge base).

4.2.12 Servizio di host hardening

Il Fornitore eroga un servizio di host hardening che consiste nel supporto all'amministrazione per la definizione, manutenzione ed il controllo di procedure e politiche di configurazione sicura, nonché di cancellazione sicura dei dati, e di aggiornamento dei sistemi server e storage, apparati di rete e sistemi client e mobile, considerando anche eventuali spostamenti in territori considerati non sicuri, in linea con policy di sicurezza adottate dall'Amministrazione che saranno condivise, con le figure professionali dell'IT, interno all'Ente, del Fornitore dei servizi di IT System Management o di eventuali altre figure professionali che operano per conto dell'Amministrazione.

4.2.13 Servizio di security awareness

Il Fornitore dovrà mettere a disposizione un sistema integrato con il quale eseguire simulazioni e testing e valutare conoscenze inerenti argomenti specifici sulla sicurezza informatica per i quali coinvolgere tutto il personale, oltre a quello IT. L'Amministrazione si riserva di poter valutare altri servizi alternativi che il Fornitore dovrà rendersi disponibile a proporre.

Il servizio richiesto deve essere erogato secondo criteri da stabilire con l'Amministrazione e, comunque, deve essere in grado di adattarsi dinamicamente alle esigenze dell'Amministrazione stessa, con metodologie di approccio innovative, indipendentemente dai contenuti. A titolo esemplificativo e non esaustivo, si possono elencare simulazioni di eventi di attacco di diversa tipologia e con modalità differenti di remediation, gestione di campagne di phishing massive e altre forme di sfida in modalità interattiva con diversi livelli di difficoltà che si rendessero particolarmente interessanti per migliorare le conoscenze nell'ambito.

Il servizio deve proporre aggiornamenti in grado di stare al passo con la rapida evoluzione delle tecniche di attacco e, conseguentemente, la creazione di nuove metodologie di difesa, che quindi devono essere ricomprese nel servizio offerto.

Come noto, infatti, il campo della sicurezza informatica si caratterizza per la rapidità con le quali si modificano le tecniche di attacco e conseguentemente la ricerca e sviluppo di metodologie di difesa, che devono essere ricomprese nelle simulazioni rivolte anche alle figure specialistiche

dell'Amministrazione come quelle citate, e che sono anche quelle ad essere le prime chiamate ad individuare e bloccare con efficacia gli attacchi mirati, e a risolvere rapidamente le violazioni sospette. È quindi fondamentale che il servizio sia nativamente predisposto alla flessibilità e adattabilità secondo le esigenze dell'Amministrazione in tempi rapidi ed adeguati alle esigenze del momento.

La forma di fruizione del servizio dovrà ricomprendere le licenze necessarie per l'erogazione dello stesso, incluso il supporto di gestione dei test di verifica del livello di preparazione raggiunto, oltre ai servizi di erogazione delle simulazioni suddette.

Le modalità di erogazione dei corsi devono essere strutturate in aderenza alle linee guida sull'accessibilità, le WCAG 2.1 (https://www.w3.org/Translations/WCAG21-it/) a livello A e AA.

4.2.14 CyberSecurity & Privacy Legal Advisor

Il Fornitore mette a disposizione la figura professionale del Cyber security and Privacy legal advisor che rappresenta il supporto in affiancamento al team Sicurezza e al Servizio Legale dell'Amministrazione e contribuisce alla valutazione e analisi dei rischi, alla stesura di procedure e disciplinari ed eventuali documenti programmatici relativi alla sicurezza, all'elaborazione e all'implementazione legale di un modello di sicurezza informatica e dei sistemi di gestione della sicurezza delle informazioni (ISMS) e agli aspetti legali collegati al verificarsi delle minacce di attacchi informatici, sia in fase di reazione all'evento e sia nella fase di elaborazione dell'incident response.

La consulenza e il supporto legale richiesto ricomprendono tutti gli aspetti connessi alla sicurezza fisica e logica, inclusi quelli relativi alle strumentazioni informatiche utilizzate dall'Amministrazione, quindi dai personal computer ai dispositivi mobili e ai server, le comunicazioni digitali, la videosorveglianza, ecc.

Gli aspetti sui quali si chiede la consulenza devono ricomprendere:

- Interruzione dell'attività clinico-sanitaria;
- Perdite economiche e finanziarie conseguenti ai danni post-incident;
- Furto di informazioni private e/o cliniche;
- Diffusione di informazioni private e/o cliniche;
- Supporto relativo agli adempimenti ed obblighi di notifica al Garante Privacy (data breach)
- Contenziosi connessi agli incidenti di sicurezza informatica;
- Implicazioni connesse al trattamento dei dati degli utenti;
- Verifiche sulla compliance rispetto le normative sulla sicurezza informatica;
- Danno reputazionale e di immagine.

La consulenza legale deve essere offerta sia per una gestione preventiva degli incidenti e sia post-incident e basarsi sulle norme principali note in ambito di sicurezza come: il regolamento europeo GDRP e s.m.i., le misure minime di sicurezza per le pubbliche amministrazioni dell'AGID, la Direttiva UE 2016/1148 (Direttiva NIS).

Deve inoltre fornire supporto alla gestione e coordinamento delle diverse figure professionali sia interne all'Amministrazione e sia esterne, tra cui l'Alta Direzione, il DPO, l'Ufficio Legale, il Servizio Informatico, l'Ufficio Comunicazione, eventuali Agenzie di assicurazione.

4.2.15 Servizio di security advisoring

Il Fornitore dovrà erogare un servizio di Security Advisoring per l'elaborazione e la pianificazione di attività di diagnostica e verifiche di sicurezza, anche periodiche, e relativi bollettini, utilizzando modalità e standard riconosciuti a livello nazionale ed internazionale. Il servizio dovrà prevedere tecniche di rilevamento ed analisi delle vulnerabilità in diversi ambienti, quali ad esempio a titolo esemplificativo e non esaustivo, applicativi aziendali sia web based e sia non web based, reti wired e wireless, sistemi operativi (tipicamente Microsoft e Debian/Linux) e DBMS.

Il Fornitore predispone, emette ed invia periodicamente bollettini di sicurezza volti a rappresentare una sintesi delle evidenze rilevate dal monitoraggio continuo delle fonti aperte e proprietarie, necessarie ad acquisire informazioni su nuove minacce e vulnerabilità e correlate con i sistemi presenti nell'infrastruttura dell'Amministrazione che ha richiesto il servizio di Monitoraggio in tempo reale di eventi di sicurezza al fine di valutare potenziali rischi.

Nel caso di eventi particolarmente critici e nel caso di una elevata esposizione al rischio che richiedano l'intervento con tempi di reazione ridotti, vengono inviate delle segnalazioni ad-hoc sia ai referenti tecnici dell'Amministrazione che ai referenti tecnici del SOC per verificare quali regole e correlazioni siano da applicare sui sistemi di monitoraggio, oltre alla verifica dei possibili eventuali rimedi da applicare a sistemi e reti, in collaborazione con le figure professionali dell'IT, interno all'Ente, del Fornitore dei servizi di System Management o di eventuali altre figure professionali che operano per conto dell'Amministrazione.

4.2.16 Servizi di Service e Performance Management

È compito del Fornitore assicurare che i servizi di gestione in ambito sicurezza informatica siano organizzati e strutturati secondo un approccio process-driven, in cui la complessa struttura organizzativa/operativa dei servizi sia scomposta in una serie di processi integrati e correlati tra loro in accordo con le best practices ITIL, con l'obiettivo, in ambito di sicurezza informatica, di:

- migliorare la qualità dei servizi;

- ridurre i costi di erogazione dei servizi;
- allineare i servizi con i bisogni correnti e futuri del business e dei clienti.

Nel caso in cui l'Amministrazione abbia già definito a priori la strutturazione dei processi di gestione secondo le best practices ITIL, il Fornitore dovrà erogare i servizi adottando i processi già definiti; nel caso in cui, invece, l'Amministrazione non abbia definito, in tutto o in parte, la strutturazione dei processi di gestione, il Fornitore dovrà, su richiesta e in accordo con l'Amministrazione, proporre e adottare un'adeguata strutturazione dei processi previsti.

Si ritiene utile sottolineare, in maniera più puntuale, il valore aggiunto atteso dall'operatività del Fornitore nell'ambito di alcuni tra i processi più significativi per l'evoluzione del modello di erogazione dei servizi.

Si precisa che non tutti i processi per cui ci si attende un impegno dal Fornitore sono di seguito elencati, fermo restando che il Fornitore deve supportare l'Amministrazione effettuando tutte le attività di competenza, sulla base di quanto stabilito nelle procedure operative che saranno rese disponibili o implementate nel corso della gestione contrattuale.

4.2.16.1 Gestione delle Richieste e delle Segnalazioni

In coerenza con i processi in uso presso l'Amministrazione, è richiesto che il Fornitore utilizzi gli strumenti resi disponibili dall'Amministrazione per tracciare le attività a carattere operativo nonché le richieste di informazioni e di segnalazione di disservizio.

In particolare, il Fornitore stesso deve:

- alimentare gli strumenti di tracciatura;
- effettuare la ricezione e la presa in carico delle richieste nei tempi concordati;
- aggiornare le informazioni di ciascun ticket con l'effettivo stato/andamento delle attività;
- fornire una stima dei tempi di esecuzione e una diagnosi relativa all'intervento da effettuare;
- effettuare la chiusura dei ticket;
- gestire, per quanto di competenza, gli interventi dei fornitori terzi.

4.2.16.2 Supporto al Processo di Incident e Problem Management

Al fine di garantire la corretta fruizione dei servizi da parte dell'utenza di riferimento, il Fornitore è responsabile della gestione di tutti i casi in cui sia rilevabile una interruzione o un degrado nella fruizione del servizio. Tale responsabilità è indipendente dalla causa dell'interruzione/degrado, che può essere legato al software, all'hardware e relativo firmware sistemi e/o apparati di sicurezza.

Il Fornitore è tenuto ad effettuare le attività necessarie al ripristino del servizio all'utenza di riferimento entro i tempi massimi prefissati, anche attraverso l'attivazione delle procedure di escalation concordate.

Tali procedure tengono conto del livello di gravità del malfunzionamento e dell'impatto dello stesso sull'operatività dell'utenza.

L'attività di gestione dei malfunzionamenti deve essere sia proattiva, ossia rivolta alla prevenzione, sia reattiva, ossia rivolta alla gestione ed infine alla risoluzione di tutti gli eventi che comportano l'interruzione o il degrado nella fruizione del servizio.

Pertanto, tra le attività richieste si includono:

- l'identificazione del malfunzionamento, la sua documentazione, la gestione delle comunicazioni e dell'escalation e la sua risoluzione, anche attraverso l'attività di terze parti;
- l'analisi del verificarsi di problemi ripetitivi. I risultati dell'analisi sono inseriti nella knowledge base e sugli elementi interessati sono eseguiti controlli approfonditi atti ad individuare e risolvere problemi di tipo strutturale, secondo quanto concordato con la l'Amministrazione nell'ambito del processo di Problem management;
- l'analisi delle informazioni derivanti dall'esecuzione delle attività di verifica di performance dei sistemi, tenendo conto delle informazioni provenienti dai sistemi di monitoraggio.

In ultimo, è responsabilità del Fornitore il salvataggio dei dati ai fini dell'analisi di incidenti di sicurezza. Il Fornitore deve assicurarsi che i sistemi, anche non direttamente gestiti, inviino al sistema di Log Management le informazioni utili alle attività di analisi da parte del SOC, attivando - in caso negativo - le procedure concordate con l'Amministrazione.

È richiesto, infatti, che sia effettuata la conservazione di tutti i log di auditing relativi sistemi e apparati di sicurezza e quanto altro possa essere necessario alla ricostruzione di comportamenti insidiosi e per l'individuazione di possibili responsabilità penali e civili conseguenti a condotte illecite. Tali log devono essere mantenuti in linea per il periodo concordato con l'Amministrazione. Su tali log l'Amministrazione si riserva di richiedere al team di effettuare ricerche ed elaborazioni statistiche puntuali.

Si precisa che i dati da raccogliere e da salvare ai fini dell'indagine sugli incidenti di sicurezza saranno concordati successivamente all'avvio della fornitura.

4.2.16.3 Supporto al Processo di Change e Release & Deployment Management

Al fine di garantire il corretto funzionamento, lo sviluppo e l'evoluzione dell'infrastruttura ICT dell'Amministrazione, il Fornitore è responsabile della pianificazione, dell'attuazione, del tracciamento e della verifica dei cambiamenti dell'hardware, del firmware, dell'evoluzione dei

sistemi operativi, dei prodotti di sicurezza informatica e delle relative correzioni coerentemente con i processi di Change Management e Release & Deployment Management.

4.2.16.4 Supporto al Processo di Service Asset & Configuration Management

Il Fornitore deve garantire il costante, accurato e continuo allineamento delle basi dati del CMDB; nel caso in cui tali aggiornamenti non possano essere eseguiti automaticamente, il Fornitore deve procedere con l'aggiornamento manuale. Si precisa che l'aggiornamento del CMDB è prevalentemente effettuato in automatico attraverso prodotti di scansione le cui politiche sono definite dall'Amministrazione e sono supportati da script/procedure automatiche che potrebbero essere realizzate da terzi.

Si precisa che i processi e le procedure operative sono oggetto di revisione e miglioramento continuo, pertanto, nel periodo contrattuale, le modalità indicate potrebbero variare. In ogni caso i fornitori sono obbligati a seguire qualsiasi variazione dei processi e delle procedure operative che l'Amministrazione indicherà.

L'aggiornamento costante e accurato della baseline, in particolare del CMDB, è ritenuto il nucleo fondamentale sui cui si fondano:

- i processi già in uso nonché i processi che potrebbero essere eventualmente adottati ed implementati nel corso della durata contrattuale;
- il patrimonio informativo relativo alla consistenza e alla configurazione dell'infrastruttura ICT dell'Amministrazione;
- la valutazione di eventuali impatti per i servizi di business dell'Amministrazione a fronte di evoluzioni, cambiamenti di carattere infrastrutturale;
- le analisi volte all'integrazione e/o all'introduzione di nuovi servizi a supporto dell'attività istituzionale dell'Amministrazione;
- la rilevazione e la misurazione della qualità del servizio all'utenza di riferimento.

Si ritiene utile precisare che, alla data di inizio attività, il CMDB potrebbe non essere completo di tutte le informazioni previste.

Ad inizio fornitura, è richiesto al Fornitore un security assessment per la verifica sulla postura di sicurezza oltre alla verifica sulla consistenza e coerenza dei dati di Asset & Configuration, degli Utenti Amministratori e delle relazioni tra gli stessi.

4.2.16.5 Supporto al Processo Capacity Management

Il Fornitore è responsabile dell'esecuzione delle attività operative a supporto del processo di Capacity Management. Pertanto, è responsabile della raccolta dei dati, dell'analisi periodica dello stato di

salute dell'Infrastruttura ICT, in ambito sicurezza informatica, affidata in gestione, dell'analisi dei trend di carico e della produzione di reportistica che mostri la situazione riassuntiva di ciascun sistema e che ne evidenzi eventuali criticità o necessità di evoluzione.

Si precisa che l'Amministrazione si riserva di richiedere la produzione di ulteriore reportistica il cui contenuto, formato e periodicità è concordato ad inizio fornitura ed eventualmente rivisto, nel corso della durata dei servizi, ai fini della predisposizione del Piano della Capacità.

Il Fornitore, nell'erogazione del servizio, può utilizzare gli strumenti e i prodotti resi disponibili dall'Amministrazione ovvero può utilizzare script e/o le funzionalità native del software di sistema.

4.2.16.6 ServiceDesk Sistemistico di Sicurezza Informatica

Nell'ambito dei processi strutturati di Service Management, il Fornitore deve prevedere una funzione di Service Desk Sistemistico di sicurezza informatica, che agisca come punto di contatto tra i referenti informatici dell'Amministrazione e l'IT Security Management, per gestire incidenti e richieste degli utenti e fornire un'interfaccia per gli altri processi, tra cui Change, Problem, Configuration, Release, gestendo tutto il ciclo di vita dell'incidente, assieme alle figure professionali preposte, o della service request.

Gli elementi distintivi della funzione di Service Desk Sistemistico sono:

- prima diagnosi e tentativo di risoluzione delle segnalazioni/richieste al primo livello, anche attraverso l'utilizzo delle informazioni presenti nella Knowledge base;
- classificazione degli incidenti o richieste, attraverso modalità' obiettive per classificare gli incidenti in modo che siano assegnati opportunamente;
- assegnazione della priorità, attraverso modalità obiettive per l'assegnamento della priorità di un incidente (ad esempio attraverso una matrice di impatto/urgenza);
- assegnazione degli incidenti/richieste, automatizzando il più' possibile il routing dei casi in base al workload e alle competenze di ogni tecnico, in modo da ottimizzare le risorse;
- assegnazione a gruppi esterni, attraverso accordi con Fornitori terzi responsabili di specifiche attività.
    - La funzione di service desk sistemistico è relativa alle problematiche di system management dei sistemi di sicurezza informatica descritte nel presente Capitolato Tecnico e ha come principale utenza di riferimento i referenti informatici dell'Amministrazione. E' compresa l'assistenza agli utenti per problematiche che riguardano specifici incidenti di sicurezza che coinvolgono le postazioni di lavoro e gli utenti medesimi.

5. LOTTI 1 - 2. MODELLI DI EROGAZIONE E REMUNERAZIONE DEI SERVIZI

Nei capitoli precedenti i servizi di System Management e Sicurezza Informatica sono descritti e classificati dettagliatamente in base ai contenuti e alle specificità tecniche di ciascuno. In questo capitolo, invece, tali servizi sono sintetizzati e classificati in macrocategorie organizzate dal punto di vista dei modelli di erogazione e di remunerazione piuttosto che da quello dei contenuti tecnici. Tali modelli costituiscono la base per il dimensionamento dei servizi e per la formulazione delle offerte economiche. Le modalità di erogazione /remunerazione e la misura del canone annuo sono riepilogate nelle tabelle seguenti:

Lotto 1

Macro Categoria	Modalità di erogazione/remunerazione	Il canone annuo corrisponde al prezzo per
Servizio di monitoraggio NOC	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi e Apparati di rete;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi mail server;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi DB server;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi Web server;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi Back office;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi Storage backup;	Canone annuo	Server/Appliance (virtuale o fisico)
Figure Professionali:		
TEM - ICT Operation Manager;	GG/uomo	
CET - Enterprise Architect;	GG/uomo	
SPP - System Architect;	GG/uomo	
SIS - System Administrator Senior;	GG/uomo	
SIM - System Administrator Middle;	GG/uomo	
SIJ - System Administrator Junior;	GG/uomo	

DBS - Database Administrator Senior;	GG/uomo	
DBJ - Database Administrator Junior;	GG/uomo	
SRS - Network Specialist Senior;	GG/uomo	
SRJ - Network Specialist Junior.	GG/uomo	

Lotto 2

Macro Categoria	Modalità di erogazione/remunerazione	Il canone annuo corrisponde al prezzo per
Servizio di monitoraggio SOC	Canone annuo	FASCIA DI EPS*
Sistemi Firewall, IDS,IPS	Canone annuo	PIATTAFORMA**
Sistemi Antivirus e di telemetria xDR/EDR/NDR	Canone annuo	PIATTAFORMA**
Sistemi WAF,	Canone annuo	PIATTAFORMA**
Sistemi SIEM, SOAR,	Canone annuo	PIATTAFORMA**
Servizio di Incident response & remediation		ENTE ***
Servizio di threat intelligence / APT-feed / asset tracker & data leak	Canone annuo	DOMINIO
Servizio di User and entity behavior analytics (UEBA)	Canone annuo	UTENTE
Servizio di host hardening	Canone annuo	DEVICE MODEL****
Servizio di security awareness	Canone annuo	UTENTE
Servizio di Vulnerability Management	Canone annuo	IP
Servizio di Application Security Testing	Canone annuo	APPLICAZIONE
Figure Professionali:		
Security Project Manager	GG/uomo	
Governance & risk compliance (GRC) consultant	GG/uomo	
Security architect & engineer	GG/uomo	
Security Advisor senior	GG/uomo	
Security Advisor junior	GG/uomo	
Security specialist	GG/uomo	
Security specialist con reperibilità H24	GG/uomo	
Security Analyst senior	GG/uomo	
Security Analyst junior	GG/uomo	
Vulnerability researcher / Ethical Hacker senior	GG/uomo	

Vulnerability researcher / Ethical Hacker junior	GG/uomo	
Incident handler / response senior	GG/uomo	
Incident handler / response junior	GG/uomo	
Digital forensic	GG/uomo	
CyberSecurity & Privacy Legal Advisor	GG/uomo	

Note:

*Per le Fasce di EPS vedere in calce al paragrafo 5.1 seguente;

** Per Piattaforma si intende un'infrastruttura costituita da componenti hardware e software per l'erogazione di servizi informatici tramite interfacce applicative e funzionalità specifiche;

*** Sono inclusi fino ad un massimo di 3 incidenti e 5 segnalazioni all'anno;

****Per Device Model si intende la tipologia del dispositivo ovvero una aggregazione di device.

5.1 Servizi a Canone

Nell'ambito della presente Convenzione sono definite due distinte modalità di presidio del servizio: **"Presidio on-site"** o **"Presidio da remoto"** corrispondenti ad un servizio erogato da personale del Fornitore allocato fisicamente nella sede dell'Amministrazione nel primo caso, presso il Centro Servizi del Fornitore nel secondo caso, con l'utilizzo di strumenti che potranno essere quelli del fornitore o quelli dell'Amministrazione secondo le esigenze dell'Amministrazione stessa e che saranno oggetto di valutazione in fase di assessment.

Il "**Servizio di monitoraggio sistemi e reti**" comprende i servizi di monitoraggio dei sistemi per la rilevazione di malfunzionamenti hardware e/o software, gli interventi di primo livello e le attività di escalation verso i livelli superiori a seguito di procedure schedulate.

Il servizio può essere erogato sia in modalità di presidio on site che in modalità remota dal Centro Servizi del Fornitore.

Il **"Servizio di Monitoraggio in tempo reale di eventi di sicurezza**" comprende tutte le attività di monitoraggio dell'infrastruttura IT dell'Amministrazione al fine di rilevare e gestire in tempo reale gli eventi relativi alla sicurezza informatica.

Il servizio può essere erogato sia in modalità di presidio on site che in modalità remota dal Centro Servizi del Fornitore. La "**conduzione operativa sistemi**", la "**conduzione operativa reti**" e la "**conduzione operativa di apparati e sistemi di sicurezza"** comprende in generale tutti i **servizi**

base di gestione di tipo continuativo svolti nell'orario base di lavoro, includendo gestione e configurazione sistemi e reti, manutenzione sistemi, gestione software di base e di ambiente e basi dati, descritti nel lotto 1; gestione e configurazione manutenzione apparati e sistemi sicurezza, descritti nel lotto 2.

I servizi di "**Monitoraggio sistemi e reti**", "**Monitoraggio in tempo reale di eventi di sicurezza"** e "**Conduzione operativa**" possono essere erogati sia in modalità di presidio on site che in modalità remota dal Centro Servizi del Fornitore, a seconda delle preferenze dell'Amministrazione.

La **remunerazione dei servizi è a canone** ed è basata sulla dimensione e le caratteristiche dell'infrastruttura tecnologica oggetto del servizio stesso, ovvero è indipendente dal numero e dalla tipologia di risorse professionali impiegate dal Fornitore.

Nel caso specifico dei servizi di Monitoraggio (NOC e SOC) e conduzione operativa, oltre alle fasce orarie di erogazione del servizio, concorre alla formazione del canone anche la classificazione dei sistemi ed il livello di criticità ed eventualmente, come nel caso della conduzione operativa, la reperibilità come meglio definito di seguito.

Inoltre, per il servizio di Monitoraggio SOC (Lotto 2) il canone è differenziato nelle seguenti fasce in base al numero di EPS (eventi per secondo):

- fino a 1000 EPS;
- da 1001÷5000 EPS;
- da 5001÷10000 EPS;
- da 10001 EPS in su,

sia per il servizio con ORARIO BASE che per il servizio con ORARIO CONTINUATO.

5.1.1 Orari del servizio

L'effort dedicato alle attività di monitoraggio sistemi, conduzione operativa dei sistemi, delle reti, della sicurezza informatica e reperibilità standard varia in base all'orario di servizio richiesto al Fornitore. Per tale motivo, nell'ambito della presente Convenzione si definiscono, ove previste, per il **Lotto 1** tre fasce orarie di riferimento:

Finestra di erogazione dei servizi Sistemistici		
Orario BASE	**Orario ESTESO**	**Orario CONTINUATO**
Lun-Ven 8.00 – 18.00	Lun-Ven 7.30 – 19.00; Sab 7.30 - 14.00	H24, 7 giorni su 7

Per il **Lotto 2**:

Finestra di erogazione dei servizi Sicurezza informatica

Orario BASE		Orario CONTINUATO
Lun-Ven 8.00 – 18.00		H24, 7 giorni su 7

5.1.2 Classificazione dei sistemi, livello di criticità e livello di severità

Le tipologie di Sistemi oggetto della presente fornitura corrispondono a:

Lotto 1:

Sistemi Mail Server
Sistemi DB Server
Sistemi Application Server / Web Server / Middleware
Sistemi infrastrutturali/backoffice

Lotto 2:

Sistemi Firewall, IDS/IPS;
Sistemi Antivirus e di telemetria (xDR/EDR/NDR);
Sistemi WAF;
Sistemi SIEM, SOAR;

In particolare, per quanto attiene alla classificazione per **livello di criticità** in ambito IT System Management (Lotto 1) si intende:

◦ **Sistema non critico**: disponibilità =< 99,8%, tempo di presa in carico malfunzionamenti entro 4 ore, ambiente di produzione, sistemi di test/sviluppo o sistemi che comunque non impattano in modo significativo sui processi di business dell'Ente*;*

◦ **Sistema Business critical**: disponibilità > 99,8%, tempo di presa in carico malfunzionamenti entro 2 ore, ambiente di produzione, tipicamente sistemi che impattano in modo significativo sui processi di business dell'Ente*;*

◦ **Sistema Mission critical**: disponibilità > 99,8%, tempo di presa in carico malfunzionamenti entro 1 ora, ambiente di produzione tipicamente sistemi il cui malfunzionamento blocca i processi di business dell'Ente.

Inoltre, posto che tutti i sistemi di sicurezza (Lotto 2) sono considerati con il livello di criticità "Sistema Mission Critical" e pertanto deve essere garantita la disponibilità di cui sopra, per l'operatività di apparati e sistemi, nonché per la gestione degli incidenti di sicurezza gestiti dal SOC e dal Incident Response and Remediation Team (IRRT), deve essere considerata la seguente **classificazione per severità** in base alla quale la presa in carico del disservizio o dell'incidente deve essere effettuata entro gli SLA indicati in tabella 5 o in tabella 6 e tabella 7:

◦ **BASSA**:

- impatto ridotto sull'operatività di un servizio o un sistema di sicurezza in ambiente di

produzione, test/sviluppo;

- incidente derivante da un possibile rischio di minacce da virus o malware oppure dall'intrusione da parte di utenti non autorizzati oppure che provoca la parziale inattività di un esiguo numero di utenti autorizzati;

◦ **MEDIA**:

- impatto che degrada e rende parzialmente interrotto un servizio o un sistema di sicurezza in ambiente di produzione;
- incidente che compromette e degrada le prestazioni o il parziale funzionamento di reti, sistemi e applicazioni oppure che provoca la parziale inattività di un significativo gruppo di utenti autorizzati;

◦ **ALTA**:

- impatto grave sull'operatività e sul livello di compromissione di un servizio o di un sistema di sicurezza in ambiente di produzione;
- grave incidente di sicurezza a causa di sistemi compromessi, accessi abusivi, rischio frodi e furti di dati dell'Amministrazione, estesa infezione da parte di virus e malware, perdita di immagine e/o reputazionale.

I suddetti criteri di classificazione concorrono all'individuazione dei canoni annui (la cui applicazione deve essere definita dall'Amministrazione nella fase di assessment iniziale, vedasi paragrafo 7.1) e/o dei relativi SLA.

5.1.3 Reperibilità ed interventi fuori orario

Reperibilità standard

Il modello di remunerazione previsto per il servizio di reperibilità standard è basato su un canone annuale complessivo calcolato in base ai valori scelti per le variabili già descritte nel dettaglio al paragrafo 5.1.2.

Reperibilità individuale

Per le attività di conduzione operativa e di supporto specialistico di tipo continuativo, l'Amministrazione può richiedere la reperibilità, al di fuori del normale orario di lavoro, del personale già impegnato nelle attività onsite, per rispondere tempestivamente ad eventuali situazioni critiche. Per tale servizio, il modello di remunerazione è strettamente dipendente dal numero e tipologia di risorse professionali impiegate nell'erogazione del servizio stesso, pertanto viene prevista una remunerazione differente per la reperibilità di ciascuna figura professionale.

La singola Amministrazione, sulla base delle proprie esigenze, definirà gli impegni per la reperibilità complessivamente richiesti, in termini di giornate uomo per figura professionale.

Intervento on site fuori orario

Per le attività di conduzione operativa e di supporto specialistico, l'Amministrazione può richiedere interventi onsite al di fuori del normale orario di lavoro a seguito di malfunzionamenti o eventi collegati alla sicurezza informatica, oppure estensioni temporanee dell'orario di servizio per esigenze contingenti di durata limitata nel tempo che richiedano la piena disponibilità del personale di conduzione e/o di supporto oltre l'orario standard.

5.2 Supporto Specialistico

Il servizio di "supporto specialistico" comprende due modalità di erogazione dei servizi sistemistici e di sicurezza informatica, che sono strettamente dipendenti dal numero e tipologia di risorse professionali impiegate dal Fornitore nell'erogazione dei servizi stessi:

- attività di supporto continuativo;
- attività di supporto a richiesta.

Si richiede, infine, che le risorse impegnate ad erogare il supporto specialistico, in loco o da remoto, possano interagire con in Centri di Competenza del Fornitore, a titolo esemplificativo (e non esaustivo) si elencano alcuni possibili Centri di Competenza:

- Centri di Competenza su Tecnologie SAP;
- Centri di Competenza su Tecnologie OpenSource;
- Centri di Competenza su Tecnologie Cloud e Virtualizzazione;
- Centri di Competenza su Tecnologie Storage;
- Centri di Competenza su Tecnologie Database;
- Centri di Competenza su Tecnologie Firewall, IDS/IPS, Antivirus e xDR/EDR/NDR;
- Centri di Competenza su Tecnologie WAF;
- Centri di Competenza di Tecnologie SIEM, SOAR.

5.2.1 Attività di supporto continuativo

Tali attività rientrano nell'ambito generale delle attività di gestione e sviluppo sistemi ma, per i motivi tecnici e/o organizzativi, non possono essere ricomprese nel modello dei servizi di conduzione operativa, e si configurano quindi come affiancamento al personale dell'Amministrazione e/o al personale del Fornitore impiegato nei servizi di conduzione.

I motivi tecnici alla base della necessità di supporto specialistico continuativo possono ad esempio derivare dalla necessità di effettuare attività che richiedono specifiche competenze in ambiti

particolari (ad esempio team di analisi delle politiche di sicurezza).

I motivi organizzativi possono invece essere relativi, ad esempio, ai casi in cui le attività di conduzione operativa sono effettuate direttamente da personale dell'Amministrazione e il personale del Fornitore è di supporto a quello dell'Amministrazione e opera di concerto con quest'ultimo e sotto il suo controllo diretto. In questo caso le attività e le responsabilità suddette sono anche a carico dell'Amministrazione, quindi, la responsabilità del Fornitore è limitata ed è generalmente orientata a garantire la disponibilità e l'operatività delle risorse impiegate.

La durata minima del servizio di supporto specialistico continuativo è annuale e sono incluse eventuali sostituzioni per ferie e malattia del personale. Per quanto riguarda la modalità di presidio è di tipo onsite. La singola Amministrazione, sulla base delle proprie esigenze, definirà le attività di supporto continuativo richieste, in termini di numero e tipologia di figure professionali, che saranno quantificate. Il modello di remunerazione, per il servizio, è a GG/uomo.

5.2.2 Attività di supporto a richiesta

Tali attività comprendono:

- attività di supporto specialistico con affiancamento al personale dell'Amministrazione e/o al personale di conduzione operativa, che possono essere richieste ed erogate in modalità estemporanea (pur nell'ambito di un'opportuna pianificazione), per durate variabili e per periodi non contigui. La remunerazione del servizio è a "GG/uomo" ed è dipendente dal numero e dalla tipologia di risorse professionali richieste al Fornitore.
- attività di sviluppo/evoluzione delle infrastrutture tecnologiche definite in termini temporali (inizio e fine attività) e con specifici prodotti di output. Tali attività riguardano modificazioni significative dell'ambiente elaborativo, che richiedono un effort elevato ma limitato nel tempo, per le quali non ci si può avvalere del servizio di conduzione operativa, né del servizio di supporto continuativo. La remunerazione del servizio è "GG/uomo" ed è basata sull'effort stimato ad inizio attività, ovvero sul numero e sulla tipologia di risorse professionali previste;

Per le tipologie di attività suddette, l'orario di lavoro di riferimento per una singola risorsa professionale è di 8 ore al giorno.

Per le attività di supporto specialistico con affiancamento al personale dell'Amministrazione e/o al personale di conduzione operativa, la modalità di presidio è di tipo onsite.

Le attività di supporto specialistico a richiesta sono svolte dalle Figure professionali riportate nell'Allegato A al presente Capitolato.

5.3 Modalità di attivazione ed esecuzione della fornitura

Le risorse che verranno impiegate nelle attività devono essere di gradimento dell'Amministrazione, e devono avere i requisiti di professionalità richiesti e dichiarati dal Fornitore; l'Amministrazione si riserva la facoltà di ricusare detto personale per giustificati motivi.

È facoltà dell'Amministrazione verificare in via preventiva le competenze tecnico-professionali del personale specialistico proposto.

I controlli e le verifiche del personale effettuati dall'Amministrazione non liberano il Fornitore dagli obblighi e dalle responsabilità inerenti al contratto.

Competeranno all'Amministrazione la supervisione ed il controllo delle prestazioni rese dal personale inviato dal Fornitore per l'adempimento dei servizi ordinati.

5.4 Documentazione

Le attività richieste comportano la stesura e l'aggiornamento di tutta la documentazione necessaria secondo gli standard adottati dall'Amministrazione. La documentazione degli interventi eseguiti riguardanti attività tecniche o progettuali è da intendersi parte integrante della fornitura e dovrà essere consegnata in formato elettronico secondo la pianificazione concordata.

La documentazione tecnico-specialistica relativa ad interventi ed attività eseguite è a carico del Fornitore e deve essere prodotta utilizzando strumenti di gestione documentale e di reporting forniti dall'Amministrazione; strumenti alternativi potranno essere proposti dal Fornitore nell'offerta tecnica. In ogni caso l'Amministrazione si riserva di sottoporli a verifica ed eventualmente accettarli in fase di avviamento della fornitura. Per l'utilizzo di eventuali prodotti aggiuntivi non è previsto alcun corrispettivo.

5.5 Orario e luogo di lavoro

Le prestazioni oggetto del presente capitolato si svolgeranno nella modalità on-site presso gli uffici dell'Amministrazione (anche con utilizzo di una strumentazione di supporto messa a disposizione dall'Amministrazione stessa) o da remoto presso il Centro Servizi del Fornitore.

Tali prestazioni saranno erogate nelle fasce orarie previste dalle singole Amministrazioni in sede di contratto.

5.6 Avvicendamento contrattuale

Al fine di rendere il più efficace possibile l'avvicendamento contrattuale, dopo l'emissione di un ordinativo di fornitura da parte di una Pubblica Amministrazione aderente alla Convenzione, il Fornitore dovrà rendere disponibili entro 5 giorni lavorativi le risorse necessarie al passaggio di

consegne dall'attuale Fornitore del servizio. La tipologia di figure professionali, il loro numero e le modalità di esecuzione di tale passaggio dovranno essere concordate con l'Amministrazione e comunque entro e non oltre 3 mesi. La presa in carico di tale know-how dovrà avvenire a titolo non oneroso per l'Amministrazione.

Entro il termine della fornitura, il Fornitore dovrà essere disponibile a trasferire il know-how acquisito all'Amministrazione o a terzi dalla stessa designati. Tale attività sarà remunerata secondo le tariffe del contratto allora vigente.

6. LOTTI 1 - 2. CARATTERISTICHE DELLE FIGURE PROFESSIONALI

6.1 Figure professionali

Si rinvia all'Allegato A – Figure professionali al presente Capitolato.

7. LOTTI 1 - 2. SERVIZIO DI ASSESSMENT E DI DEFINIZIONE DEL PIANO DI ESECUZIONE DEI SERVIZI

I servizi di Assessment e di definizione del Piano di Esecuzione dei Servizi sono volti all'esatta definizione tecnica, economica e gestionale del perimetro dei servizi oggetto del Contratto di Fornitura. Essi sono svolti dal Fornitore sia nella fase preliminare all'eventuale stipula del Contratto di Fornitura, sia nel corso dello stesso.

7.1 Assessment

Con l'Assessment, il Fornitore, anche sulla base della classificazione di cui al punto 5.1.2, individua le caratteristiche:

- dei sistemi da gestire/manutenere e, per ciascuno di essi, le caratteristiche che ne determinano il prezzo di gestione/manutenzione;
- dell'Amministrazione, dal punto di vista dell'organizzazione e delle procedure interne, al fine di definire e personalizzare le modalità e i processi di esecuzione dei servizi.

Il servizio si compone di:

- sopralluoghi, effettuati dai tecnici del Fornitore che effettueranno una ricognizione "fisica" presso le sedi dell'Amministrazione al fine di raccogliere le "informazioni di dettaglio" degli apparati da gestire ed eventualmente manutenere;
- raccolta di tutte le ulteriori informazioni relative alla configurazione software ed hardware dei suddetti apparati, necessarie o comunque utili all'efficace erogazione dei servizi;
- raccolta delle informazioni relative agli aspetti logistici, organizzativi e procedurali dell'Amministrazione, pure necessarie o utili all'efficace erogazione dei servizi;

Le attività saranno svolte dal Fornitore non solo a seguito delle predette richieste, ma nel corso dell'intera durata del Contratto di Fornitura, allo scopo di:

- rendere disponibile e mantenere aggiornata una base informativa completa e dettagliata del parco macchine in servizio presso l'Amministrazione e delle relative configurazioni hardware e software;
- adattare/ottimizzare modalità e processi di erogazione dei servizi ai mutati aspetti organizzativi e procedurali dell'Amministrazione.

Con il Security Assessment il Fornitore può verificare il livello di maturità della postura di sicurezza informatica dell'Amministrazione coinvolta. I controlli da applicare devono basarsi sul Framework Nazionale di Cyber Security (FNCS).

Il servizio si compone nel:

- predisporre la checklist (ove sia necessario), definire i referenti e il piano di interviste;
- essere di supporto all'organizzazione nell'effettuare le interviste, nel compilare la checklist ed eseguire la raccolta documentale;
- analizzare i dati;
- identificare e definire la postura iniziale e di riferimento al fine di predisporre un report di valutazione da presentare all'alta direzione dell'organizzazione e per definire il perimetro necessario ed utile all'efficace erogazione dei servizi.

Le attività saranno svolte dal Fornitore non solo per la fase iniziale ma anche nel corso dell'intera durata del contratto di fornitura con periodicità concordata allo scopo di:

- identificare le iniziative di sicurezza raccomandate;
- predisporre piani di sviluppo che permettano di migliorare il livello di sicurezza.
- supportare l'organizzazione per la predisposizione dell'analisi dei rischi, del trattamento del rischio e del piano di rientro.

Le attività potranno essere erogate dal Fornitore:

- in loco, contestualmente all'esecuzione dei sopralluoghi, o nel corso dell'esecuzione del Contratto di Fornitura;
- e/o con modalità automatizzate per la rilevazione dei componenti hardware e software, da riscontrare poi in loco in funzione della completezza dello strumento di discovery utilizzato e/o delle risultanze emerse;
- e/o fornendo all'Amministrazione indicazioni puntuali e dettagliate su come reperire e inviare al Fornitore le informazioni richieste, limitatamente a quelle di facile reperimento, e da

riscontrare comunque in loco in caso di dati dubbi.

Tutte le informazioni raccolte dal Fornitore e relative agli apparati dell'Amministrazione, dovranno essere memorizzate nel "Data Base degli Asset", base di dati centralizzata del Fornitore. Tale DB dovrà essere aggiornato a fronte di ogni evento che abbia impatto sulle informazioni stesse (es: interventi, installazioni/aggiornamenti HW e SW).

Con riferimento alle attività di conduzione degli apparati dell'Amministrazione, il Fornitore dovrà preliminarmente individuare gli eventuali:

- apparati che, alla data prevista per l'Avvio dei Servizi, risulteranno "End Of Support" da parte del Produttore;
- verificare se sia già nota la futura data di "End Of Support" dell'apparato e, in caso contrario, formulare le proprie previsioni basate sul ciclo di vita di apparati di stessa tipologia e produttore.

7.2 Piano di Esecuzione dei Servizi

Il Piano di Esecuzione dei Servizi dovrà contenere:

Risultati dell'Assessment

- Elenco, degli apparati oggetto della prestazione dei servizi di gestione ed eventualmente manutenzione, con le caratteristiche rilevanti ai fini della definizione tecnico/economica dei servizi stessi;
- Elenco degli apparati per i quali il Fornitore si avvale della facoltà di non prestare il servizio di gestione e/o manutenzione (apparati che risultino "End of Support" alla data di avvio dei servizi);
- Evidenza degli aspetti logistici, organizzativi e procedurali peculiari dell'Amministrazione, significativi ai fini della definizione delle modalità e dei processi di erogazione dei servizi.

Piano Tecnico-Organizzativo

- Esatta definizione tecnica dei servizi e delle modalità di erogazione tra cui:
  - descrizione delle attività che saranno svolte da remoto, con indicazione degli strumenti utilizzati e delle eventuali configurazioni e/o installazioni di software sugli apparati dell'Amministrazione;
  - descrizione delle attività che saranno svolte con indicazione della frequenza programmata;
- Definizione dei processi che regoleranno l'esecuzione dei servizi, relativamente alle attività:
  - di ordinaria gestione/manutenzione (monitoraggio apparati, interventi di manutenzione preventiva, etc.);
  - eseguite a seguito di specifiche richieste dell'Amministrazione;

  - scaturite da richieste di assistenza o segnalazione di malfunzionamenti, con descrizione dell'iter di escalation;
  - di change management, con riferimento alle politiche ed ai processi di change e alle procedure di ripristino;
  - di terze parti (fornitori di servizi di connettività, fornitori incaricati della gestione/assistenza/manutenzione di apparati nell'ambito di contratti preesistenti, etc.);
- Attività e tempistiche per l'Avvio dei servizi, con particolare riferimento alle attività di:
  - presa in carico degli apparati e start up dei servizi, con indicazione di quali saranno svolte in loco;
  - configurazione apparati e/o installazione software per la gestione da remoto;
  - migrazione da precedenti contratti e sistemi di gestione;
- Identificazione del Personale del Fornitore, che, in aggiunta al Referente locale, sarà coinvolto nell'esecuzione del Contratto Attuativo, con particolare riferimento alle risorse che effettueranno attività in loco.

Piano Economico

Il Piano Economico dovrà determinare, analiticamente, il costo di ciascuno dei servizi oggetto del Piano, per l'intera durata del Contratto di Fornitura, in conformità all'Offerta Economica, all'assessment e alla definizione del perimetro dei servizi di cui sopra, alle modalità di erogazione dei servizi e alla determinazione degli importi per i singoli servizi.

Il Piano Economico dovrà contenere inoltre l'importo complessivo dei servizi, suddiviso in:

- Importo complessivo dei servizi a canone (conduzione operativa, manutenzione, presidio, etc.);
- Importo forfettario complessivo dei servizi a consumo (GG/uomo) indicato in maniera presuntiva, e non vincolante per l'Amministrazione, che si vedrà fatturare, per i citati servizi, unicamente gli importi relativi ai servizi effettivamente utilizzati.

Su iniziativa del Fornitore, qualora le evidenze della gestione contrattuale suggeriscano l'opportunità di apportare modifiche ai processi e alle modalità di erogazione dei servizi – nel rispetto sempre di quanto previsto nel presente Capitolato e nell'Offerta Tecnica del Fornitore – tali da rendere i servizi più efficaci al contesto specifico dell'Amministrazione, il Piano di Esecuzione dei Servizi potrà essere aggiornato.

Nel caso in cui il Piano di Esecuzione dei Servizi sia aggiornato su richiesta dell'Amministrazione, qualora quest'ultima sia interessata ad estendere il perimetro dei servizi e/o degli apparati su cui prestare i servizi, il Piano Economico dovrà indicare esplicitamente la variazione degli importi

complessivi rispetto a quelli relativi al precedente Piano approvato. Laddove il Piano di Esecuzione dei Servizi aggiornato sia accettato dall'Amministrazione, tale variazione sarà pari all'importo del relativo Ordinativo Collegato.

8. LOTTI 1 - 2. OSSERVANZA DI NORME, LEGGI E REGOLAMENTI

Il Fornitore è tenuto all'osservanza delle norme di legge e di regolamento adottate dalle Autorità competenti in materia di contratti di lavoro, sicurezza, protezione dei dati personali, certificazioni e di quant'altro possa comunque interessare l'ambito della presente fornitura, compresi i successivi aggiornamenti.
Inoltre, gli Enti che potranno aderire alla Convenzione adottano al proprio interno policy, linee guida, disciplinari in ambito ICT e sicurezza informatica che il Fornitore è tenuta a rispettare.

9. LOTTI 1 - 2. QUALITA' E LIVELLI DEI SERVIZI

Il Fornitore dovrà produrre ed inviare all'Amministrazione, con cadenza trimestrale e in corrispondenza di ciascun trimestre di fatturazione e all'indirizzo di posta elettronica da essa indicato, un report con i dati relativi ai livelli di servizio, effettivamente conseguiti, per ciascuno dei tre mesi cui il report si riferisce, nell'ambito del contratto di fornitura. Tale report dovrà essere inviato entro i 20 giorni successivi alla chiusura del trimestre di riferimento al Referente tecnico dell'Amministrazione.

Il report dovrà contenere tutti i dati relativi ai livelli di servizio previsti nelle Tabelle dalla 1 alla 10 del successivo paragrafo per il lotto di riferimento. Dovranno essere pertanto forniti i dati analitici, estrapolati dai sistemi di trouble ticketing con dettaglio tale da consentire all'Amministrazione la verifica sia della correttezza dei dati relativi al singolo intervento, sia del calcolo degli SLA conseguiti in ciascun mese.

Ricordando che l'erogazione dei servizi della presente Convenzione avverrà, se non diversamente specificato in altre parti del Capitolato, per il Lotto 1 all'interno di 3 fasce orarie: orario Base, orario Esteso ed orario Continuato, per il Lotto 2 all'interno di 2 fasce orarie: orario Base e orario Continuato, i valori dei parametri di SLA saranno misurati, come dettagliato nelle successive tabelle, in riferimento alla finestra temporale di erogazione dei servizi precedentemente riportata.

9.1 SLA

Nel presente paragrafo sono elencati i Livelli di Servizio oggetto di monitoraggio. Per ciascuno dei Livelli di Servizio è definito uno SLA minimo, corrispondente alla qualità prevista dalla Convenzione.

I valori di SLA si applicano sui servizi dove il Fornitore ha il controllo completo della filiera tecnologica e non sui sistemi PaaS e SaaS di fornitori terzi di servizi in cloud.

Tutti gli SLA delle Tabelle 1, 8, 9 e 10 sono espressi in giorni lavorativi, mentre i tempi previsti nelle Tabelle 2, 3, 4, 5, 6 e 7 sono da riferirsi alle finestre di erogazione dei servizi definiti nel precedente paragrafo 5.1. In tali casi, quando lo SLA è espresso in giorni, è da intendersi entro l'n-esimo giorno lavorativo (all'interno cioè della finestra di erogazione) successivo a quello di apertura del ticket.

Gli SLA di cui alle Tabelle 2, 3, 4, 5, 6 e 7 sono tutti riferiti, anche ai fini del calcolo delle penali, ad un periodo di osservazione mensile e, nel caso in cui un'attività sia eseguita a cavallo di due periodi di osservazione, essa verrà riferita al periodo di osservazione in cui l'attività è completata.

Tabella 1 – SLA Assessment, Piano di Esecuzione e Avvio dei Servizi (Lotto 1 e Lotto 2)

Tipologia Servizio	Descrizione KPI	SLA Minimo – GG Lavorativi
Assessment e Piano Esecuzione dei Servizi	Tempo dall'invio della Richiesta di Assessment da parte dell'Amministrazione, alla conclusione delle attività di sopralluogo	entro **20 gg** (entro **30 gg** per un numero di sedi coinvolte maggiore di 3)
	Tempo dall'invio della Richiesta di Assessment da parte dell'Amministrazione, all' invio all'Amministrazione del Piano di Esecuzione dei Servizi	entro **40 gg** (entro **50 gg** per un numero di sedi coinvolte maggiore di 3)
	Tempo dall'invio delle richieste di modifica al Piano da parte dell'Amministrazione, all' invio all'Amministrazione del nuovo Piano di Esecuzione dei Servizi	entro **20 gg**
Avvio dei Servizi	Tempo dall'emissione dell'Ordinativo di Fornitura Principale, all'avvio dei servizi	entro **10 gg**
	Tempo dall'invio della Richiesta di aggiornamento del Piano di Esecuzione dei Servizi da parte dell'Amministrazione, all' invio all'Amministrazione della comunicazione di validità della	entro **7 gg**

Tipologia Servizio	Descrizione KPI	SLA Minimo – GG Lavorativi
	richiesta stessa	
Aggiornamento del Piano di Esecuzione dei Servizi	Tempo dall'invio della Richiesta di aggiornamento del Piano di Esecuzione dei Servizi da parte dell'Amministrazione, alla conclusione delle attività di sopralluogo	entro **15 gg** (entro **25 gg** per un numero di sedi coinvolte maggiore di 3)
	Tempo dall'invio della Richiesta di aggiornamento del Piano di Esecuzione dei Servizi da parte dell'Amministrazione, all' invio all'Amministrazione del Piano di Esecuzione dei Servizi aggiornato	entro **30 gg** (entro **40 gg** per un numero di sedi coinvolte maggiore di 3)
	Tempo dall'invio delle richieste di modifica al Piano da parte dell'Amministrazione, all' invio all'Amministrazione del nuovo Piano di Esecuzione dei Servizi Aggiornato	entro **10 gg**
Avvio dei nuovi Servizi	Tempo dall'emissione dell'Ordinativo di integrazione, all'avvio dei servizi	entro **10 gg**

Tabella 2 – SLA Gestione Sistemi, Rete (Lotto 1)

Tipologia Servizio	Descrizione KPI	Livello		
		Sistema Non Critico	Sistema Business Critical	Sistema Mission Critical
Presa in carico	Tempo di presa in carico malfunzionamento	Entro 4 ore	Entro 2 ore	Entro 1 ora
Risoluzione Malfunzionamento nella conduzione dei sistemi	Tempo di risoluzione malfunzionamento	Entro 8 ore	Entro 4 ore	Entro 2 ore
Intervento pianificato nell'ambito della conduzione dei sistemi	Tempo di completamento intervento	Entro 12 ore	Entro 6 ore	Entro 3 ore

Tabella 3 – SLA NOC (Lotto 1)

Tipologia Servizio	Descrizione KPI	Livello		
		Sistema Non Critico	Sistema Business Critical	Sistema Mission Critical
Presa in carico	Tempo di presa in carico malfunzionamento /segnalazione da sistema di monitoraggio	Entro 4 ore	Entro 2 ore	Entro 1 ora
Risoluzione malfunzionamento	Tempo di risoluzione malfunzionamento / segnalazione da sistema di monitoraggio	Entro 8 ore	Entro 4 ore	Entro 2 ore

Tabella 4 – SLA service desk sistemistico (Lotto 1)

Tipologia Servizio	Descrizione KPI	Livello		
		Richiesta su Sistema Non Critico	Richiesta su Sistema Business Critical	Richiesta su Sistema Mission Critical
Richieste al Service Desk sistemistico	Tempo di gestione richieste service desk	Entro 8 ore	Entro 3 ore	Entro 2 ore
	Tasso di risoluzione ticket al service desk (esclusi interventi che richiedono manutenzione HW, e soluzioni IaaS, PaaS, SaaS di fornitori terzi).	Almeno 50%	Almeno 60%	Almeno 70%

Tabella 5 – SLA Gestione Apparati e Sistemi di Sicurezza (Lotto 2)

Tipologia Servizio	Descrizione KPI	Livello di severità		
		BASSA	MEDIA	ALTA
Presa in carico	Tempo di presa in carico malfunzionamento	Entro 4 ore	Entro 2 ore	Entro 1 ora
Risoluzione Malfunzionamento nella conduzione dei sistemi	Tempo di risoluzione malfunzionamento	Entro 8 ore	Entro 4 ore	Entro 2 ore
Intervento pianificato nell'ambito della conduzione dei sistemi	Tempo di completamento intervento	Entro 12 ore	Entro 6 ore	Entro 3 ore

Tabella 6: SLA Monitoraggio in tempo reale eventi di sicurezza (SOC) (Lotto 2)

Tipologia Servizio	Descrizione KPI	Livello di severità		
		BASSA	MEDIA	ALTA
Presa in carico di un alert e prima analisi	Tempo di prima analisi evento di sicurezza/incidente da sistema di monitoraggio indicazione prime contromisure da applicare (identificazione, verifica, notifica)	Entro 2 ore	Entro 1 ora	Entro 30 minuti
Azioni da intraprendere	Indicazione procedure operative di contenimento, gestione dell'incidente, ingaggio del Incident Response Team. Indicazione contromisure da applicare e risoluzione reattiva di incidente di sicurezza	Entro 4 ore	Entro 2 ore	Entro 1 ora

Tabella 7 – SLA Incident Response (Lotto 2)

Tipologia Servizio	Descrizione KPI	Livello di severità		
		BASSA	MEDIA	ALTA
Presa in carico di un alert	Tempo di rilevazione e presa in carico di un alert di incidente di sicurezza (da sistema di monitoraggio e/o da segnalazione SOC)	Entro 12 ore	Entro 8 ore	Entro 4 ore
Convalida e risoluzione	Validazione e gestione dell'incidente, Indicazione contromisure da applicare e risoluzione reattiva e proattiva di incidente di sicurezza	Entro 4 ore	Entro 2 ore	Entro 1 ora

Per quanto attiene all'affidabilità e alla tempestività (Tabella 8) della messa a disposizione delle risorse si deve fare riferimento a:

- la variazione delle risorse (VRIS) nel tempo (per ciascuna fornitura), calcolata secondo la seguente formula, non deve essere superiore al 15% al semestre:

  VRIS = RSOS / RERO * 100

  dove

  RSOS = numero risorse sostituite

  RERO = numero risorse erogate a tempo pieno nel periodo di riferimento
- il tempo di sostituzione/aggiunta di risorse su richiesta del Referente tecnico dell'Amministrazione (RTMP) (durata contrattuale di ciascuna fornitura) calcolato secondo la seguente formula, non deve essere superiore a 10 giorni lavorativi:

  RTMP = Data disponibilità della risorsa – Data della richiesta

Il Fornitore dovrà garantire il passaggio di consegne, senza oneri per l'Amministrazione, nel caso di sostituzione dei tecnici nel corso della validità del contratto. La verifica delle competenze e delle capacità dei nuovi tecnici andrà svolta preventivamente, con trasmissione ai referenti dell'Amministrazione dei relativi curricula, e sul campo durante l'attività di affiancamento, al termine della quale i nuovi tecnici dovranno essere in grado di lavorare in assoluta autonomia. La presa in carico di tale know-how dovrà avvenire a titolo non oneroso per l'Amministrazione.

Tabella 8 – SLA messa a disposizione delle risorse professionali (Lotto 1 e Lotto 2)

Tipologia Servizio	Descrizione KPI	Livello
Messa a disposizione delle risorse	Variazione risorse nel tempo	< 15% a semestre
	Tempo sostituzione / aggiunta	< 10 giorni lavorativi

Tabella 9 – SLA Reportistica (Lotto 1)

Tipologia Servizio	Descrizione KPI	SLA min – GG Lavorativi
Report degli Asset e dei Servizi per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	entro **20 gg**
Report dei Livelli di Servizio conseguiti per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	entro **20 gg**

Tabella 10 – SLA Reportistica (Lotto 2)

Tipologia Servizio	Descrizione KPI	SLA min – GG Lavorativi
Report Servizi di sicurezza per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	entro **20 gg**
Report dei Livelli di Servizio conseguiti per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	entro **20 gg**

ALLEGATI

È parte integrante del presente Capitolato l'Allegato A – Figure professionali

ALLEGATO “A” AL CAPITOLATO TECNICO

LOTTI 1 e 2

PROFILI PROFESSIONALI

(RETTIFICATO)

INDICE

1. PREMESSA

Le figure professionali proposte per lo svolgimento dei servizi oggetto del **Lotto 1** dovranno rispettare i profili di seguito descritti e sintetizzati nella tabella di correlazione tra figure professionali e servizi/attività.

Servizi / Attività	TEM	CET	SPP	SSS	SIM	SIJ	DBS	DBJ	SRS	SRJ	
Servizi di Monitoraggio Sistemi e Reti	X			X	X	X	X	X			
Servizi di Conduzione Operativa Sistemi	X			X	X	X	X	X			
Servizi di Sviluppo e Integrazione Architetture e Sistemi	X	X	X	X	X	X	X	X			
Servizi di Conduzione Operativa Reti	X								X	X	
Servizi di Rete: progettazione e sviluppo	X		X								
Manutenzione Hardware	X				X	X					
Servizi di Service e Performance Management	X										

Legenda

TEM: ICT Operation Manager

CET: Enterprise Architect

SPP: System Architect

SSS: System Administrator Senior

SIM: System Administrator Middle

SIJ: System Administrator Junior

DBS: Database Administrator Senior

DBJ: Database Administrator Junior

SRS: Network Specialist Senior

SRJ: Network Specialist Junior

Le figure professionali proposte per lo svolgimento dei servizi oggetto del **Lotto 2** dovranno rispettare i profili di seguito indicati:

1. Security Project Manager
2. Governance & risk compliance (GRC) consultant
3. Security architect & engineer
4. Security Advisor senior

5. Security Advisor junior
6. Security specialist
7. Security specialist H24
8. Security Analyst senior
9. Security Analyst junior
10. Vulnerability researcher / Ethical Hacker senior
11. Vulnerability researcher / Ethical Hacker junior
12. Incident handler / response senior
13. Incident handler / response junior
14. Digital forensic
15. CyberSecurity & Privacy Legal Advisor

È richiesto che il Fornitore indichi nell'Offerta il mix di risorse che si impegna ad utilizzare per l'erogazione dei servizi remunerati a canone.
Qualunque sia l'organizzazione che il Fornitore intenda proporre per i diversi team, nel formulare la propria Offerta, in particolare **per il Lotto 1** tenga presente la tabella di correlazione tra i servizi e le figure professionali, ferma restando la facoltà per il Fornitore stesso di proporre il mix di figure professionali ritenuto più funzionale alle finalità e agli obiettivi di qualità della fornitura.

Per entrambi i Lotti si precisa che:

- la cultura equivalente può corrispondere, indicativamente: a 4 anni di esperienza lavorativa addizionale in ambito informatico oppure **(per il Lotto 2)** a 3 di esperienza in ambito specialistico della sicurezza informatica;
- nei profili professionali vengono a volte indicate competenze/certificazioni su ambienti tecnologici diversi. È evidente che tali conoscenze devono essere presenti nel complesso delle risorse professionali richieste al fornitore sulle diverse attività e/o servizi e non in un'unica persona e possono essere intese come fra loro alternative, in funzione del servizio di assegnazione e delle esigenze progettuali. Le certificazioni richieste devono essere valide, mantenute valide per tutta la durata della fornitura e comunque **non più vecchie di 3 anni** ad eccezione delle certificazioni che per loro stessa natura non scadono ancorché conseguite prima dei 3 anni.
- rimane fermo l'obbligo per il Fornitore di erogare i servizi richiesti anche a fronte di significative variazioni del contesto tecnologico avvenute in corso d'opera, adeguando le conoscenze del personale impiegato nell'erogazione dei servizi anche mediante percorsi formativi organizzati internamente o inserendo nei gruppi di lavoro risorse con skills adeguate, senza alcun onere aggiuntivo per l'Amministrazione. Pertanto, le competenze e conoscenze tecniche delle figure che seguono non sono da considerarsi esaustive delle esigenze della fornitura, in quanto la Committente potrà richiedere, competenze specifiche in relazione ad ulteriori tematiche, prodotti, sistemi e metodologie.
- requisito fondamentale è individuare figure professionali con una forte propensione alla comunicazione e ai rapporti personali, con l'attitudine ad operare nella Pubblica Amministrazione.

LOTTO 1 - DESCRIZIONE DEI PROFILI PROFESSIONALI

Nei paragrafi seguenti è fornita la descrizione dei profili professionali minimi da impiegare nella fornitura, diversificati, ove significativo, in base al servizio/attività di competenza.

1.1 ICT OPERATION MANAGER

Qualifica professionale	ICT Operation Manager - TEM
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 12 anni di cui almeno 7 nella funzione
Esperienze consolidate	- Comprovata esperienza in progetti complessi e/o di grandi dimensioni - Conduzione di progetti strategici - Comprovata esperienza nel coordinamento di risorse umane - Comprovata esperienza nel garantire, per conto del Fornitore, gli SLA definiti e concordati con l'Amministrazione. - Stima di risorse per realizzazione di progetto - Comprovata esperienza nel garantire l'applicazione degli standard tecnologici e delle policy di sicurezza definite dall'Amministrazione. - Tecniche di gestione progetti - Spiccate capacità relazionali
Conoscenze	- Conoscenze approfondite di tecniche per project e risk management - Conoscenze approfondite su metodologie di analisi, metodologie di documentazione e metodologie di pianificazione - Conoscenze approfondite su Piano di Qualità, la definizione degli standard di progetto, delle procedure e delle metriche - Conoscenza delle principali tendenze evolutive delle architetture tecnologiche per sistemi enterprise; - Conoscenza a livello senior dei sistemi operativi Windows, Linux e Unix; - Conoscenza a livello senior delle problematiche di clustering; - Conoscenza a livello senior delle architetture applicative.NET e J2EE; - Conoscenza a livello senior delle infrastrutture informatiche applicative datacenter oriented; - Conoscenza a livello senior delle architetture applicative a Container; - Conoscenza a livello senior delle architetture applicative in Cloud; - Conoscenza a livello senior delle problematiche di business continuity; - Conoscenza a livello senior delle problematiche d'integrazione in ambienti tecnologici complessi; Si richiede il possesso di almeno una delle seguenti certificazioni: • ITIL® V3 per il disegno e l'operatività dei servizi o ITIL® V4 equivalente • Certificazioni Microsoft per System Engineer

1.2 ENTERPRISE ARCHITECT

Qualifica professionale	Enterprise Architect - CET
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 12 anni di cui almeno 7 nella funzione
Esperienze consolidate	- Analisi e progettazione di sistemi informativi, package, procedure complesse - Redazione di specifiche e documentazione di progetto - Stesura documentazione e manualistica tecnica - Stima di risorse per realizzazione di progetto - Tecniche di gestione progetti - Progettazione test integrati - Capacità di analisi e risoluzione problemi - Spiccate capacità relazionali - Certificazioni nei diversi ambiti tecnologici, ad esempio: SuSe, Red Hat o altra certificazione di una distribuzione Linux; Microsoft server e database; VMWare (VCAP, VCDX); Oracle (DBA Professional/Master, Enterprise manager, ecc.); IBM (Certified specialist, ecc.); Red Hat Openshift o Kubernetes Amazon AWS, Microsoft Azure, Google Cloud Platform (GCP) ITIL expert/intermediate level
Conoscenze in ambito system architecture	- Disegno di architetture tecnologiche complesse (multivendor, container,multicloud); - Attività di dimensionamento sistemi e capacity planning; - Conoscenza delle principali tendenze evolutive delle architetture tecnologiche - Conoscenze approfondita degli elementi tecnologici che costituiscono un sistema complesso (sia On Prem che Cloud-based o a Container); - Conoscenza approfondita degli strumenti tecnologici di CD/CI (Azure, DevOps, Jenkins, GitLab, GitHub, Ansible,…) - Metodologia per l'analisi, il disegno e la revisione dell'IT Service Management; - Analisi delle necessità di impianto delle applicazioni in ambienti complessi.
Conoscenze approfondite in ambito System Administration	- Amministrazione e gestione Sistemi Operativi, installazione, configurazione, personalizzazione/tuning e gestione dei principali sistemi operativi di tipo Open Source (distribuzioni di Linux quali SUSE, Red Hat, Debian, ecc.) e dei sistemi operativi Microsoft, anche in configurazione cluster; - Gestione delle procedure di startup e shutdown;
Conoscenze approfondite in ambito Database e prodotti middleware	- Database administration (Oracle Db, Sql server, mysql, postgress slq, Mongo DB, Cassandra ecc.) - Application Server administration (IBM Websphere, Oracle iAS, Oracle Web Logic, Jboss, Microsoft IIS, ecc..); - Amministrazione dei prodotti per portali applicativi (Oracle Portal, web logic portal, OpenCMS, WebSphere Portal Server, Plone, ecc.) - Applicazioni enterprise conformi agli standard Java 2 Platform Enterprise Edition ed in particolare dei componenti Enterprise JavaBeans, servlet e JavaServer Pages.
Conoscenze approfondite in ambito SAN e Backup	- Tipologie di Raid - Tecnologie e best practice di integrazione tra host e apparati di storage - Mobilità dei dati

	- SCSI e FC – LUN e associazione con File System - Zoning e LUN Masking - Multipathing - Disaster Recovery e funzioni di alta affidabilità degli storage - Remote Mirroring e aggiornamento Sincrono-Asincrono - Orchestrazione del backup - Data loss prevention - Data retention e deduplica - Offline Backup - Object Storage
Conoscenze approfondite in ambito networking	- Amministrazione Sistemi operativi degli apparati di rete - Tecniche di bilanciamento del traffico - Tecniche di ridondanza ed alta affidabilità - Disegno e progettazione di reti TCP/IP complesse - Implementazione di infrastrutture gestionali per reti complesse - Protocolli di rete (Ethernet, FCoE, FDDI, ATM,…) - Protocolli di routing (IGRP, OSPF,…) - Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173) - Apparati di rete (switch, bridge, router, ecc..) - Sistemi di network management - Sicurezza delle reti.
Conoscenze approfondite nell'ambito delle tecnologie di virtualizzazione	- Installazione, configurazione, personalizzazione/tuning e gestione delle tecnologie di virtualizzazione (VMWare, Citrix, Microsoft) in ambienti complessi con storage su SAN - Disegno e implementazione di server, storage e modalità di backup e restore - Supporto di ambienti enterprise.
Conoscenze approfondite in ambito sicurezza	- Amministrazione sistemi operativi degli apparati di sicurezza quali Firewall, terminatori VPN, sistemi di autenticazione forte, ecc. - Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc. - Principali vulnerabilità/tipi di attacchi di rete e dei sistemi - Tecniche di ridondanza ed alta affidabilità - Amministrazione ISS Intrusion Detection/Prevention, SSL Gateways - Amministrazione sistemi Antivirus; - Analisi di problematiche complesse ed individuazione del componente in errore - Comprovata esperienza nella definizione e progettazione di architetture di sicurezza - Approfondita conoscenza dei principali standard di sicurezza (ITSEC, BS7799) - Conduzione di assesment di sicurezza logica, fisica e organizzativa.
Conoscenze approfondite in ambito Operation Management	- Installazione, configurazione, customizzazione, tuning e troubleshooting degli strumenti di system monitoring, application performance monitoring, workload automation, prodotti di analisi log
Conoscenze approfondite in ambito Service Management	- Installazione, configurazione, customizzazione, tuning e troubleshooting dei prodotti di IT Service Management - Metodologia per l'analisi, il disegno, la revisione dell'IT Service Management

1.3 SYSTEM ARCHITECT

Qualifica professionale	System Architect - SPP
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 8 anni di cui almeno 4 nella funzione
Esperienze consolidate	- Analisi e progettazione di sistemi informativi, package, procedure complesse - Redazione di specifiche di progetto - Stima di risorse per realizzazione di progetto - Tecniche di gestione progetti - Controllo realizzazione procedure - Progettazione test integrati - Capacità di analisi e risoluzione problemi - Spiccate capacità relazionali - Certificazioni nei diversi ambiti tecnologici
Conoscenze Linux	Comprovate competenze nell'ambito dei sistemi GNU/Linux ed esperienza di almeno 2 anni nell'installazione e configurazione di Linux su sistemi server e/o infrastrutture professionali. Possiede almeno una delle seguenti conoscenze o ha effettuato una delle esperienze: - progettazione di Sistemi Informativi basati integralmente su FLOSS (Free Libre Open Source Software); - partecipazione a progetti di sviluppo di software Open Source; - certificazione SuSe, Red Hat o altra certificazione di una distribuzione Linux - conoscenza del mondo dell'Open Source Community e dei relativi tool.
Conoscenze sistemi operativi Microsoft	Conoscenza approfondita in tema di installazione, personalizzazione, tuning e troubleshooting di server e client in ambienti Microsoft. In particolare è richiesta una specifica competenza sulle configurazioni cluster Windows MSCS e NLB, sulla tecnologia .NET, sul database SQL Server e Share Point. Certificazioni possedute: - Certificazioni Microsoft per Systems Engineer – Windows Server - Certificazioni Microsoft per Database Administrator - SQL Server - Certificazioni Microsoft per App Builder for Microsoft .NET - Certificazioni Microsoft per Systems Administrator on Microsoft Windows Server
Conoscenze Application Server IBM WebSphere	Specifiche competenze sull'application server WebSphere con particolare riguardo alle attività di analisi delle problematiche complesse ed individuazione del componente in errore comprovate dal possedere la certificazione IBM WebShere Application Server "IBM Certified System Administrator – WebSphere"
Conoscenze Application server Microsoft IIS	- Conoscenza specialistica in tema di installazione, personalizzazione, tuning e troubleshooting del sistema Microsoft Internet Information Services in ambiente Microsoft Windows Server.

	- Richiesta specifica conoscenza dell'application server in tutte le sue componenti.
Conoscenze Application server Open	- Conoscenza specialistica in tema di installazione, personalizzazione, tuning e troubleshooting degli application server Apache Tomcat in ambiente Linux/Unix. - Richiesta specifica conoscenza degli application server in tutte le sue componenti.
Conoscenze specifiche in ambito CMS – MS SharePoint	Conoscenza specialistica in tema di installazione, personalizzazione, tuning e troubleshooting di servizi di gestione dei contenuti in ambienti Microsoft Sharepoint. In particolare è richiesta una specifica competenza sulle tecniche di integrazione dei servizi e di sviluppo di smart application "APP" e della piattaforma in tutte le sue componenti.
Conoscenze specifiche in ambito Microsoft Exchange e Zimbra	- Conoscenza specialistica in tema di installazione, personalizzazione, tuning e troubleshooting del sistema Microsoft Exchange in ambiente Microsoft Windows Server e Zimbra in ambiente Linux. Richiesta specifica conoscenza della piattaforma in tutte le sue componenti.
Conoscenze nell'ambito delle tecnologie di virtualizzazione	- Conoscenza approfondita della tecnologia VMWare, con particolare riferimento a piattaforma ESX/ESXi, in ambienti complessi con storage su SAN. - Esperienza nel disegno e implementazione di soluzioni di virtualizzazione dei client (VDI), dei server e delle applicazioni attraverso le maggiori tecnologie di virtualizzazione (VMWARE, CITRIX e Microsoft Hyper-V). - Supporto di ambienti enterprise (hardware x86, VMWare Virtual Infrastructure, amministrazione di sistemi Windows e Linux) utilizzando best practices standard e processi operativi (ITIL like). - Esperienza nell'installazione, personalizzazione e test di prodotto, applicazione di patch e service pack. - Esperienza nel disegno e implementazione di server, storage e modalità di backup e restore (VMWARE consolidated backup). - Possiede le certificazioni VMWare VCP-DCV
Conoscenze Oracle RDBMS e Oracle Fusion Middleware	Skill specifico nella gestione di database large-scale e di applicazioni "enterprise". Conseguimento dei titoli previsti dal programma Oracle Certified Professional. Conoscenza approfondita in tema di installazione, tuning, personalizzazione e trouble shooting di prodotti Oracle del tipo: - Oracle RDBMS (RAC); - Oracle Enterprise MGR, Grid Control; Certificazione: Varie Piattaforme Oracle
Conoscenze nell'ambito delle tecnologie Java	Possiede conoscenze specialistiche delle applicazioni enterprise conformi agli standard Java 2 Platform Enterprise Edition ed in particolare dei componenti Web Services (JAX-RS e JAX-WS), Java Servlet, JavaServer Faces (JSF), JavaServer Pages (JSP), Enterprise JavaBeans (EJB), nonché i client Java che li utilizzano. Possiede certificazioni Oracle o equivalenti in ambito Java.

Conoscenza piattaforme di Backup	Possiede conoscenze approfondite dell'infrastruttura e dei prodotti di backup (Tivoli, Commvault, ecc..) con una esperienza di almeno 5 anni maturata sulle problematiche relative.
Conoscenze altre piattaforme Enterprise	Possiede conoscenze approfondite dell'infrastruttura e dei prodotti SAP e SAS con una esperienza di almeno 5 anni maturata sulle problematiche relative.

1.4 SYSTEM ADMINISTRATOR SENIOR

Qualifica professionale	System Administrator Senior - SSS
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 10 anni, di cui almeno 5 nella funzione
Esperienze consolidate	- Problem determination e problem solving - Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi - Tecniche di gestione progetti - Elaborazione e redazione di specifiche di progetto e di studi di fattibilità - Conoscenze di best practices ITIL - Tecniche di progettazione e dimensionamento di architetture hardware/software - Tecniche di pianificazione - Tecniche e strumenti di monitoraggio - Tecniche di analisi del rischio - Controllo della qualità del servizio - Controllo dello stato di avanzamento delle attività - Progettazione, analisi e realizzazione di architetture di BC/DR - Sistemista DB/DC in ambiente open e loro sottosistemi - Progettazione, analisi, disegno e realizzazione di test integrati tra diversi sistemi di gestione dati - Progettazione, analisi e realizzazione di architetture di BC/DR nell'ambito degli ambienti inerenti il presente profilo. - Operativi (UNIX, Linux, Windows) e con altri middleware (DB2, CICS, Oracle, WebSphere) - Partecipazione alla progettazione e realizzazione di test integrati tra DBMS eterogenei - Architetture client/server e web - Architetture a Container e Cloud - Protocollo e architettura di rete TCP/IP - Ambienti LAN e WAN
Conoscenze specifiche approfondite	- Architetture di BC/DR - Tematiche applicative gestionali, preferibilmente in ambito Pubblica Amministrazione - Tecniche di problem solving - assistenza alla risoluzione dei problemi che gli utenti possono incontrare nell'interazione con i servizi di business dell'Amministrazione - supporto per l'utilizzo corretto dei servizi di business
System Administration	- Gestione Data Center, con particolare riguardo alle tecnologie HP, IBM, FUJITSU e DELL - Sistemi di gestione Blade - Amministrazione e gestione Sistemi Operativi Microsoft

	- Installazione, configurazione, personalizzazione/tuning e gestione del sistema operativodei principali sistemi operativi di tipo Open Source (distribuzioni di Linux quali Red Hat, SuSe,) - Configuration management - Analisi e progettazione di sistemi informativi, package e procedure complesse - Configurazione e personalizzazione/tuning di cluster dei principali sistemi operativi di tipo Open Source (distribuzioni di Linux quali Red Hat, SuSe) - Personalizzazione protezione file di sistema (es. password, group, hosts) - Gestione delle procedure di startup e shutdown; - Conoscenza (installazione, configurazione, personalizzazione/tuning e gestione) dei seguenti prodotti: Database Management System RDBMS: DB2 - Oracle – SQL Server – MySQL – PostgreSQL Database Management System NoSQL: Mongo DB, Cassandra Application Server: IBM Websphere - Oracle Application Server - Apache/Tomcat – Jboss, Oracle Fusion Middleware Business Intelligence : Business objects– prodotti di ETL (ad esempio Power Center e InfoSphere) Web server: Apache, Oracle application HR, OFA, OGL, OHS Oracle portal, Oracle login server UCM, Content Server e Bea Web Logic - Prodotti di analisi log (es. Webtrend) Conoscenza approfondita delle tecniche di eliminazione delle vulnerabilità dei sistemi.
Amministrazione Database in ambiente open e prodotti middleware	- Database administration (DB2, Oracle, SQL, mysql, PostGresSQL, MongoDB, Cassandra) - Analisi performance e tuning Database - Supporto allo sviluppo applicativo - Studio metodologie di recovery/backup: utilities, concurrent copy, flash copy, time finder, mirroring (SRDF) - Personalizzazione e utilizzo tools - Application Server administration (Oracle iAS, Oracle Web Logic, jboss,ecc..) - Amministrazione dei prodotti per portali applicativi (Oracle Portal, web logic portal, OpenCMS, WebSphere Portal Server, Liferay, ecc.) - Oracle Identity Management - Oracle Active Data Guard - Architetture SOA/cooperazione applicativa e modelli concettuali correlati (XML, SOAP, WSDL, UDDI) - Business Intelligence: metodologie di progettazione e amministrazione prodotti (business object, ecc.). - Amministrazione di sistemi di collaborazione (es. MS Sharepoint, MS Teams)

Test integrati	- Progettazione, analisi, disegno e realizzazione di test integrati tra diversi sistemi di gestione dati (DB2, Oracle, ..). - Progettazione e realizzazione di test integrati con altre piattaforme (Superdome, System P, Intel), con altri Sistemi Operativi (UNIX, Linux, Windows) e con altri middleware (DB2, CICS, Oracle, WebSphere). - Progettazione, analisi e realizzazione di architetture di BC/DR nell'ambito degli ambienti inerenti il presente profilo. - Redazione di specifiche di progetto
Conoscenze in ambito SAN e Backup	- Concetti e tipologie di Raid - Padronanza dei comandi necessari per i diversi host collegati ai box EMC2, IBM - Padronanza di soluzioni di virtualizzazione dello storage (ad esempio IBM SAN volume controller, per la gestione di ambienti multivendor) - Tecnologie e best practice di integrazione per i diversi host collegati agli apparati di storage - Concetti di mobilità dei dati - Multipathing - Zoning e LUN Masking - Disaster Recovery e funzioni di alta affidabilità degli storage - Remote Mirroring e aggiornamento Sincrono-Asincrono - Concetti di orchestrazione del backup - Concetti di data loss prevention - Concetti di data retention e deduplica - Offline Backup - Object Storage
Conoscenze in ambito networking	- Amministrazione Sistemi operativi degli apparati di rete - Tecniche di bilanciamento del traffico - Tecniche di ridondanza ed alta affidabilità - Disegno e progettazione di reti TCP/IP complesse - Implementazione di infrastrutture gestionali per reti complesse - Protocolli di rete (Ethernet, FCoE, FDDI, ATM,…) - Protocolli di routing (IGRP, OSPF,…) - Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173) - Reti di trasporto ottiche, tecnologia DWDM, Cisco Ons 15454 - Apparati di rete (switch, bridge, router, ecc..) - Sistemi di network management - Sistemi di network monitoring proprietari (Cisco Works, ecc.) ed open source (Zabbix, NAGIOS, MRTG, ecc) - Sistemi di Analisi e Problem determination proprietari ed Open Source (Tcpdump, Wireshark, Flow tools ecc.) - Sicurezza delle reti - Sicurezza perimetrale (Cisco Pix-Firewall, Cisco FW-Blade, Iptables) e logica (sistemi IDS ed IPS proprietari ed Open Source - Snort, ecc., Vpn , Nac, Ldap, 802.1x ecc.) - Protocolli di crittografia (IPSEC, PPtp, L2tp,ecc.) - Infrastruttura PKI (certificati digitali, ecc.) - Partecipazione ad analisi e disegno di progetti di reti WIRELESS, LAN, WAN in

	presenza di architetture diverse (SNA, TCP/IP) e con supporto di traffico multimediale - Installazione personalizzazione e utilizzo di: VTAM, TCP/IP, MPLS, PPP, ISDN, NCP, Router, Switch, Access server, protocolli di routing (RIP, OSPF), Multicast, VoIP, applicativi video on demand, QoS
Conoscenze nell'ambito delle tecnologie di virtualizzazione	- Conoscenza approfondita (installazione, configurazione, personalizzazione/tuning e gestione) delle tecnologie di virtualizzazione (VMWare, Citrix, Microsoft) in ambienti complessi con storage su SAN - Disegno e implementazione di server, storage e modalità di backup e restore (anche su infrastruttura virtuale) - Supporto di ambienti enterprise (hardware x86, VMWare Virtual Infrastructure, amministrazione di sistemi Windows e Linux)
Conoscenze specifiche in ambito Microsoft	- Amministrazione Sistemi operativi Windows - Progettazione ed implementazione di infrastrutture basate su piattaforme Microsoft - Amministrazione e configurazione: - Active directory e directory services - Active directory server role - Group policy ed impatto sui client del dominio - Network access e remote access - Windows deployment services - Terminal services - Windows registry - Windows services - Remote desktop - Certificate management - Conoscenza approfondita (installazione, configurazione, personalizzazione/tuning e gestione) di: sistema operativo Windows Server .Net Framework cluster Windows MSCS Network Load Balancing (NLB) Personalizzazione, configurazione delle componenti di back office, configurazione e personalizzazione/tuning file system Microsoft, anche in ambiente cluster Configurazione e personalizzazione/tuning cluster Microsoft Conoscenza approfondita (installazione, configurazione, personalizzazione/tuning e gestione) dei seguenti prodotti: - SQL server, IIS, Microsoft SharePoint, Microsoft Exchange, Microsoft System Center Configuration Manager SCCM , Microsoft Data Protection Manager, Microsoft Teams, Microsoft Forefront Identity Manager
Conoscenze in ambito sicurezza e log management	- Amministrazione sistemi operativi degli apparati di sicurezza quali Firewall, terminatori VPN, sistemi di autenticazione forte, ecc. - Protocolli applicativi di base quali http, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc.

	- Principali vulnerabilità/tipi di attacchi di rete e dei sistemi - Tecniche di ridondanza ed alta affidabilità - Amministrazione ISS Intrusion Detection/Prevention, SSL Gateways - Amministrazione sistemi di Log Management SIEM (es. RSA Envision) - Amministrazione sistemi Antivirus (es. McAfee) - Analisi di problematiche complesse ed individuazione del componente in errore - Comprovata esperienza nella definizione e progettazione di architetture di sicurezza - Approfondita conoscenza dei principali standard di sicurezza (ITSEC, CC, BS7799) - Conduzione di assessment di sicurezza logica, fisica e organizzativa.
Conoscenza piattaforme di CD/CI	Conoscenza approfondita in tema di installazione, personalizzazione, tuning e troubleshooting delle piattaforme di CD/CI. Richiesta specifica conoscenza delle tecnologie Azure, DevOps, GitLab, GitHub, Ansible, Maven, Docker, Terraform, ecc…
Conoscenza piattaforme di Containerizzazione	Conoscenza approfondita in tema di installazione, personalizzazione, tuning e troubleshooting delle piattaforme di Containerizzazione, con particolare riferimento alle funzioni di automation, orchestration e provisioning. Richiesta specifica conoscenza di tipologie e architetture di Containerizzazione basate su piattaforma Kubernates (es. OpenShift)
Conoscenza piattaforme Cloud Computing	Conoscenza approfondita in tema di installazione, personalizzazione, tuning e troubleshooting della piattaforme di Cloud Computing, con particolare riferimento alle funzioni di automation, orchestration e provisioning. Richiesta specifica conoscenza di tipologie e architetture di Cloud Computing basate su piattaforme Amazon Web Services (AWS), Azure Microsoft, Google Cloud Platform (GCP)
Conoscenze in ambito Service Management	- Metodi di Business Process Rengineering - Conoscenza approfondita sui processi e sui principali prodotti disponibili per la razionalizzazione di: Service Desk Incident management Problem management Change Management Service Request Management Knowledge management - Competenze di data modeling, disegno e sviluppo di procedure ETL - Esperienza nell'attività di integrazione tra diversi sistemi informativi - Esperienza nell'attività di predisposizione e conduzione di sessioni formative e di coaching - Partecipazione a progetti di Service Management dell' IT - Conoscenza approfondita delle principali metodologie e best practices sul Service Management IT (Cobit, ITIL, ISO 20000)
Certificazioni	Si richiede il possesso di una o più delle seguenti certificazioni: - ITIL® V3 per l'operatività dei servizi o ITIL® V4 equivalente ; - Certificazioni Microsoft per System Engineer

	- Certificazioni Microsoft per Technology Specialist SQL Server; - Oracle OCP DBA - SAP Certified - VMware Certified Professional (VCP) - LBL®LoadBalancer Application Availability Infrastructure 1° e 2° livello; - Trend Micro Certified Security Expert (TCSE); - CCA - Citrix Certified Administrator - Red Hat Certified Engineer (RHCE) - Red Hat Certified Specialist in OpenShift Administration - Amazon AWS, Microsoft Azure, Google Cloud Platform (GCP)

1.5 SYSTEM ADMINISTRATOR MIDDLE

Qualifica professionale	System Administrator – SIM
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 6 anni, di cui almeno 4 nella funzione
Esperienze consolidate	- Interazione e relazione con gli utenti; - Gestione delle interazioni, riguardo alle competenze ed alle responsabilità del settore di competenza nei confronti degli ambiti applicativi, di rete e sistemistici; - Problem determination e problem solving; - Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi; - Elaborazione e redazione di specifiche di progetto e di studi di fattibilità; - Metodologie di project management e di best practices ITIL; - Tecniche di progettazione e dimensionamento di architetture hardware/software; - Tecniche di pianificazione; - Tecniche e strumenti di monitoraggio; - Tecniche di analisi del rischio; - Controllo della qualità del servizio; - Controllo dello stato di avanzamento della attività; - Progettazione test integrati; - Certificazioni nei diversi ambiti tecnologici
Conoscenze in ambito System Administration	- Amministrazione e gestione Sistemi Operativi, installazione, configurazione, personalizzazione/tuning e gestione dei principali sistemi operativi di tipo Open Source (distribuzioni di Linux quali SUSE, Red Hat, Debian, ecc.) e dei sistemi operativi Microsoft, anche in configurazione cluster; - Personalizzazione di file di sistema (es. password, group, hosts) - Gestione delle procedure di startup e shutdown; - Attività di tuning applicativo e ottimizzazione con l'uso di strumenti per il test di carico.
Conoscenze in ambito Database e prodotti middleware	- Database administration (Oracle Db, Sql server, mysql, postgress slq, MongoDB, Cassandra ,ecc.) - Application Server administration (IBM Websphere, Oracle iAS, Oracle Web Logic, jboss, Microsoft IIS, ecc..); - Amministrazione dei prodotti per portali applicativi (Oracle Portal, web logic portal, OpenCMS, WebSphere Portal Server, Plone, ecc.) - Applicazioni enterprise conformi agli standard Java 2 Platform Enterprise Edition ed in particolare dei componenti Enterprise JavaBeans, servlet e JavaServer Pages:

	- Ottimizzazione delle strutture dati.
Conoscenze approfondite in ambito SAN e Backup	- Tipologie di Raid - Tecnologie e best practice di integrazione tra host e apparati di storage - Mobilità dei dati - SCSI e FCS – LUN e associazione con File System - Zoning e LUN Masking - Multipathing - Disaster Recovery e funzioni di alta affidabilità degli storage - Remote Mirroring e aggiornamento Sincrono-Asincrono - Orchestrazione del backup - Data loss prevention - Data retention e deduplica - Offline Backup - Object Storage
Conoscenze in ambito networking	- Amministrazione Sistemi operativi degli apparati di rete - Tecniche di bilanciamento del traffico - Tecniche di ridondanza ed alta affidabilità - Disegno e progettazione di reti TCP/IP complesse - Implementazione di infrastrutture gestionali per reti complesse - Protocolli di rete (Ethernet, FCoE, FDDI, ATM,…) - Protocolli di routing (IGRP, OSPF,…) - Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173) - Apparati di rete (switch, bridge, router, ecc..) - Sistemi di network management - Sicurezza delle reti.
Conoscenze nell'ambito delle tecnologie di virtualizzazione	- Installazione, configurazione, personalizzazione/tuning e gestione delle tecnologie di virtualizzazione (VMWare, Citrix, Microsoft) in ambienti complessi con storage su SAN - Disegno e implementazione di server, storage e modalità di backup e restore - Supporto di ambienti enterprise.
Conoscenze specifiche in ambito Microsoft	- Amministrazione Sistemi operativi Windows - Progettazione ed implementazione di infrastrutture basate su piattaforme Microsoft - Amministrazione e configurazione: - Active directory e directory services - Active directory server role - Group policy ed impatto sui client del dominio - Network access e remote access - Windows deployment services - Terminal services - Windows registry - Windows services - Remote desktop - Certificate management - Conoscenza approfondita (installazione, configurazione, personalizzazione/tuning e gestione) di: sistema operativo Windows Server .Net Framework cluster Windows MSCS Network Load Balancing (NLB)

	Personalizzazione e configurazione componenti di back office, configurazione e personalizzazione/tuning file system Microsoft, anche in ambiente cluster Configurazione e personalizzazione/tuning cluster Microsoft Conoscenza approfondita (installazione, configurazione, personalizzazione/tuning e gestione) dei seguenti prodotti: - SQL server - IIS - Microsoft SharePoint - Microsoft Exchange - Microsoft System Center Configuration Manager SCCM - Microsoft Data Protection Manager - Microsoft Teams - Microsoft ISA, TMG e successive - Microsoft Forefront Identity Manager
Conoscenze in ambito sicurezza	- Amministrazione sistemi operativi degli apparati di sicurezza quali Firewall, terminatori VPN, sistemi di autenticazione forte, ecc. - Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc. - Principali vulnerabilità/tipi di attacchi di rete e dei sistemi - Tecniche di ridondanza ed alta affidabilità - Amministrazione ISS Intrusion Detection/Prevention, SSL Gateways - Amministrazione sistemi Antivirus; - Analisi di problematiche complesse ed individuazione del componente in errore - Comprovata esperienza nella definizione e progettazione di architetture di sicurezza - Approfondita conoscenza dei principali standard di sicurezza (ITSEC, BS7799) - Conduzione di assessment di sicurezza logica, fisica e organizzativa.
Conoscenze in ambito Operation Management	- Installazione, configurazione, customizzazione, tuning e troubleshooting degli strumenti di system monitoring, application performance monitoring, workload automation, prodotti di analisi log
Conoscenze in ambito Service Management	- Installazione, configurazione, customizzazione, tuning e troubleshooting dei prodotti di IT Service Management - Controllo dei Processi IT e delle relative procedure operative
Conoscenze in ambito Client	- Architetture dei sistemi client Microsoft e Linux - principali prodotti di software distribution e di remote desktop control - sistemi operativi client e dispositivi mobili (es. Windows, Apple, Android) - web browser (es. Internet Explorer, Firefox, Chrome, Safari) - antivirus (es. MCAfee, Norton, Kaspersky ecc.) - Sistemi di virtualizzazione (es. XenApp, XenDesktop)
Certificazioni	Si richiede il possesso di una o più delle seguenti certificazioni: - ITIL® V3 per l'operatività dei servizi o ITIL® V4 equivalente; - RedHat Certified Engineer RHCE; - Certificazioni Microsoft per System Engineer - SAP NetWeaver Security; - VMware Certified Professional (VCP) - CCA - Citrix Certified Administrator - IBM Certified Specialist - Open System Storage Solutions;

	- IBM Certified System Administrator - WebSphere App. Server Network Deployment; - LBL®LoadBalancer Application Availability Infrastructure 1° livello.

1.6 SYSTEM ADMINISTRATOR JUNIOR

Qualifica professionale	System Administrator Junior – SIJ
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 3 anni, di cui almeno 1 nella funzione
Esperienze consolidate	- Interazione e relazione con gli utenti; - Gestione delle interazioni, riguardo alle competenze ed alle responsabilità del settore di competenza nei confronti degli ambiti applicativi, di rete e sistemistici; - Problem determination e problem solving; - Supporto alla redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi; - Supporto all'elaborazione ed alla redazione di specifiche di progetto e di studi di fattibilità; - Metodologie di project management e di best practices ITIL; - Certificazioni nei diversi ambiti tecnologici
Conoscenze base in ambito System Administration	- Amministrazione e gestione Sistemi Operativi, installazione, configurazione, personalizzazione/tuning e gestione dei principali sistemi operativi di tipo Open Source (distribuzioni di Linux quali SUSE, Red Hat, Debian, ecc.) e dei sistemi operativi Microsoft, anche in configurazione cluster; - Personalizzazione di file di sistema (es. password, group, hosts) - Gestione delle procedure di startup e shutdown; - Attività di tuning applicativo e ottimizzazione con l'uso di strumenti per il test di carico.
Conoscenze base in ambito Database e prodotti middleware	- Database administration (Oracle Db, Sql server, mysql, postgress slq, ecc.) - Application Server administration (IBM Websphere, Oracle iAS, Oracle Web Logic, jboss,Microsoft IIS, ecc..); - Amministrazione dei prodotti per portali applicativi (Oracle Portal, web logic portal, OpenCMS, WebSphere Portal Server, ecc.) - Applicazioni enterprise conformi agli standard Java 2 Platform Enterprise Edition ed in particolare dei componenti Enterprise JavaBeans, servlet e JavaServer Pages; - Ottimizzazione delle strutture dati.
Conoscenze base in ambito SAN e Backup	- Tipologie di Raid - Tecnologie e best practice di integrazione tra host e apparati di storage - Mobilità dei dati - SCSI e FCS – LUN e associazione con File System - Zoning e LUN Masking - Multipathing - Disaster Recovery e funzioni di alta affidabilità degli storage - Remote Mirroring e aggiornamento Sincrono-Asincrono - Orchestrazione del backup - Data loss prevention - Data retention e deduplica
Conoscenze base in ambito networking	- Amministrazione Sistemi operativi degli apparati di rete - Tecniche di bilanciamento del traffico - Tecniche di ridondanza ed alta affidabilità

	- Disegno e progettazione di reti TCP/IP complesse - Implementazione di infrastrutture gestionali per reti complesse - Protocolli di rete (Ethernet, FCoE, FDDI, ATM,…) - Protocolli di routing (IGRP, OSPF,…) - Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173) - Apparati di rete (switch, bridge, router, ecc..) - Sistemi di network management - Sicurezza delle reti.
Conoscenze base nell'ambito delle tecnologie di virtualizzazione	- Installazione, configurazione, personalizzazione/tuning e gestione delle tecnologie di virtualizzazione (VMWare, Citrix, Microsoft) in ambienti complessi con storage su SAN - Disegno e implementazione di server, storage e modalità di backup e restore - Supporto di ambienti enterprise.
Conoscenze base in ambito sicurezza	- Amministrazione sistemi operativi degli apparati di sicurezza quali Firewall, terminatori VPN, sistemi di autenticazione forte, ecc. - Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc. - Principali vulnerabilità/tipi di attacchi di rete e dei sistemi - Tecniche di ridondanza ed alta affidabilità - Amministrazione ISS Intrusion Detection/Prevention, SSL Gateways - Amministrazione sistemi Antivirus; - Analisi di problematiche complesse ed individuazione del componente in errore - Comprovata esperienza nella definizione e progettazione di architetture di sicurezza - Approfondita conoscenza dei principali standard di sicurezza (ITSEC, BS7799) - Conduzione di assessment di sicurezza logica, fisica e organizzativa.
Conoscenze base in ambito Operation Management	- Installazione, configurazione, customizzazione, tuning e troubleshooting degli strumenti di system monitoring, application performance monitoring, workload automation, prodotti di analisi log
Conoscenze base in ambito Service Management	- Installazione, configurazione, customizzazione, tuning e troubleshooting dei prodotti di IT Service Management - Controllo dei Processi IT e delle relative procedure operative
Certificazioni	Si richiede il possesso di una o più delle seguenti certificazioni: - ITIL® V3 foundation o ITIL® V4 equivalente ; - Red Hat Certified System Administrator (RHCSA); - Certificazioni Microsoft per System Administrator; - VMware Certified Professional (VCP) - CCA - Citrix Certified Administrator

1.7 DATABASE ADMINISTRATOR SENIOR

Qualifica professionale	Database Administrator Senior - DBS
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 10 anni, di cui almeno 5 nella funzione
Esperienze consolidate	- Problem determination e problem solving - Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi - Tecniche di gestione progetti - Elaborazione e redazione di specifiche di progetto e di studi di fattibilità - Conoscenze di best practices ITIL - Tecniche di progettazione e dimensionamento di architetture hardware/software - Tecniche di pianificazione - Tecniche e strumenti di monitoraggio - Tecniche di analisi del rischio - Controllo della qualità del servizio - Controllo dello stato di avanzamento delle attività - Progettazione, analisi e realizzazione di architetture di BC/DR - Progettazione, analisi, disegno e realizzazione di test integrati tra diversi sistemi di gestione dati - Progettazione, analisi e realizzazione di architetture di BC/DR nell'ambito degli ambienti inerenti il presente profilo. - Partecipazione alla progettazione e realizzazione di test integrati tra DBMS eterogenei
Conoscenze	- Conoscenza a livello operativo dei sistemi Windows, Linux e Unix; - Conoscenza a livello senior dei sistemi Oracle, SQL Server, MySql e PostGreSQL, MongoDB, Cassandra; - Conoscenza a livello operativo delle problematiche di networking; - Conoscenza a livello senior delle problematiche di clustering in ambito database; - Conoscenza a livello senior delle architetture applicative .NET e J2EE in ambito database; - Conoscenze a livello senior delle piattaforme software enterprise (SAP, SAS e BO) in ambito database; - Conoscenza a livello senior delle problematiche di monitoring e performance tuning in ambito database; - Conoscenza a livello senior delle problematiche di storage su architetture SAN in ambito database; - Conoscenza a livello senior delle problematiche di consolidation in ambito database; - Conoscenza a livello senior delle problematiche di business continuity e disaster recovery in ambito database.
Conoscenze in ambito SAN e Backup	- Concetti e tipologie di Raid - Padronanza dei comandi necessari per i diversi host collegati ai box EMC2, IBM - Padronanza di soluzioni di virtualizzazione dello storage (ad esempio IBM SAN volume controller, per la gestione di ambienti multivendor) - Tecnologie e best practice di integrazione per i diversi host collegati agli apparati di storage - Concetti di mobilità dei dati

	- Multipathing - Zoning e LUN Masking - Disaster Recovery e funzioni di alta affidabilità degli storage - Remote Mirroring e aggiornamento Sincrono-Asincrono - Concetti di orchestrazione del backup - Concetti di data loss prevention - Concetti di data retention e deduplica - Offline Backup - Object Storage
Conoscenze in ambito Service Management	- Metodi di Business Process Rengineering - Conoscenza approfondita sui processi e sui principali prodotti disponibili per la razionalizzazione di: Service Desk Incident management Problem management Change Management Service Request Management Knowledge management - Competenze di data modeling, disegno e sviluppo di procedure ETL - Esperienza nell'attività di integrazione tra diversi sistemi informativi - Esperienza nell'attività di predisposizione e conduzione di sessioni formative e di coaching - Partecipazione a progetti di Service Management dell' IT - Conoscenza approfondita delle principali metodologie e best practices sul Service Management IT (Cobit, ITIL, ISO 20000)
Certificazioni	Si richiede il possesso di una o più delle seguenti certificazioni: - ITIL® V3 per l'operatività dei servizi o ITIL® V4 equivalente ; - Certificazioni Microsoft per Database Administrator - SQL Server - Oracle OCP DBA - Oracle Certified Associate PL/SQL Developer; - Managing Oracle on Linux Certified Expert; - SAP NetWeaver Sys. Admin. Oracle.

1.8 DATABASE ADMINISTRATOR JUNIOR

Qualifica professionale	Database Administrator Junior - DBJ
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 3 anni, di cui almeno 2 nella funzione
Esperienze consolidate	- Problem determination e problem solving - Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi - Tecniche di gestione progetti - Elaborazione e redazione di specifiche di progetto e di studi di fattibilità - Conoscenze di best practices ITIL - Tecniche di progettazione e dimensionamento di architetture hardware/software - Tecniche e strumenti di monitoraggio - Controllo della qualità del servizio - Controllo dello stato di avanzamento delle attività - Partecipazione alla progettazione e realizzazione di test integrati tra DBMS eterogenei
Conoscenze	- Conoscenza a livello operativo dei sistemi Windows, Linux e Unix; - Conoscenza a livello operativo dei sistemi Oracle, SQL Server, MySql e PostGreSQL; - Conoscenza a livello operativo delle problematiche di networking; - Conoscenza a livello operativo delle problematiche di clustering in ambito database; - Conoscenza a livello operativo delle architetture applicative .NET e J2EE in ambito database; - Conoscenza a livello operativo delle problematiche di monitoring e performance tuning in ambito database.
Conoscenze in ambito SAN e Backup	- Concetti e tipologie di Raid - Padronanza dei comandi necessari per i diversi host collegati ai box - Padronanza di soluzioni di virtualizzazione dello storage (ad esempio IBM SAN volume controller, per la gestione di ambienti multivendor) - Tecnologie e best practice di integrazione per i diversi host collegati agli apparati di storage - Concetti di mobilità dei dati - Multipathing - Zoning e LUN Masking - Disaster Recovery e funzioni di alta affidabilità degli storage - Remote Mirroring e aggiornamento Sincrono-Asincrono - Concetti di orchestrazione del backup - Concetti di data loss prevention - Concetti di data retention e deduplica
Conoscenze in ambito Service Management	- Conoscenza base sui processi e sui principali prodotti disponibili per la razionalizzazione di: Service Desk Incident management Problem management Change Management Service Request Management Knowledge management

	- Competenze di data modeling, disegno e sviluppo di procedure ETL - Esperienza nell'attività di integrazione tra diversi sistemi informativi - Partecipazione a progetti di Service Management dell' IT
Certificazioni	Si richiede il possesso di una o più delle seguenti certificazioni: - ITIL® V3 foundation o ITIL® V4 equivalente ; - Certificazioni Microsoft per Database Administrator - SQL Server - Oracle OCP DBA

1.9 NETWORK SPECIALIST SENIOR

Qualifica professionale	Network Specialist Senior - SRS
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 7 anni di cui almeno 3 nella funzione
Esperienze consolidate	- Problem determination e problem solving - Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi - Tecniche di gestione progetti - Elaborazione e redazione di specifiche di progetto e di studi di fattibilità - Conoscenze di best practices ITIL - Tecniche di pianificazione - Tecniche e strumenti di monitoraggio - Tecniche di analisi del rischio - Controllo della qualità del servizio - Controllo dello stato di avanzamento delle attività - Progettazione, analisi e realizzazione di architetture di BC/DR nell'ambito degli ambienti inerenti il presente profilo. - Architetture client/server e web - Protocollo e architettura di rete TCP/IP - Ambienti LAN e WAN
Conoscenze approfondite	Possiede un'approfondita conoscenza di molteplici architetture tecnologiche e protocolli di rete locale e geografica, e si mantiene aggiornato continuamente sulle loro evoluzioni. È in grado di analizzare i requisiti di comunicazione dei progetti e di disegnare sistemi di rete via cavo e/o senza fili, tenendo conto delle esigenze degli utenti e dei sistemi. È responsabile dell'installazione, configurazione e collegamento tra loro degli apparati di rete, prestando attenzione a garantire sicurezza, prestazioni elevate ed affidabilità dei servizi prestati. Garantisce il presidio ed il buon funzionamento della rete, attraverso la configurazione e l'uso degli appositi strumenti di monitoraggio. È in grado di intervenire in caso di gravi problemi sulla rete, sa analizzarne a fondo le cause e sa trovare e proporre soluzioni alternative per il ripristino dei servizi. Le attività di questa figura professionale sono: -progettare, in collaborazione con i tecnici dell'Amministrazione, le architetture necessarie all'evoluzione dell'infrastruttura di rete, garantendo il rispetto delle policies regionali; -realizzare configurazioni complesse su apparati di rete locale e geografica, anche per gestire protocolli di trasporto multimediali; - ricercare errori e guasti, anche con l'aiuto di strumenti HW e SW dedicati; - risolvere problemi nelle configurazioni; analizzare le prestazioni degli apparati; - collaborare alla gestione degli strumenti di Network Management su piattaforma Open Source e OpenVMS;

	- gestire in autonomia malfunzionamenti complessi sui circuiti di telecomunicazione; - gestire le configurazioni d'interfaccia con i fornitori di connettività, approfondendo le tecnologie di routing dinamico e di gestione del Virtual Routing and Forwarding; - dedicare attenzione agli aspetti di sicurezza interna e perimetrale, dando supporto alla gestione del firewall; - collaborare alla gestione dei Domain Name System pubblici.
Conoscenze approfondite in ambito networking	- Tecniche di bilanciamento del traffico - Tecniche di ridondanza ed alta affidabilità - Protocolli di rete (Ethernet, FCoE, FDDI, ATM,…) - Protocolli di routing (BGP, IGRP, OSPF,…) - Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173) - Apparati di rete (switch, bridge, router, ecc..) - Sistemi di network management - Sicurezza delle reti.
Certificazioni	Si richiede il possesso di una o più delle seguenti certificazioni: - CISCO CCIE - CISCO CCNP - Ulteriori certificazioni specifiche di prodotto nell'ambito networking

1.10 NETWORK SPECIALIST JUNIOR

Qualifica professionale	Network Specialist Junior - SRJ
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 3 anni, di cui almeno 1 nella funzione
Esperienze consolidate	- Interazione e relazione con gli utenti; - Gestione delle interazioni, riguardo alle competenze ed alle responsabilità del settore di competenza nei confronti degli ambiti applicativi, di rete e sistemistici; - Problem determination e problem solving; - Supporto alla redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi; - Supporto all'elaborazione ed alla redazione di specifiche di progetto e di studi di fattibilità; - Metodologie di project management e di best practices ITIL;
Conoscenze approfondite	Conosce le architetture tecnologiche ed i protocolli di rete locale e geografica più diffusi, e si mantiene aggiornato continuamente sulle loro evoluzioni. Sulla base dei documenti di progetto, è in grado di installare, configurare e collegare alle infrastrutture di cablaggio strutturato gli apparati di rete, le postazioni di lavoro ed i server. Verifica il buon funzionamento della rete, attraverso l'uso degli appositi strumenti di monitoraggio. In caso di problemi, si rapporta con gli utenti, con gli altri tecnici che lavorano sulle infrastrutture informatiche dell'Amministrazione e con i fornitori di servizi di connettività, segnalando malfunzionamenti e guasti, che segue fino alla risoluzione. Le attività di questa figura professionale sono: - gestire in autonomia guasti e malfunzionamenti su cablaggi o reti locali e geografiche; - garantire l'help desk specialistico di secondo livello per problematiche di rete; - predisporre la configurazione iniziale ed installare nuovi apparati di rete, su indicazione dei tecnici regionali e dello specialista senior; - mantenere continuamente aggiornata la documentazione online sugli apparati di rete, sui circuiti e sui sistemi di trouble ticketing; - gestire i disservizi sui servizi di telecomunicazione in caso di malfunzionamenti dei circuiti, con apertura delle chiamate verso i fornitori di connettività.
Conoscenze base in ambito networking	- Tecniche di bilanciamento del traffico - Tecniche di ridondanza ed alta affidabilità - Protocolli di rete (Ethernet, FCoE, FDDI, ATM,…) - Protocolli di routing (BGP, IGRP, OSPF,…) - Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173) - Apparati di rete (switch, bridge, router, ecc..) - Sistemi di network management - Sicurezza delle reti.
Certificazioni	Si richiede il possesso di una o più delle seguenti certificazioni: - CISCO CCNA - Ulteriori certificazioni specifiche di prodotto nell'ambito networking

2. LOTTO 2 – DESCRIZIONE DEI PROFILI PROFESSIONALI

Nei paragrafi seguenti è fornita la descrizione dei profili professionali minimi da impiegare nella fornitura, diversificati, ove significativo, in base al servizio/attività di competenza.
Tali figure dovranno possedere preferibilmente le principali certificazioni professionali in ambito sicurezza informatica quali:

- ITIL® V3 / ITIL® V4;
- Auditor IEC/ISO 270xx family
- Certificazione privacy
- CISSP - Certified Information Systems Security Professional
- CompTIA A+
- CompTIA Security+
- CREST Certified Incident Manager
- CSX-P - Cybersecurity Practitioner Certification
- SSCP - Systems Security Certified Practitioner
- Certificazioni di vendor SIEM specifici (es. IBM, MicroFocus/OpenText, ecc)
- Cyber Defense
- Offensive Operations
- Certified Ethical Hacker (C|EH o CEH)
- Certified Hacking Forensic Investigator (C|HFI)
- Certificazioni vendor neutral
- Certificazioni di vendor specifici (es. Checkpoint, Fortinet, TrendMicro, BitDefender, ecc)
- Cloud Security
- GIAC Certified Incident Handler (GCIH)
- CSX Forensics Analysis Certificate
- GIAC Certified Forensic Analyst
- GIAC Reverse Engineering Malware
- CTIA - Certified Threat Intelligence Analyst
- GCTI - GIAC Cyber Threat Intelligence
- CSA - Certified SOC Analyst
- Digital Forensics
- Incident Response.

2.1 SECURITY PROJECT MANAGER

Qualifica professionale	Security project manager
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 5 anni, di cui 4 nella funzione
Profilo professionale	**Progettazione**

	Assiste nella definizione, implementazione e gestione dei progetti di sicurezza informatica sulla base di obiettivi ed esigenze dell'Ente Sviluppa progetti in materia di sicurezza informatica e ne coordina le fasi sino al completamento entro i limiti di tempo e budget assegnati, anche coordinando la comunicazione tra i vari attori coinvolti nel processo
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica ITIL® V3 per il disegno e l'operatività dei servizi o ITIL® V4 equivalente
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Comprovata esperienza nella definizione e progettazione di architetture di sicurezza Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali Conoscenza delle metodologie di analisi, valutazione e gestione del rischio Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità

2.2 GOVERNACE & RISK COMPLIANCE (GRC) CONSULTANT

Qualifica professionale	Governace & risk compliance (GRC) consultant
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 8 anni, di cui 5 nella funzione

Profilo professionale	**Progettazione** Sviluppa e partecipa all'implementazione di progetti per la riduzione del rischio tecnologico, la governance della sicurezza e la conformità alle policy dell'Ente ed alle normative vigenti ed agli standard ISO **Analisi dei rischi** Effettua analisi e valutazioni del rischio di sicurezza informatica Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni, valuta, analizza e rivede in modo continuativo i risultati dell'attività di ricerca su potenziali minacce e delle contromisure adottate **Policy e strategie** Definisce policy, standard, procedure, linee guida e documentazione per la sicurezza dei sistemi Pianifica / esegue / revisiona audit di sicurezza per garantire la conformità alle normative, agli standard ed alle policy dell'Ente Redige ed aggiorna le policy e le procedure di gestione degli incidenti **Processi** Migliora il livello di sicurezza informatica dell'Ente attraverso il miglioramento dei processi di gestione della sicurezza Supporta l'Ente nella progettazione di processi conformi agli standard (ISO27001, GDPR, ecc….) per la gestione degli incidenti Documenta e segnala criticità nei processi esistenti, fornisce indicazioni per il loro miglioramento, fornisce reportistica sulle attività di miglioramento
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica ITIL® V3 per il disegno e l'operatività dei servizi o ITIL® V4 equivalente
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Comprovata esperienza nella definizione e progettazione di architetture di sicurezza Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali

	Conoscenza delle metodologie di analisi, valutazione e gestione del rischio Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità

2.3 SECURITY ARCHITECT & ENGINEER

Qualifica professionale	Security architect & engineer (Specialista infrastrutture e di processo della sicurezza delle informazioni)
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 8 anni, di cui 5 nella funzione
Profilo professionale	**Analisi dei rischi** Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni e supporta lo sviluppo di contromisure di sicurezza e soluzioni per la mitigazione dei problemi rilevati **Policy e strategie** Definisce policy, standard, procedure e misure di sicurezza per la gestione del rischio e ne coordina l'implementazione Supporta la pianificazione delle strategie in materia di sicurezza dei sistemi e delle informazioni Redige ed aggiorna le policy e le procedure di gestione degli incidenti **Processi** Progetta e implementa misure di sicurezza e piani di salvaguardia e ripristino dei dati Progetta misure di sicurezza per proteggere reti e sistemi **Tecnologie e sistemi di sicurezza** Progetta, sviluppa per l'Ente infrastrutture informatiche sicure sfruttando tecnologie e sistemi di sicurezza informatica ed applicando le best practices del settore Supervisiona i processi di change management in chiave di sicurezza dei sistemi Supporta l'Ente nella selezione e implementazione di piattaforme e sistemi di sicurezza
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica

	ITIL® V3 per il disegno e l'operatività dei servizi o ITIL® V4 equivalente
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Comprovata esperienza nella definizione e progettazione di architetture di sicurezza Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali Conoscenza delle metodologie di analisi, valutazione e gestione del rischio Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità

2.4 SECURITY ADVISOR SENIOR

Qualifica professionale	Security Advisor senior
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 5 anni, di cui 3 nella funzione
Profilo professionale	**Analisi dei rischi** Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni, valuta, analizza e rivede in modo continuativo i risultati dell'attività di ricerca su potenziali minacce e delle contromisure adottate **Policy e strategie** Definisce policy, standard, procedure, linee guida e documentazione per la sicurezza dei sistemi Supporta la pianificazione delle strategie in materia di sicurezza dei sistemi e delle informazioni Pianifica / esegue / revisiona audit di sicurezza per garantire la conformità alle normative, agli standard ed alle policy dell'Ente Redige ed aggiorna le policy e le procedure di gestione degli incidenti **Processi**

	Progetta e implementa misure di sicurezza e piani di salvaguardia e ripristino dei dati Progetta misure di sicurezza per proteggere reti e sistemi Tecnologie e sistemi di sicurezza Supervisiona i processi di change management in chiave di sicurezza dei sistemi Supporta l'Ente nella selezione e implementazione di piattaforme e sistemi di sicurezza **Analisi dei sistemi** Valuta ed effettua test dei sistemi di sicurezza utilizzando strumenti e standard del settore **Awareness** Predispone e fornisce materiali inerenti le procedure di sicurezza che il personale deve adottare, interagisce con il personale per l'adozione e l'implementazione di procedure e best practices **Operations** Svolge il ruolo di facilitatore per la gestione della sicurezza informatica nell'operatività dei sistemi e delle postazioni di lavoro
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Comprovata esperienza nella definizione e progettazione di architetture di sicurezza Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali Conoscenza delle metodologie di analisi, valutazione e gestione del rischio Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità Competenze sulle metodologie e sui tool di analisi forense

2.5 SECURITY ADVISOR JUNIOR

Qualifica professionale	Security Advisor junior
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 3 anni, di cui 1 nella funzione
Profilo professionale	**Analisi dei rischi** Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni, valuta, analizza e rivede in modo continuativo i risultati dell'attività di ricerca su potenziali minacce e delle contromisure adottate **Policy e strategie** Definisce policy, standard, procedure, linee guida e documentazione per la sicurezza dei sistemi **Processi** Progetta e implementa misure di sicurezza e piani di salvaguardia e ripristino dei dati Progetta misure di sicurezza per proteggere reti e sistemi **Tecnologie e sistemi di sicurezza** Supervisiona i processi di change management in chiave di sicurezza dei sistemi Supporta l'Ente nella selezione e implementazione di piattaforme e sistemi di sicurezza Analisi dei sistemi Valuta ed effettua test dei sistemi di sicurezza utilizzando strumenti e standard del settore **Awareness** Predispone e fornisce materiali inerenti le procedure di sicurezza che il personale deve adottare, interagisce con il personale per l'adozione e l'implementazione di procedure e best practices **Operations** Svolge il ruolo di facilitatore per la gestione della sicurezza informatica nell'operatività dei sistemi e delle postazioni di lavoro
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi

	Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali Conoscenza delle metodologie di analisi, valutazione e gestione del rischio Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità Competenze sulle metodologie e sui tool di analisi forense

2.6 SECURITY SPECIALIST

Qualifica professionale	Security specialist
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 5 anni, di cui 4 nella funzione
Profilo professionale	**Analisi dei rischi** Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni e supporta lo sviluppo di contromisure di sicurezza e soluzioni per la mitigazione dei problemi rilevati **Policy e strategie** Definisce policy, standard, procedure e misure di sicurezza per la gestione del rischio e ne coordina l'implementazione **Processi** Progetta e implementa misure di sicurezza e piani di salvaguardia e ripristino dei dati Progetta misure di sicurezza per proteggere reti e sistemi **Analisi dei sistemi** Valuta ed effettua test dei sistemi di sicurezza utilizzando strumenti e standard del settore Valuta l'architettura e analizza i sistemi in uso all'Ente per valutare vulnerabilità e rischi per la sicurezza **Awareness** Predispone e fornisce materiali inerenti le procedure di sicurezza che il personale deve adottare, interagisce con il personale per l'adozione e l'implementazione di procedure e best practices **Response e contromisure** A seguito delle minacce di sicurezza rilevate o di eventuali incidenti, suggerisce e sviluppa contromisure Simula scenari di perdita di dati per valutare l'efficacia dei piani di ripristino esistenti **Operations** Installa, configura e gestisce apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc.

	Configura, gestisce ed utilizza sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc. per identificare tempestivamente minacce ed eventi di sicurezza Utilizza sistemi per il monitoraggio di sicurezza delle reti e dei sistemi, ed interpreta gli avvisi generati per comprendere se gli stessi rappresentino o meno una violazione della sicurezza **Gestione incidenti** Individua le cause degli eventi di sicurezza e fornisce soluzioni per mitigare i potenziali danni in caso di violazione Fornisce competenze e leadership al team di gestione degli incidenti Esegue attività al fine di risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica ITIL® V3 per il disegno e l'operatività dei servizi o ITIL® V4 equivalente
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Amministrazione e conduzione operativa di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Amministrazione e conduzione operativa di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Conoscenze approfondite sulle metodologie e sui tool di analisi delle vulnerabilità Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse Conoscenza della metodologia OWASP e delle metodologie di application security testing, conoscenze dei linguaggi di programmazione, database relazionali, tecnologie web e sviluppo del software Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità

2.7 SECURITY SPECIALIST H24

Qualifica professionale	Security specialist H24
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 5 anni, di cui 4 nella funzione
Profilo professionale	**Analisi dei rischi** Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni e supporta lo sviluppo di contromisure di sicurezza e soluzioni per la mitigazione dei problemi rilevati **Policy e strategie** Definisce policy, standard, procedure e misure di sicurezza per la gestione del rischio e ne coordina l'implementazione **Processi** Progetta e implementa misure di sicurezza e piani di salvaguardia e ripristino dei dati Progetta misure di sicurezza per proteggere reti e sistemi **Analisi dei sistemi** Valuta l'architettura e analizza i sistemi in uso all'Ente per valutare vulnerabilità e rischi per la sicurezza **Awareness** Predispone e fornisce materiali inerenti le procedure di sicurezza che il personale deve adottare, interagisce con il personale per l'adozione e l'implementazione di procedure e best practices **Response e contromisure** A seguito delle minacce di sicurezza rilevate o di eventuali incidenti, suggerisce e sviluppa contromisure Simula scenari di perdita di dati per valutare l'efficacia dei piani di ripristino esistenti **Operations** Installa, configura e gestisce apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Configura, gestisce ed utilizza sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... per identificare tempestivamente minacce ed eventi di sicurezza Utilizza sistemi per il monitoraggio di sicurezza delle reti e dei sistemi, ed interpreta gli avvisi generati per comprendere se gli stessi rappresentino o meno una violazione della sicurezza **Gestione incidenti** Individua le cause degli eventi di sicurezza e fornisce soluzioni per mitigare i potenziali danni in caso di violazione Fornisce competenze e leadership al team di gestione degli incidenti Esegue attività al fine di risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza
Conoscenze e competenze	Capacità di comprendere le esigenze del committente

	Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica ITIL® V3 per il disegno e l'operatività dei servizi o ITIL® V4 equivalente
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Amministrazione e conduzione operativa di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Amministrazione e conduzione operativa di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Conoscenze approfondite sulle metodologie e sui tool di analisi delle vulnerabilità Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse Conoscenza della metodologia OWASP e delle metodologie di application security testing, conoscenze dei linguaggi di programmazione, database relazionali, tecnologie web e sviluppo del software Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità

2.8 SECURITY ANALYST SENIOR

Qualifica professionale	Security Analyst senior (malware analyst, Intrusion detection, etc)
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 5 anni, di cui 4 nella funzione
Profilo professionale	**Analisi dei rischi** Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni, valuta, analizza e rivede in modo continuativo i risultati dell'attività di ricerca su potenziali minacce e delle contromisure adottate

	Policy e strategie Pianifica / esegue / revisiona audit di sicurezza per garantire la conformità alle normative, agli standard ed alle policy dell'Ente Tecnologie e sistemi di sicurezza Supporta l'Ente nella selezione e implementazione di piattaforme e sistemi di sicurezza **Analisi dei sistemi** Valuta l'architettura e analizza i sistemi in uso all'Ente per valutare vulnerabilità e rischi per la sicurezza **Operations** Utilizza sistemi per il monitoraggio di sicurezza delle reti e dei sistemi, ed interpreta gli avvisi generati per comprendere se gli stessi rappresentino o meno una violazione della sicurezza **Gestione incidenti** Individua le cause degli eventi di sicurezza e fornisce soluzioni per mitigare i potenziali danni in caso di violazione Effettua attività di reverse engineering per analizzare malware ed il relativo potenziale impatto nel corso di attacchi o a seguito di incidente di sicurezza Analizza le tracce lasciate nel corso di attacchi per comprenderne tattiche e strumenti impiegati **VA & PT** Analizza i report sulle vulnerabilità per determinare i livelli di rischio e consigliare soluzioni per mitigarlo
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Amministrazione e conduzione operativa di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Amministrazione e conduzione operativa di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Conoscenze approfondite sulle metodologie e sui tool di analisi delle vulnerabilità Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse

	Conoscenza della metodologia OWASP e delle metodologie di application security testing, conoscenze dei linguaggi di programmazione, database relazionali, tecnologie web e sviluppo del software Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità

2.9 SECURITY ANALYST JUNIOR

Qualifica professionale	Security Analyst junior
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 3 anni, di cui 2 nella funzione
Profilo professionale	**Analisi dei rischi** Identifica eventuali minacce che incombono sulla sicurezza logica e fisica dei sistemi e delle informazioni, valuta, analizza e rivede in modo continuativo i risultati dell'attività di ricerca su potenziali minacce e delle contromisure adottate **Tecnologie e sistemi di sicurezza** Supporta l'Ente nella selezione e implementazione di piattaforme e sistemi di sicurezza **Analisi dei sistemi** Valuta l'architettura e analizza i sistemi in uso all'Ente per valutare vulnerabilità e rischi per la sicurezza **Operations** Utilizza sistemi per il monitoraggio di sicurezza delle reti e dei sistemi, ed interpreta gli avvisi generati per comprendere se gli stessi rappresentino o meno una violazione della sicurezza **Gestione incidenti** Individua le cause degli eventi di sicurezza e fornisce soluzioni per mitigare i potenziali danni in caso di violazione Effettua attività di reverse engineering per analizzare malware ed il relativo potenziale impatto nel corso di attacchi o a seguito di incidente di sicurezza Analizza le tracce lasciate nel corso di attacchi per comprenderne tattiche e strumenti impiegati **VA & PT** Analizza i report sulle vulnerabilità per determinare i livelli di rischio e consigliare soluzioni per mitigarlo
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate

	Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Amministrazione e conduzione operativa di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Amministrazione e conduzione operativa di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Conoscenze approfondite sulle metodologie e sui tool di analisi delle vulnerabilità Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse Conoscenza della metodologia OWASP e delle metodologie di application security testing, conoscenze dei linguaggi di programmazione, database relazionali, tecnologie web e sviluppo del software Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità

2.10 VULNERABILITY RESEARCHER / ETHICAL HACKER SENIOR

Qualifica professionale	Vulnerability researcher / Ethical Hacker senior
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 5 anni, di cui 4 nella funzione
Profilo professionale	**VA & PT** Analizza i sistemi esposti e la struttura della rete dell'Ente ed identifica potenziali siti di penetrazione. Evidenzia le aree a più alto rischio di sicurezza. Fornisce feedback e suggerimenti per il rimedio o la mitigazione delle vulnerabilità. Effettua analisi di vulnerabilità e penetration test Implementa nuove metodologie di test da applicare, in accordo con l'Ente per le verifica dei sistemi
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate

	Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Conoscenze approfondite sulle metodologie e sui tool di analisi delle vulnerabilità Capacità di individuare le metodologie e i tool di attacco più appropriati per effettuare penetration testing Conoscenza della metodologia OWASP e delle metodologie di application security testing, conoscenze dei linguaggi di programmazione, database relazionali, tecnologie web e sviluppo del software Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)

2.11 VULNERABILITY RESEARCHER / ETHICAL HACKER JUNIOR

Qualifica professionale	Vulnerability researcher / Ethical Hacker junior
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 3 anni, di cui 1 nella funzione
Profilo professionale	**VA & PT** Analizza i sistemi esposti e la struttura della rete dell'Ente ed identifica potenziali siti di penetrazione. Evidenzia le aree a più alto rischio di sicurezza. Fornisce feedback e suggerimenti per il rimedio o la mitigazione delle vulnerabilità. Effettua analisi di vulnerabilità e penetration test Implementa nuove metodologie di test da applicare, in accordo con l'Ente per le verifica dei sistemi
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Conoscenze approfondite sulle metodologie e sui tool di analisi delle vulnerabilità Capacità di individuare le metodologie e i tool di attacco più appropriati per effettuare penetration testing Conoscenza della metodologia OWASP e delle metodologie di application security testing, conoscenze dei linguaggi di programmazione, database relazionali, tecnologie web e sviluppo del software

	Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...)

2.12 INCIDENT HANDLER / RESPONSE SENIOR

Qualifica professionale	Incident handler / response senior
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 8 anni, di cui 5 nella funzione
Profilo professionale	**Policy e strategie** Redige ed aggiorna le policy e le procedure di gestione degli incidenti **Gestione incidenti** Individua le cause degli eventi di sicurezza e fornisce soluzioni per mitigare i potenziali danni in caso di violazione Fornisce competenze e leadership al team di gestione degli incidenti Esegue attività al fine di risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Analizza le tracce lasciate nel corso di attacchi per comprenderne tattiche e strumenti impiegati Identifica e gestisce le problematiche operative durante i processi di risposta agli incidenti, suggerisce e implementa azioni correttive In caso di incidente di sicurezza, agisce quale punto di collegamento tra il personale del SOC, dell'IT e la committenza
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Amministrazione e conduzione operativa di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Amministrazione e conduzione operativa di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse Conoscenza delle metodologie e conduzione operativa di processi di threat intelligence

	Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali Conoscenza delle metodologie di analisi, valutazione e gestione del rischio Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità

2.13 INCIDENT HANDLER / RESPONSE JUNIOR

Qualifica professionale	Incident handler / response junior
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 5 anni, di cui 3 nella funzione
Profilo professionale	**Policy e strategie** Redige ed aggiorna le policy e le procedure di gestione degli incidenti **Gestione incidenti** Individua le cause degli eventi di sicurezza e fornisce soluzioni per mitigare i potenziali danni in caso di violazione Esegue attività al fine di risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Analizza le tracce lasciate nel corso di attacchi per comprenderne tattiche e strumenti impiegati Identifica e gestisce le problematiche operative durante i processi di risposta agli incidenti, suggerisce e implementa azioni correttive In caso di incidente di sicurezza, agisce quale punto di collegamento tra il personale del SOC, dell'IT e la committenza
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica
Conoscenze approfondite in ambito sicurezza	Capacità di conduzione di assessment di sicurezza logica, fisica e organizzativa Conoscenza delle architetture delle principali tipologie di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Amministrazione e conduzione operativa di sistemi di monitoraggio di eventi di sicurezza, SIEM, SOAR, ecc... Conoscenza delle architetture delle principali tipologie di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc...

	Amministrazione e conduzione operativa di apparati e sistemi di sicurezza quali: firewall, next generation firewall, web application firewall, content filtering, content security, IPS, IDS, xDR/EDR e NDR, ecc... Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Capacità di analizzare ed interpretare report di vulnerabilità e di proporre adeguati piani di rientro e contromisure per le vulnerabilità emerse Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali Conoscenza delle metodologie di analisi, valutazione e gestione del rischio Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Conoscenza delle architetture e delle tecniche di ridondanza ed alta affidabilità

2.14 DIGITAL FORENSIC

Qualifica professionale	Digital forensic
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 6 anni, di cui 5 nella funzione
Profilo professionale	Effettua raccolte ed analisi di dati relativi ad attacchi informatici e attività illecite sui sistemi dell'Ente E' responsabile del rilevamento, della raccolta e dell'analisi di tutte le potenziali prove di reato informatico su sistemi, reti e dispositivi Sottopone le prove raccolte al personale dell'Ente, collabora e supporta l'Ente nello svolgimento di indagini da parte delle Forze di polizia e nell'attivazione di azioni penali. Supporta ed assiste l'avvocatura dell'Ente nel comprendere le implicazioni di quanto rilevato in merito alle prove raccolte. Fornisce competenze avanzate per il l'analisi dei dati relativi agli incidenti di sicurezza, criminalità informatica, pirateria informatica, frode, archiviazione e distribuzione di contenuti illegali Fornisce consulenza in merito a normative e standard in caso di violazione di sicurezza Assiste l'Ente durante le indagini penali in caso di richieste tecniche da parte delle forze di Polizia o della Magistratura Redige relazioni tecniche che possano essere utilizzate in tribunale
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica

Conoscenze approfondite in ambito sicurezza	Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali Conoscenza delle metodologie di analisi, valutazione e gestione del rischio Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Competenze sulle metodologie e sui tool di analisi forense

2.15 CYBERSECURITY & PRIVACY LEGAL ADVISOR

Qualifica professionale	CyberSecurity & Privacy Legal Advisor
Titolo di studio	Laurea in discipline tecniche / giuridiche o cultura equivalente
Anzianità lavorativa	Minimo 6 anni, di cui 5 nella funzione
Profilo professionale	**Policy e strategie** Pianifica / esegue / revisiona audit di sicurezza per garantire la conformità alle normative, agli standard ed alle policy dell'Ente **Legal** Eroga consulenza normativa in materia di sicurezza informatica Verifica la conformità delle policy e delle procedure dell'Ente rispetto alla normativa in materia di protezione dei dati personali e di cybersecurity Redige DPIA, Accordi sul trattamento dei dati, privacy policy, informative, valutazione in merito alla base giuridica dei trattamenti Assiste l'Ente durante eventuali indagini penali inerenti reati informatici
Conoscenze e competenze	Capacità di comprendere le esigenze del committente Conoscenza delle architetture tecnologiche infrastrutturali e applicative e loro evoluzioni Esperienza e conoscenza dei principali sistemi operativi, applicazioni, protocolli di rete e delle vulnerabilità ad essi associate Capacità di coordinare e produrre, secondo quanto richiesto dal committente, la redazione della reportistica
Conoscenze approfondite in ambito sicurezza	Conoscenza delle principali vulnerabilità / tipi di attacchi alle reti ed ai sistemi Conoscenza dei principali standard di sicurezza (ITSEC, BS7799, ISO27000, ecc...) Conoscenza approfondita della normativa in materia di sicurezza informatica e protezione dei dati personali Conoscenza delle metodologie di analisi, valutazione e gestione del rischio Capacità di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza Competenze sulle metodologie e sui tool di analisi forense

Lotto	Voce	CIG	DESCRIZIONE LOTTO	CODICE REGIONALE	DESCRIZIONE CODICE REGIONALE	CODICE CPV	UM OGGETTO INIZIATIVA	QUANTITA' (2 dec.)	NOTE AGENZIA	VALORE A BASE D'ASTA IVA ESCLUSA (2 dec.)	IMPORTO PER ATTUAZIONE SICUREZZA (2 dec.)	IMPORTO OPZIONI (2 dec.)
1		0	SERVIZI DI IT SYSTEM MANAGEMENT							65.000.000,00	0,00	0,00
1		1			NOC - Sistemi e Firewall - ORARIO BASE -	72250000-2	CANONE	246	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			
1		2			NOC - Sistemi e Firewall - ORARIO ESTESO -	72250000-2	CANONE	251	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			
1		3			NOC - Sistemi e Firewall - ORARIO CONTINUATO -	72250000-2	CANONE	1.049	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			
1		4			NOC - Apparati di Rete (Switch, router, ecc.) - ORARIO BASE -	72250000-2	CANONE	1.082	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			
1		5			NOC - Apparati di Rete (Switch, router, ecc.) - ORARIO ESTESO -	72250000-2	CANONE	758	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			
1		6			NOC - Apparati di Rete (Switch, router, ecc.) - ORARIO CONTINUATO -	72250000-2	CANONE	1.164	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			
1		7			SMS - Sistemi Mail Server - Sistema non critico - ORARIO BASE -	72250000-2	CANONE	218	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			
1		8			SMS - Sistemi Mail Server - Server Mission Critical - ORARIO ESTESO -	72250000-2	CANONE	218	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			
1		9			SMS - Sistemi Mail Server - Server Mission Critical - ORARIO CONTINUATO -	72250000-2	CANONE	233	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			
1		10			SDS - Sistemi DB Server - Sistema non critico - ORARIO BASE -	72250000-2	CANONE	296	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			
1		11			SDS - Sistemi DB Server - Sistema non critico - ORARIO ESTESO -	72250000-2	CANONE	242	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			
1		12			SDS - Sistemi DB Server - Sistema non critico - ORARIO CONTINUATO -	72250000-2	CANONE	378	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			
1		13			SDS - Sistemi DB Server - Sistema Business Critical - ORARIO BASE -	72250000-2	CANONE	245	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)			

1	14	SDS - Sistemi DB Server - Sistema Business Critical - ORARIO ESTESO -	72250000-2	CANONE	551	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	15	SDS - Sistemi DB Server - Sistema Business Critical - ORARIO CONTINUATO -	72250000-2	CANONE	358	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	16	SDS - Sistemi DB Server - Server Mission Critical - ORARIO BASE -	72250000-2	CANONE	223	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	17	SDS - Sistemi DB Server - Server Mission Critical - ORARIO ESTESO -	72250000-2	CANONE	253	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	18	SDS - Sistemi DB Server - Server Mission Critical - ORARIO CONTINUATO -	72250000-2	CANONE	516	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	19	SAS - Sistemi Application / Web Server / Middleware - Sistema non critico - ORARIO BASE -	72250000-2	CANONE	242	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	20	SAS - Sistemi Application / Web Server / Middleware - Sistema non critico - ORARIO ESTESO -	72250000-2	CANONE	226	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	21	SAS - Sistemi Application / Web Server / Middleware - Sistema non critico - ORARIO CONTINUATO -	72250000-2	CANONE	952	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	22	SAS - Sistemi Application / Web Server / Middleware - Sistema Business Critical - ORARIO BASE -	72250000-2	CANONE	560	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	23	SAS - Sistemi Application / Web Server / Middleware - Sistema Business Critical - ORARIO ESTESO -	72250000-2	CANONE	4.776	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	24	SAS - Sistemi Application / Web Server / Middleware - Sistema Business Critical - ORARIO CONTINUATO -	72250000-2	CANONE	974	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	25	SAS - Sistemi Application / Web Server / Middleware - Server Mission Critical - ORARIO ESTESO -	72250000-2	CANONE	325	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	26	SAS - Sistemi Application / Web Server / Middleware - Server Mission Critical - ORARIO CONTINUATO -	72250000-2	CANONE	1.224	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	27	SIS - Sistemi Infrastrutturali / BackOffice - Sistema non critico - ORARIO BASE -	72250000-2	CANONE	595	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)

1	28	SIS - Sistemi Infrastrutturali / BackOffice - Sistema non critico - ORARIO ESTESO -	72250000-2	CANONE	679	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	29	SIS - Sistemi Infrastrutturali / BackOffice - Sistema non critico - ORARIO CONTINUATO -	72250000-2	CANONE	323	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	30	SIS - Sistemi Infrastrutturali / BackOffice - Sistema Business Critical - ORARIO BASE -	72250000-2	CANONE	223	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	31	SIS - Sistemi Infrastrutturali / BackOffice - Sistema Business Critical - ORARIO ESTESO -	72250000-2	CANONE	286	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	32	SIS - Sistemi Infrastrutturali / BackOffice - Sistema Business Critical - ORARIO CONTINUATO -	72250000-2	CANONE	223	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	33	SIS - Sistemi Infrastrutturali / BackOffice - Server Mission Critical - ORARIO BASE -	72250000-2	CANONE	328	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	34	SIS - Sistemi Infrastrutturali / BackOffice - Server Mission Critical - ORARIO ESTESO -	72250000-2	CANONE	2.873	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	35	SIS - Sistemi Infrastrutturali / BackOffice - Server Mission Critical - ORARIO CONTINUATO -	72250000-2	CANONE	1.097	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	36	SSB - Sistemi Storage/Backup - Sistema non critico - ORARIO BASE -	72250000-2	CANONE	241	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	37	SSB - Sistemi Storage/Backup - Sistema Business Critical - ORARIO CONTINUATO -	72250000-2	CANONE	389	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	38	SSB - Sistemi Storage/Backup - Server Mission Critical - ORARIO BASE -	72250000-2	CANONE	223	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	39	SSB - Sistemi Storage/Backup - Server Mission Critical - ORARIO ESTESO -	72250000-2	CANONE	463	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	40	SSB - Sistemi Storage/Backup - Server Mission Critical - ORARIO CONTINUATO -	72250000-2	CANONE	341	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)
1	41	Apparati di rete (Core, Centro Stella) - ORARIO BASE -	72250000-2	CANONE	262	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)

1	42		Apparati di rete (Core, Centro Stella) - ORARIO ESTESO -	72250000-2	CANONE	260	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)	
1	43		Apparati di rete (Core, Centro Stella) - ORARIO CONTINUATO -	72250000-2	CANONE	898	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)	
1	44		Altri apparati di rete (switch, router, ecc.) - ORARIO BASE -	72250000-2	CANONE	1.825	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)	
1	45		Altri apparati di rete (switch, router, ecc.) - ORARIO ESTESO -	72250000-2	CANONE	1.795	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)	
1	46		Altri apparati di rete (switch, router, ecc.) - ORARIO CONTINUATO -	72250000-2	CANONE	7.271	Le Quantità (triennali) rappresentano il numero indicativo di SERVER/APPLIANCE (virtuale e fisico). Il canone annuo corrisponde al prezzo per SERVER/APPLIANCE (virtuale o fisico)	
1	47		ICT Operation Manager -	72250000-2	GIORNO	1.534		
1	48		Enterprise Architect -	72250000-2	GIORNO	1.429		
1	49		Progettista di architetture di sistemi /System Architect -	72250000-2	GIORNO	5.099		
1	50		System Administrator Senior -	72250000-2	GIORNO	16.273		
1	51		System Administrator Middle -	72250000-2	GIORNO	4.978		
1	52		System Administrator Junior -	72250000-2	GIORNO	5.938		
1	53		Data Base Administrator Senior -	72250000-2	GIORNO	3.322		
1	54		Data Base Administrator Junior -	72250000-2	GIORNO	2.572		
1	55		Network Specialist Senior -	72250000-2	GIORNO	2.179		
1	56		Network Specialist Junior -	72250000-2	GIORNO	2.486		
2	0	SERVIZI DI SICUREZZA INFORMATICA						40.000.000,00
2	1		SOC - Monitoraggio in tempo reale di eventi di sicurezza (su apparati dell'amministrazione o del fornitore) - ORARIO BASE - fino a 1000 EPS	72250000-2	CANONE	60	Le Quantità (triennali) rappresentano il numero indicativo di ENTI. Il canone annuo corrisponde al prezzo per fascia di EPS .	
2	2		SOC - Monitoraggio in tempo reale di eventi di sicurezza (su apparati dell'amministrazione o del fornitore) - ORARIO BASE - 1001-5000 EPS	72250000-2	CANONE	25	Le Quantità (triennali) rappresentano il numero indicativo di ENTI. Il canone annuo corrisponde al prezzo per fascia di EPS .	
2	3		SOC - Monitoraggio in tempo reale di eventi di sicurezza (su apparati dell'amministrazione o del fornitore) - ORARIO BASE - 5001-10000 EPS	72250000-2	CANONE	15	Le Quantità (triennali) rappresentano il numero indicativo di ENTI. Il canone annuo corrisponde al prezzo per fascia di EPS .	
2	4		SOC - Monitoraggio in tempo reale di eventi di sicurezza (su apparati dell'amministrazione o del fornitore) - ORARIO BASE - >10000 EPS	72250000-2	CANONE	3	Le Quantità (triennali) rappresentano il numero indicativo di ENTI. Il canone annuo corrisponde al prezzo per fascia di EPS .	
2	5		SOC - Monitoraggio in tempo reale di eventi di sicurezza (su apparati dell'amministrazione o del fornitore) - ORARIO CONTINUATO -fino a 1000 EPS	72250000-2	CANONE	70	Le Quantità (triennali) rappresentano il numero indicativo di ENTI. Il canone annuo corrisponde al prezzo per fascia di EPS .	
2	6		SOC - Monitoraggio in tempo reale di eventi di sicurezza (su apparati dell'amministrazione o del fornitore) - ORARIO CONTINUATO - 1001-5000 EPS	72250000-2	CANONE	30	Le Quantità (triennali) rappresentano il numero indicativo di ENTI. Il canone annuo corrisponde al prezzo per fascia di EPS .	
2	7		SOC - Monitoraggio in tempo reale di eventi di sicurezza (su apparati dell'amministrazione o del fornitore) - ORARIO CONTINUATO - 5001-10000 EPS	72250000-2	CANONE	15	Le Quantità (triennali) rappresentano il numero indicativo di ENTI. Il canone annuo corrisponde al prezzo per fascia di EPS .	
2	8		SOC - Monitoraggio in tempo reale di eventi di sicurezza (su apparati dell'amministrazione o del fornitore) - ORARIO CONTINUATO - >10000 EPS	72250000-2	CANONE	3	Le Quantità (triennali) rappresentano il numero indicativo di ENTI. Il canone annuo corrisponde al prezzo per fascia di EPS .	

2	9	Sistemi Firewall,IDS/IPS - ORARIO BASE	72250000-2	CANONE	350	Le Quantità (triennali) rappresentano il numero indicativo di PIATTAFORME. Il canone annuo corrisponde al prezzo per PIATTAFORMA.
2	10	Sistemi Firewall,IDS/IPS - ORARIO CONTINUATO	72250000-2	CANONE	250	Le Quantità (triennali) rappresentano il numero indicativo di PIATTAFORME. Il canone annuo corrisponde al prezzo per PIATTAFORMA.
2	11	Sistemi antivirus e di telemetria xDR/EDR/NDR - ORARIO BASE	72250000-2	CANONE	200	Le Quantità (triennali) rappresentano il numero indicativo di PIATTAFORME. Il canone annuo corrisponde al prezzo per PIATTAFORMA.
2	12	Sistemi antivirus e di telemetria xDR/EDR/NDR - ORARIO CONTINUATO	72250000-2	CANONE	150	Le Quantità (triennali) rappresentano il numero indicativo di PIATTAFORME. Il canone annuo corrisponde al prezzo per PIATTAFORMA.
2	13	Sistemi WAF - ORARIO BASE -	72250000-2	CANONE	100	Le Quantità (triennali) rappresentano il numero indicativo di PIATTAFORME. Il canone annuo corrisponde al prezzo per PIATTAFORMA.
2	14	Sistemi WAF - ORARIO CONTINUATO -	72250000-2	CANONE	80	Le Quantità (triennali) rappresentano il numero indicativo di PIATTAFORME. Il canone annuo corrisponde al prezzo per PIATTAFORMA.
2	15	Sistemi SIEM, SOAR - ORARIO BASE -	72250000-2	CANONE	120	Le Quantità (triennali) rappresentano il numero indicativo di PIATTAFORME. Il canone annuo corrisponde al prezzo per PIATTAFORMA.
2	16	Sistemi SIEM, SOAR - ORARIO CONTINUATO -	72250000-2	CANONE	80	Le Quantità (triennali) rappresentano il numero indicativo di PIATTAFORME. Il canone annuo corrisponde al prezzo per PIATTAFORMA.
2	17	Servizio di Incident response & remediation - ORARIO CONTINUATO -	72250000-2	CANONE	300	Le Quantità (triennali) rappresentano il numero indicativo di ENTI. Il canone annuo corrrisponde al prezzo per ENTE (per un max di tre incidenti e cinque segnalazioni all'anno) .
2	18	Servizio di threat intelligence / APT-feed / asset tracker & data leak - ORARIO CONTINUATO -	72250000-2	CANONE	348	Le Quantità (triennali) rappresentano il numero indicativo di DOMINI. Il canone annuo corrisponde al prezzo per DOMINIO.
2	19	Servizio di User and entity behavior analytics (UEBA) - ORARIO BASE -	72250000-2	CANONE	40.000	Le Quantità (triennali) rappresentano il numero indicativo di UTENTI. Il canone annuo corrisponde al prezzo per UTENTE.
2	20	Servizio di User and entity behavior analytics (UEBA) - ORARIO CONTINUATO -	72250000-2	CANONE	60.000	Le Quantità (triennali) rappresentano il numero indicativo di UTENTI. Il canone annuo corrisponde al prezzo per UTENTE.
2	21	Servizio di host hardening - ORARIO BASE -	72250000-2	CANONE	450	Le Quantità (triennali) rappresentano il numero indicativo di DEVICE MODELS. Il canone annuo corrisponde al prezzo per DEVICE MODEL.
2	22	Servizio di security awareness - ORARIO BASE -	72250000-2	CANONE	100.000	Le Quantità (triennali) rappresentano il numero indicativo di UTENTI. Il canone annuo corrisponde al prezzo per UTENTE.

2	23	Servizio di Vulnerability Management (sistema di monitoraggio dell'amministrazione o del fornitore) - ORARIO BASE -	72250000-2	CANONE	45.000	Le Quantità (triennali) rappresentano il numero indicativo di IP. Il canone annuo corrisponde al prezzo per IP.
2	24	Servizio di Application Security Testing (sistema di test dell'amministrazione o del fornitore) - ORARIO BASE -	72250000-2	CANONE	1.200	Le Quantità (triennali) rappresentano il numero indicativo di APPLICAZIONI. Il canone annuo corrisponde al prezzo per APPLICAZIONE.
2	25	Security Project Manager -	72250000-2	GIORNO	792	
2	26	Governance & risk compliance (GRC) consultant -	72250000-2	GIORNO	1.567	
2	27	Security architect & engineer (Specialista infrastrutture e di processo della sicurezza delle informazioni) -	72250000-2	GIORNO	4.123	
2	28	Security Advisor senior -	72250000-2	GIORNO	1.641	
2	29	Security Advisor junior -	72250000-2	GIORNO	2.196	
2	30	Security specialist -	72250000-2	GIORNO	4.992	
2	31	Security specialist con reperibilità H24 -	72250000-2	GIORNO	2.635	
2	32	Security Analyst senior (malware analyst, Intrusion detection, etc) -	72250000-2	GIORNO	2.249	
2	33	Security Analyst junior -	72250000-2	GIORNO	2.099	
2	34	Vulnerability researcher / Ethical Hacker senior -	72250000-2	GIORNO	2.702	
2	35	Vulnerability researcher / Ethical Hacker junior -	72250000-2	GIORNO	3.855	
2	36	Incident handler / response team senior -	72250000-2	GIORNO	1.421	
2	37	Incident handler / response team junior -	72250000-2	GIORNO	380	
2	38	Digital forensic -	72250000-2	GIORNO	830	
2	39	CyberSecurity & Privacy Legal Advisor -	72250000-2	GIORNO	808	

PROCEDURA APERTA PER L'ACQUISIZIONE DI SERVIZI DI IT SYSTEM MANAGEMENT E SICUREZZA INFORMATICA 2

ALLEGATO 6

SCHEMA DI CONVENZIONE

LOTTI 1 e 2

(RETTIFICATO)

CONVENZIONE PER L'ACQUISIZIONE DI SERVIZI DI IT SYSTEM MANAGEMENT (LOTTO 1)

CONVENZIONE PER L'ACQUISIZIONE DI SERVIZI DI SICUREZZA INFORMATICA (LOTTO 2)

TRA

Agenzia Regionale Intercent-ER, (di seguito nominata, per brevità, anche Agenzia), con sede legale in Bologna, Via dei Mille n. 21, C.F. 91252510374, in persona del Direttore e legale rappresentante, Ing. Adriano Leli;

E

___, sede legale in _____, via _____, iscritta al Registro delle Imprese presso il Tribunale di _____ al n. _____, P. IVA_____, domiciliata ai fini del presente atto in _____, via _____, in persona del _____ legale rappresentante _____, giusti poteri allo stesso conferiti da _____ (di seguito nominata, per brevità, anche "***Fornitore***");

OPPURE

___, sede legale in _____, via _____, iscritta al Registro delle Imprese presso il Tribunale di _____ al n. _____, P. IVA _____, domiciliata ai fini del presente atto in _____, via _____, in persona del _____ legale rappresentante _____, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo tra, oltre alla stessa, la mandante _____, sede legale in _____, Via _____, iscritta al Registro delle Imprese presso il Tribunale di _____ al n. _____, P. IVA _____, domiciliata ai fini del presente atto in _____, via _____, e la mandante _____, sede legale in _____, via _____, iscritta al Registro delle Imprese presso il Tribunale di _____ al n. _____, P. IVA _____, domiciliata ai fini del presente atto in _____, via _____, giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in _____,_____, repertorio n. _____ (di seguito nominata, per brevità, anche "***Fornitore***")

PREMESSO

a) che l'Agenzia, nel rispetto dei principi in materia di scelta del contraente, ha ravvisato la necessità di procedere, ed infatti ha proceduto, all'individuazione del Fornitore per la fornitura di servizi di, mediante procedura ad evidenza pubblica di cui al Bando di gara inviato alla G.U.U.E il -_____2023;

b) che l'obbligo del Fornitore di prestare quanto oggetto della presente Convenzione sussiste fino alla concorrenza dell'importo massimo spendibile, nei modi e nelle forme disciplinati dalla presente Convenzione e da tutta la documentazione di gara, ai prezzi unitari, alle condizioni, alle modalità ed ai termini stabiliti;

c) che i singoli contratti vengono conclusi a tutti gli effetti tra le singole Amministrazioni contraenti, da una parte, ed il Fornitore, dall'altra parte, attraverso l'emissione degli Ordinativi di Fornitura (i.e. contratti);

d) che il Fornitore è risultato aggiudicatario della gara di cui sopra a tal fine indetta dall'Agenzia e, per l'effetto, ha manifestato espressamente la volontà di impegnarsi a fornire i servizi oggetto della presente Convenzione ed eseguire gli Ordinativi di Fornitura, alle condizioni, modalità e termini di seguito stabiliti;

e) che il Fornitore dichiara che quanto risulta dalla presente Convenzione, dal Bando di gara e dal Disciplinare di gara e dagli allegati, definisce in modo adeguato e completo l'oggetto delle prestazioni da fornire e, in ogni caso, ha potuto acquisire tutti gli elementi per una idonea valutazione tecnica ed economica delle stesse e per la formulazione dell'offerta;

f) che il Fornitore ha presentato valida documentazione amministrativa, tecnica e l'offerta economica ai fini della stipula della presente Convenzione;

g) che nei confronti del Fornitore sono state esperite le verifiche concernenti le dichiarazioni presentate in sede di gara e lo stesso ha presentato quanto previsto nel Disciplinare di gara e nei suoi allegati per la stipula della Convenzione;

h) che il Fornitore ha stipulato una polizza assicurativa per la responsabilità civile, richiesta ai fini di legge nonché per la stipula della presente Convenzione;

i) che il Fornitore ha presentato l'autodichiarazione circa il possesso dei requisiti di idoneità tecnica e professionale, di cui all'art. 26 comma 1 lettera a) del Decreto Legislativo 81 del 2008 e s.m.i., nonché l'ulteriore documentazione richiesta ai fini della stipulazione della presente Convenzione;

j) che la presente Convenzione non è fonte di obbligazione per la Agenzia nei confronti del Fornitore, rappresentando in ogni caso la medesima Convenzione, le condizioni generali delle prestazioni che verranno concluse dalle singole Amministrazioni contraenti con l'emissione dei relativi Ordinativi di Fornitura i quali, nei limiti ivi previsti, saranno per ciascuna delle stesse fonti di obbligazione.

Ciò premesso, tra le parti come in epigrafe rappresentate e domiciliate

SI CONVIENE E SI STIPULA QUANTO SEGUE

Articolo 1 - Valore delle premesse e degli allegati

Le premesse di cui sopra, gli Atti e i documenti richiamati nelle medesime premesse e nella restante parte del presente Atto, il Capitolato Tecnico, l'elenco dei servizi aggiudicati al Fornitore, l'Offerta Tecnica ed Economica sono fonti delle obbligazioni oggetto della presente Convenzione.

Articolo 2 - Definizioni

1. Nell'ambito della Convenzione si intende per:

   a) Amministrazioni contraenti : le Amministrazioni Contraenti presso le quali il Fornitore si impegna a eseguire i servizi richiesti;

   b) Convenzione: il presente Atto compresi tutti i suoi allegati, nonché i documenti ivi richiamati;

   c) Fornitore: l'Impresa, il Raggruppamento Temporaneo d'Imprese o il Consorzio o la Rete di Imprese risultata/o aggiudicataria/o e che conseguentemente sottoscrive la presente Convenzione, obbligandosi a quanto nello stesso previsto e, comunque, ad eseguire gli Ordinativi di Fornitura;

   d) Ordinativo di Fornitura (i.e. contratto): il documento, disponibile sul Sito delle Convenzioni, con il quale le Amministrazioni Contraenti comunicano la volontà di acquisire le prestazioni oggetto della Convenzione, impegnando il Fornitore all'esecuzione della prestazione richiesta;

   e) Sito: lo spazio *web* sul Portale internet all'indirizzo http://intercenter.regione.emilia-romagna.it, dedicato e gestito dalla Agenzia, contenente un'area riservata a ciascuna Convenzione.

Articolo 3 - Norme regolatrici e disciplina applicabile

1. L'erogazione dei servizi oggetto della presente Convenzione e degli Ordinativi di Fornitura è regolata in via graduata:

a) dalle clausole della presente Convenzione e dagli Allegati ivi richiamati, in particolare dal Capitolato Tecnico, dall'Offerta Tecnica e dall'Offerta Economica dell'Aggiudicatario, che costituiscono la manifestazione integrale di tutti gli accordi intervenuti con il Fornitore relativamente alle attività e prestazioni contrattuali;
b) dai regolamenti di accesso e utilizzo delle Convenzioni riportati sul Sito di cui il Fornitore dichiara di avere esatta conoscenza e che, sebbene non siano materialmente allegati, fanno parte del presente Atto;
c) dalle disposizioni di cui al D. Lgs. n. 50/2016 e comunque dalle norme di settore in materia di appalti pubblici;
d) dal Codice civile e dalle altre disposizioni normative in vigore in materia di contratti di diritto privato.

2. In caso di difficoltà interpretative tra quanto contenuto nel Capitolato Tecnico e suoi allegati e quanto dichiarato nell'Offerta Tecnica, prevarrà quanto contenuto nel Capitolato Tecnico e suoi allegati, fatto comunque salvo il caso in cui l'Offerta Tecnica contenga, a giudizio dell'Agenzia, previsioni migliorative rispetto a quelle contenute nel Capitolato Tecnico e suoi allegati.
3. Le clausole della Convenzione sono sostituite, modificate o abrogate automaticamente per effetto di norme aventi carattere cogente contenute in leggi o regolamenti che entreranno in vigore successivamente, fermo restando che in ogni caso, anche ove intervengano modificazioni autoritative dei prezzi migliorative per il Fornitore, quest'ultimo rinuncia a promuovere azione o ad opporre eccezioni rivolte a sospendere o a risolvere il rapporto contrattuale in essere.
4. L'aggiudicatario è tenuto all'esatta osservanza di tutte le leggi, regolamenti e norme vigenti in materia comprese quelle che potessero essere emanate in corso di Convenzione.

Articolo 4 - Oggetto

1. La Convenzione definisce la disciplina normativa e contrattuale, comprese le modalità di conclusione ed esecuzione dei contratti per l'affidamento della procedura aperta per l'acquisizione di servizi di IT System Management e Sicurezza Informatica 2, che qui si intendono integralmente richiamati, le cui prestazioni sono dettagliatamente descritte nell'Allegato 3 del Capitolato Tecnico.
2. Con la Convenzione, il Fornitore si obbliga irrevocabilmente nei confronti delle Amministrazioni contraenti a fornire i servizi del presente Atto, con le caratteristiche tecniche e di conformità nonché a prestare tutti i servizi secondo le modalità indicate nel Capitolato Tecnico e nell'Offerta Tecnica, nonché a prestare tutti i servizi connessi nella misura richiesta dalle stesse Amministrazioni contraenti mediante gli Ordinativi di Fornitura, il tutto nei limiti del valore della Convenzione, pari a Euro 65.000.000,00 (IVA esclusa) per il Lotto 1 e pari a Euro 40.000.000,00 (IVA esclusa) per il Lotto 2.
3. Con l'emissione dell'Ordinativo di Fornitura le Amministrazioni contraenti danno origine ad un contratto per l'affidamento dei servizi oggetto della presente Convenzione. Gli Ordinativi di Fornitura possono essere prorogati di ulteriori 6 mesi nelle more dell'individuazione del nuovo Fornitore da parte dell'Agenzia Regionale Intercent-ER.
4. La presente Convenzione disciplina le condizioni generali dei singoli contratti conclusi dalle Amministrazioni contraenti, e pertanto non è fonte di alcuna obbligazione per le stesse nei confronti del Fornitore, che sorge solo a seguito dell'emissione degli Ordinativi di Fornitura.
5. Le attività di cui alla Convenzione ed ai singoli Ordinativi di Fornitura non sono affidate al Fornitore in esclusiva e, pertanto, le Amministrazioni, per quanto di propria competenza e nel rispetto della normativa vigente, potranno affidare, in tutto o in parte, le stesse attività anche a soggetti terzi diversi dal Fornitore.

6. L'Agenzia si riserva la facoltà di richiedere al Fornitore, nel periodo di efficacia del presente Atto, l'aumento delle prestazioni contrattuali, nei limiti in vigore per le forniture in favore della Pubblica Amministrazione, alle condizioni, corrispettivi e termini stabiliti nel presente Atto. In particolare, nel caso in cui prima del decorso del termine di durata della presente Convenzione, sia esaurito l'importo massimo spendibile, al Fornitore potrà essere richiesto, alle stesse condizioni e corrispettivi, di incrementare tale importo di un quinto nei termini posti dall'art. 106 comma 12 del D.lgs. 50 del 2016, sussistendo le condizioni di cui al medesimo art. 106, comma 1, lett. a) e/o e, per far fronte agli ulteriori fabbisogni delle Amministrazioni Contraenti.
7. Fermo restando quanto sopra, l'Agenzia potrà altresì, nel corso dell'esecuzione, apportare variazioni secondo quanto previsto dal suddetto articolo.

Articolo 5 - Utilizzo della Convenzione

1. L'utilizzo della Convenzione comporta la registrazione al Sistema del Punto Ordinante.
2. Le Amministrazioni contraenti utilizzano la Convenzione mediante l'emissione di Ordinativi di Fornitura sottoscritti dai Punti Ordinanti ed inviati al Fornitore.
3. È a carico del Fornitore ogni onere e rischio di controllo sulla legittimità dei soggetti che utilizzano la Convenzione; qualora il Fornitore dia esecuzione a Ordinativi di Fornitura emessi da soggetti non legittimati ad utilizzare la Convenzione, le forniture oggetto di tali Ordinativi non verranno conteggiate nell'importo massimo spendibile oggetto della Convenzione stessa.

Articolo 6 - Modalità di conclusione

1. In considerazione degli obblighi assunti dal Fornitore in forza della Convenzione, i singoli contratti con le Amministrazioni contraenti si concludono con la semplice ricezione da parte del Fornitore dei relativi Ordinativi di Fornitura inviati o trasmessi dalle Amministrazioni contraenti stesse.
2. Gli Ordinativi di Fornitura vengono compilati dai Punti Ordinanti tramite il sistema.
3. Qualora non fosse possibile eseguire la prestazione dei servizi oggetto dell'Ordinativo di Fornitura, anche solo in parte il Fornitore è tenuto a comunicare per iscritto tale impossibilità alle Amministrazioni Contraenti entro 2 giorni lavorativi dall'emissione dell'Ordinativo di Fornitura. In tale caso, l'Amministrazione contraente ha la facoltà di recedere in tutto o in parte dall'Ordinativo secondo le modalità previste nella presente Convenzione.

Articolo 7 - Durata

1. Fermo restando l'importo massimo spendibile di cui all'art. 4, comma 2, eventualmente incrementato ai sensi dell'art. 4, comma 8, la presente Convenzione ha una durata pari a 36 (trentasei) mesi a decorrere dalla sua sottoscrizione.
2. Tale durata potrà essere rinnovata, su comunicazione scritta dell'Agenzia, fino ad ulteriori 24 (ventiquattro) mesi, nel caso in cui alla scadenza del termine di durata non sia stato esaurito

l'importo massimo spendibile di cui al precedente articolo 4, comma 3, e fino al raggiungimento del medesimo.

3. Nel caso in cui, prima della scadenza del termine di durata, sia stato esaurito l'importo massimo spendibile di cui al precedente articolo 4, comma 2, eventualmente incrementato ai sensi dell'articolo 4, comma 8, la Convenzione verrà considerata conclusa.
4. Resta inteso che per durata della Convenzione si intende il periodo entro il quale le Amministrazioni contraenti possono aderire alla Convenzione, per emettere Ordinativi di Fornitura. La Convenzione resta comunque valida, efficace e vincolante per la regolamentazione degli Odf e per tutto il tempo di vigenza e durata dei medesimi.
5. Gli Ordinativi di fornitura emessi dalle singole Amministrazioni contraenti avranno durata minima annuale e massima di 36 mesi per i servizi a canone a far data dalla loro emissione; mentre per i servizi relativi alla richiesta di fabbisogni professionali la durata degli Ordinativi di Fornitura potrà essere variabile in relazione alla quantità di giornate richieste per le figure professionali previste.
6. La data di scadenza degli Ordinativi di fornitura, comunque, non potrà essere superiore alla data di scadenza, originaria o eventualmente rinnovata, della Convenzione stessa;
7. È escluso ogni tacito rinnovo del presente Atto.
8. Se, per qualsiasi motivo cessi l'efficacia della Convenzione o di ogni singolo Ordinativo di Fornitura, il Fornitore sarà tenuto a prestare la massima collaborazione, anche tecnica, affinché possa essere garantita la continuità dei servizi, soprattutto nel caso in cui gli stessi vengano successivamente affidati a Ditte diverse dal medesimo Fornitore.

Articolo 8 - Condizioni della fornitura e limitazione di responsabilità

1. Sono a carico del Fornitore, intendendosi remunerati con il corrispettivo contrattuale di cui oltre, tutti gli oneri, le spese ed i rischi relativi alla prestazione delle attività e dei servizi oggetto della Convenzione, nonché ad ogni attività che si rendesse necessaria per la prestazione degli stessi o, comunque, opportuna per un corretto e completo adempimento delle obbligazioni previste, ivi comprese quelle relative ad eventuali spese di trasporto, di viaggio e di missione per il personale addetto all'esecuzione contrattuale.
2. Il Fornitore garantisce l'esecuzione di tutte le prestazioni a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nella presente Convenzione e dagli atti e documenti in essa richiamati, pena la risoluzione di diritto della Convenzione medesima e/o dei singoli Ordinativi di Fornitura, restando espressamente inteso che ciascuna Amministrazione contraente potrà risolvere unicamente l'Ordinativo di Fornitura da essa emesso.
3. Le prestazioni contrattuali debbono necessariamente essere conformi, salva espressa deroga, alle caratteristiche tecniche ed alle specifiche indicate nel Capitolato Tecnico ovvero

nell'Offerta Tecnica, presentata dal Fornitore se migliorativa. In ogni caso, il Fornitore si obbliga ad osservare, nell'esecuzione delle prestazioni contrattuali, tutte le norme e tutte le prescrizioni tecniche e di sicurezza in vigore nonché quelle che dovessero essere emanate successivamente alla stipula della Convenzione.

4. Gli eventuali maggiori oneri derivanti dalla necessità di osservare le norme e le prescrizioni di cui sopra, anche se entrate in vigore successivamente alla stipula della Convenzione, restano ad esclusivo carico del Fornitore, intendendosi in ogni caso remunerati con il corrispettivo contrattuale di cui oltre ed il Fornitore non può, pertanto, avanzare pretesa di compensi, a qualsiasi titolo, nei confronti delle Amministrazioni contraenti o comunque dell'Agenzia, per quanto di propria competenza, assumendosene il medesimo Fornitore ogni relativa alea.
5. Il Fornitore si impegna espressamente a manlevare e tenere indenne l'Agenzia e le Amministrazioni contraenti da tutte le conseguenze derivanti dalla eventuale inosservanza delle norme e prescrizioni tecniche e di sicurezza vigenti.
6. Le attività contrattuali da svolgersi presso i locali delle Amministrazioni Contraenti debbono essere eseguite senza interferire nel normale lavoro degli uffici: le modalità ed i tempi debbono comunque essere concordati con le Amministrazioni stesse. Il Fornitore prende atto che, nel corso dell'esecuzione delle prestazioni contrattuali, i locali delle medesime Amministrazioni contraenti continuano ad essere utilizzati per la loro destinazione istituzionale dal loro personale e/o da terzi autorizzati; il Fornitore si impegna, pertanto, ad eseguire le predette prestazioni salvaguardando le esigenze dei suddetti soggetti, senza recare intralci, disturbi o interruzioni alla attività lavorativa in atto.
7. In adempimento agli obblighi normativi derivanti dal D.Lgs. n.81/2008 e s.m., l'Amministrazione contraente presso cui deve essere eseguito l'Ordinativo di Fornitura, prima dell'inizio dell'esecuzione e sempre che abbia la disponibilità giuridica dei luoghi in cui si svolge l'appalto, si impegna ad integrare il D.U.V.R.I. predisposto dall'Agenzia, riferendolo ai rischi specifici da interferenza esistenti nell'ambiente in cui il Fornitore è destinato ad operare, nonché alle misure di prevenzione e di emergenza adottate in relazione alla propria attività e quantifica gli eventuali oneri correlati. Detto documento, eventualmente integrato e/o modificato in accordo con il Fornitore, deve essere debitamente firmato per accettazione dal Fornitore medesimo, pena la nullità dell'Ordinativo di fornitura.
8. Il Fornitore rinuncia espressamente, ora per allora, a qualsiasi pretesa o richiesta di compenso nel caso in cui l'esecuzione delle prestazioni contrattuali dovesse essere ostacolata o resa più onerosa dalle attività svolte dalle Amministrazioni contraenti e/o da terzi autorizzati.
9. Il Fornitore si impegna ad avvalersi, per la prestazione delle attività contrattuali, di personale specializzato che può accedere nei locali delle Amministrazioni contraenti nel rispetto di tutte le relative prescrizioni e procedure di sicurezza e accesso, fermo restando che è cura ed onere del Fornitore verificare preventivamente tali prescrizioni e procedure.

10. Il Fornitore si obbliga a consentire all'Agenzia nonché alle Amministrazioni contraenti per quanto di rispettiva competenza, di procedere in qualsiasi momento e anche senza preavviso alle verifiche della piena e corretta esecuzione delle prestazioni oggetto degli Ordinativi di Fornitura, nonché a prestare la propria collaborazione per consentire lo svolgimento di tali verifiche.
11. Il Fornitore si obbliga, infine, a dare immediata comunicazione alle Amministrazioni contraenti e/o all'Agenzia, per quanto di rispettiva ragione, di ogni circostanza che abbia influenza sull'esecuzione delle attività di cui alla Convenzione e ai singoli Ordinativi di Fornitura.
12. Resta espressamente inteso che l'Agenzia può essere considerata responsabile solo ed esclusivamente nei confronti del Fornitore, per l'emissione di eventuali propri Ordinativi di Fornitura, e non può in nessun caso essere ritenuta responsabile nei confronti delle Amministrazioni contraenti.
13. Inoltre, ogni Amministrazione Contraente può essere considerata responsabile unicamente e limitatamente per le obbligazioni nascenti dagli Ordinativi di Fornitura da ciascuna emessi.

Articolo 9 - Obbligazioni specifiche del Fornitore

1. Il Fornitore si obbliga, oltre a quanto previsto nelle altre parti della Convenzione, a:
   a) erogare tutti i servizi oggetto della Convenzione, dettagliatamente descritti nel Capitolato Tecnico e nell'Offerta Tecnica, ove migliorativa, impiegando tutte le strutture ed il personale necessario per la loro realizzazione secondo quanto stabilito nella Convenzione e negli Atti di gara;
   b) garantire la continuità dei servizi presi in carico coordinandosi per l'esecuzione delle prestazioni con eventuali Fornitori a cui è subentrato;
   c) adottare nell'esecuzione di tutte le attività, le modalità atte a garantire la vita e l'incolumità dei propri dipendenti, dei terzi e dei dipendenti delle Amministrazioni contraenti nonché ad evitare qualsiasi danno agli impianti, a beni pubblici o privati;
   d) erogare i servizi oggetto della Convenzione ed a prestare i servizi connessi, impiegando tutte le strutture ed il personale necessario per la loro realizzazione secondo quanto stabilito nella Convenzione e negli Atti di gara predisporre tutti gli strumenti e le metodologie, comprensivi della relativa documentazione, atti a garantire elevati livelli di servizio, ivi compresi quelli relativi alla sicurezza e riservatezza, nonché atti a consentire all'Agenzia di monitorare la conformità della prestazione di servizi alle norme previste nella Convenzione e negli Ordinativi di Fornitura, e, in particolare, ai parametri di qualità predisposti;
   e) osservare integralmente tutte le Leggi, Norme e Regolamenti di cui alla vigente normativa in materia di sicurezza e salute dei lavoratori sul luogo di lavoro e a verificare che anche il personale rispetti integralmente le disposizioni di cui sopra;

f) su richiesta scritta dell'Agenzia o dalle singole Amministrazioni contraenti, il Fornitore dovrà presentare il libro unico del lavoro. Nel caso di inottemperanza agli obblighi ivi precisati accertati dalla richiedente, la medesima comunicherà, al Fornitore e se necessario all'Ispettorato del Lavoro, l'inadempienza accertata e procederà ad una detrazione del 20% sul valore del corrispettivo mensile corrisposto ovvero alla sospensione del pagamento dei successivi corrispettivi, destinando le somme accantonate a garanzia degli obblighi di cui sopra. La detrazione del 20% sarà applicata fino al momento in cui l'Ispettorato del Lavoro non abbia accertato che gli obblighi predetti siano integralmente adempiuti. Per tali detrazioni il Fornitore non può opporre eccezioni alla richiedente né ha titolo per un eventuale risarcimento del danno;

2. Il Fornitore si impegna a predisporre e trasmettere all'Agenzia in formato elettronico, tutti i dati e la documentazione di rendicontazione delle forniture secondo quanto previsto al successivo articolo 13.

Articolo 10 - Obblighi derivanti dal rapporto di lavoro

1. Il Fornitore si obbliga ad ottemperare a tutti gli obblighi verso i propri dipendenti derivanti da disposizioni legislative e regolamentari vigenti in materia di lavoro, ivi compresi quelli in tema di igiene e sicurezza, nonché la disciplina previdenziale e infortunistica, assumendo a proprio carico tutti i relativi oneri.
2. Il Fornitore si obbliga ad applicare, nei confronti dei propri dipendenti occupati nelle attività contrattuali, le condizioni normative e retributive non inferiori a quelle risultanti dai Contratti Collettivi ed Integrativi di Lavoro applicabili alla data di stipula della presente Convenzione alla categoria e nelle località di svolgimento delle attività, nonché le condizioni risultanti da successive modifiche ed integrazioni.
3. Il Fornitore si obbliga, altresì, a continuare ad applicare i su-indicati Contratti Collettivi anche dopo la loro scadenza e fino alla loro sostituzione.
4. Gli obblighi relativi ai Contratti Collettivi Nazionali di Lavoro di cui ai commi precedenti vincolano il Fornitore anche nel caso in cui non aderisca alle associazioni stipulanti o receda da esse, per tutto il periodo di validità della presente Convenzione.
5. Il Fornitore si impegna, anche ai sensi e per gli effetti dell'art. 1381 Cod. Civ., a far rispettare gli obblighi di cui ai precedenti commi del presente articolo anche agli eventuali esecutori di parti delle attività oggetto della Convenzione.
6. Si applicano le disposizioni di cui all'art. 30, commi 5 e 6 del D. Lgs. 50/2016, a salvaguardia della adempienza contributiva e retributiva.

Articolo 11 - Modalità e termini di esecuzione del servizio

1. Nel rispetto delle modalità di seguito stabilite e nei luoghi indicati dalle Amministrazioni contraenti, il Fornitore si obbliga a prestare i servizi dettagliatamente descritti nel Capitolato Tecnico e nell'Offerta Tecnica.
2. L'erogazione della prestazione si intende comprensiva di ogni onere e spesa, nessuno escluso.
3. Non sono ammesse prestazioni parziali, pertanto l'esecuzione di ciascuna prestazione deve avvenire secondo quanto disciplinato nel Capitolato Tecnico ovvero nell'Offerta Tecnica se migliorativa, salvo diverso accordo scritto intercorso tra il Fornitore e le singole Amministrazioni Contraenti.
4. Ai sensi della Legge di Bilancio 2018, ai commi 411-415, relativa agli obblighi delle Pubbliche Amministrazioni di emissione dell'ordine elettronico verso il Nodo Smistamento Ordini, considerate inoltre le disposizioni della Legge Regionale n. 11/2004 e s.m.i. e dei conseguenti atti attuativi (Delibera di Giunta Regionale 287/2015), gli Enti e le Aziende del Servizio Sanitario Regionale devono emettere gli ordini esclusivamente in forma elettronica attraverso la rete PEPPOL inviandoli al seguente PARTICIPANT ID _____ .
5. Ai sensi della Legge Regionale n. 11/2004 e s.m.i. e dei conseguenti atti attuativi (Delibera di Giunta Regionale 287/2015) la Regione, gli Enti e gli Organismi Regionali, le loro Associazioni e Consorzi, quali le Agenzie, le Aziende e gli Istituti, anche autonomi ed inoltre gli organismi di diritto pubblico e le società strumentali partecipate in misura totalitaria o maggioritaria dai suddetti soggetti o dalle Aziende del Servizio Sanitario Regionale, sottoposti all'applicazione degli obblighi di cui all'articolo 1 commi da 209 a 214 della legge 24 dicembre 2007 n. 244 (l'elenco di tali Enti è disponibile sul sito di Intercent-ER http://intercenter.regione.emilia-romagna.it, nella sezione dedicata a "ordini, DDT e fatture"), devono emettere gli ordini esclusivamente in forma elettronica attraverso la rete PEPPOL inviandoli al seguente PARTICIPANT ID _____ .
6. Inoltre, a partire dalle decorrenze indicate, il Fornitore dovrà garantire l'invio dei documenti di trasporto elettronici a fronte degli ordini ricevuti e delle consegne effettuate. Il Fornitore dovrà, pertanto, dotarsi degli strumenti informatici idonei alla gestione dei nuovi adempimenti telematici. Per i dettagli tecnici si rinvia alla sezione dedicata al sito dell'Agenzia Intercent-ER http://intercenter.regione.emilia-romagna.it, che contiene tutti i riferimenti del Sistema Regionale per la dematerializzazione del Ciclo Passivo degli Acquisti (formato dei dati, modalità di colloquio, regole tecniche, ecc.), nonché al Nodo Telematico di Interscambio NoTI-ER.
7. In alternativa, le Imprese potranno utilizzare le funzionalità semplificate per la ricezione degli ordini e l'invio dei documenti di trasporto elettronici PEPPOL che sono messe a disposizione

sulla piattaforma di Intercent-ER all'indirizzo https://piattaformaintercenter.regione.emilia-romagna.it/portale/ previa registrazione.

Articolo 12 – Servizi connessi

1. **Reportistica**: Servizio di rendicontazione verso l'Agenzia Intercent-ER. il Fornitore si impegna a mettere a disposizione della Agenzia, in ogni momento, il quadro completo per i diversi servizi in Convenzione.

   L'Agenzia, oltre a quanto sopra, si riserva altresì di chiedere l'elaborazione di report specifici, da inviare a cura del Fornitore, preferibilmente in formato elettronico, entro 15 giorni dalla richiesta, pena l'applicazione di penali.

2. **Numero dedicato:** il Fornitore si impegna, alla stipula della Convenzione, a mettere a disposizione un numero di telefono, un numero di fax e un indirizzo e-mail, attivo per tutto l'anno dalle ore 9.00 alle ore 17.00 per le operazioni di pronto intervento, per bonifiche ambientali da incidenti rilevanti, nonché per tutte le richieste e le esigenze anche urgenti riferite al servizio e per l'inoltro di reclami.

Articolo 13 - Corrispettivi

1. I corrispettivi contrattuali dovuti al Fornitore dalla singola Amministrazione Contraente in forza degli Ordinativi di Fornitura sono calcolati sulla base dei prezzi unitari di cui all'offerta economica.
2. Tutti i predetti corrispettivi si riferiscono a servizi prestati a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali e gli stessi sono dovuti unicamente al Fornitore e, pertanto, qualsiasi terzo, ivi compresi eventuali sub-fornitori o subappaltatori non possono vantare alcun diritto nei confronti delle Amministrazioni contraenti, fatto salvo quanto previsto all'articolo 105 comma 13 del Dlgs. n. 50 del 2016.
3. Tutti gli obblighi ed oneri derivanti al Fornitore dall'esecuzione della Convenzione e dei singoli Ordinativi di Fornitura e dall'osservanza di leggi e regolamenti, nonché dalle disposizioni emanate o che venissero emanate dalle competenti autorità, sono compresi nel corrispettivo contrattuale.
4. I corrispettivi contrattuali sono stati determinati a proprio rischio dal Fornitore in base ai propri calcoli, alle proprie indagini, alle proprie stime, e sono, pertanto, fissi ed invariabili indipendentemente da qualsiasi imprevisto o eventualità, facendosi carico il Fornitore di ogni relativo rischio e/o alea.
5. Il Fornitore non può vantare diritto ad altri compensi, ovvero ad adeguamenti, revisioni o aumenti dei corrispettivi come sopra indicati.
6. L'Agenzia non può in nessun caso essere ritenuta responsabile dei pagamenti delle singole Amministrazioni contraenti.

Articolo 14 - Adeguamento dei prezzi

1. È ammessa la revisione dei prezzi ai sensi dell'art. 106 comma 1 lett. a) del Codice.
2. Trascorso un anno dalla stipula della Convenzione i prezzi possono essere aggiornati, in aumento o in diminuzione, su richiesta del Fornitore sulla base dei prezzi standard rilevati dall'ANAC, degli elenchi dei prezzi rilevati dall'ISTAT, oppure, qualora i dati suindicati non siano disponibili, in misura non superiore alla differenza tra l'indice Istat dei prezzi al consumo per le famiglie di operai e impiegati, al netto dei tabacchi (c.d. FOI) disponibile al momento della richiesta revisione e quello corrispondente al mese/anno di sottoscrizione del contratto.
3. La revisione dei prezzi può essere richiesta una sola volta per ciascuna annualità.
4. La revisione dei prezzi si applica a decorrere dalla data di adozione del relativo atto ai contratti stipulati antecedentemente a tale data per le prestazioni non ancora eseguite ed a quelli stipulati successivamente a tale data. L'atto di revisione dei prezzi sarà comunicato al fornitore e pubblicato sul sito dell'Agenzia.

Articolo 15 - Fatturazione e pagamenti

1. Il Fornitore si obbliga ad effettuare la fatturazione secondo le modalità e nel rispetto dei tempi sotto previsti.
2. Il pagamento dei corrispettivi di cui al precedente articolo è effettuato delle Amministrazioni Contraenti in favore del Fornitore, sulla base delle fatture emesse da queste ultime conformemente alle modalità previste dalla normativa, anche secondaria, vigente in materia, nonché dal presente Atto.
3. Il Fornitore si obbliga a presentare un rendiconto trimestrale di tutte le attività svolte nel corso del periodo di riferimento. Il rendiconto deve essere approvato dal Referente dell'Amministrazione al fine di autorizzare l'emissione della relativa fattura, entro 5 giorni dal ricevimento dello stesso. Qualora il Referente lo ritenesse necessario, può richiedere al Fornitore l'integrazione della documentazione. Il Fornitore sarà tenuto a soddisfare la richiesta del Referente che deve approvare il rendiconto entro 5 giorni dal ricevimento di tale integrazione. L'importo della fattura potrà essere decurtato delle eventuali penali applicate e determinate nelle modalità descritte nell'articolo "Penali".
4. I pagamenti saranno effettuati ai sensi di legge.
5. L'importo delle predette fatture è bonificato sul conto corrente n. ____, dedicato alle commesse pubbliche di cui all'art. 3 della L. 136/2010, intestato al Fornitore, presso _____, e con le seguenti coordinate bancarie IBAN_____.
6. Il Fornitore, sotto la propria esclusiva responsabilità, rende tempestivamente note le variazioni circa le modalità di accredito di cui sopra; in difetto di tale comunicazione, anche se le variazioni vengono pubblicate nei modi di legge, il Fornitore non può sollevare eccezioni in ordine ad eventuali ritardi dei pagamenti, né in ordine ai pagamenti già effettuati.

7. Resta tuttavia espressamente inteso che in nessun caso, ivi compreso il caso di ritardi nei pagamenti dei corrispettivi dovuti, il Fornitore può sospendere il servizio e, comunque, lo svolgimento delle attività previste nella Convenzione e nei singoli Ordinativi di Fornitura. Qualora il Fornitore si renda inadempiente a tale obbligo, l'Ordinativo di Fornitura e/o la Convenzione si possono risolvere di diritto mediante semplice ed unilaterale dichiarazione da comunicarsi nelle modalità previste dalla vigente normativa, rispettivamente dalle Amministrazioni contraenti e/o dall'Agenzia.

Articolo 16 - Tracciabilità dei flussi finanziari e clausola risolutiva espressa

1. Il Fornitore si assume l'obbligo della tracciabilità dei flussi finanziari di cui alla L. 13 agosto 2010, n. 136 e s.m., pena la nullità assoluta della presente Convenzione e degli Ordinativi di Fornitura.
2. Il conto corrente di cui al comma 5 dell'art. 16 è dedicato, anche in via non esclusiva alle commesse pubbliche di cui all'art. 3 della L. 136/2010 e s.m.
3. Il Fornitore si obbliga a comunicare all'Agenzia e alle Amministrazioni contraenti le generalità ed il codice fiscale delle persone delegate ad operare sul predetto conto corrente, nonché ogni successiva modifica ai dati trasmessi, nei termini di cui all'art. 3, comma 7, L. 136/2010 e s.m..
4. Qualora le transazioni relative agli Ordinativi di fornitura inerenti la presente Convenzione siano eseguite senza avvalersi del bonifico bancario o postale ovvero di altri strumenti idonei a consentire la piena tracciabilità, la presente Convenzione e gli Ordinativi stessi sono risolti di diritto, secondo quanto previsto dall'art. 3, comma 9 bis, della L. 136/2010 e s.m.
5. Il Fornitore si obbliga altresì ad inserire nei contratti sottoscritti con i subappaltatori o i subcontraenti, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla Legge 13 agosto 2010 n. 136 e s.m.
6. Il Fornitore, il subappaltatore o subcontraente, che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria, ne dà immediata comunicazione alle Amministrazioni contraenti e alla Prefettura-Ufficio territoriale del Governo della provincia ove ha sede la Società; copia di tale comunicazione deve essere inviata per conoscenza anche all'Agenzia.
7. L'Agenzia verificherà che nei contratti di subappalto sia inserita, a pena di nullità assoluta del contratto, un'apposita clausola con la quale il subappaltatore assume gli obblighi di tracciabilità dei flussi finanziari di cui alla Legge 136/2010 e s.m.
8. Con riferimento ai subcontratti, il Fornitore si obbliga a trasmettere alla Agenzia e alle Amministrazioni contraenti, oltre alle informazioni di cui all'art. 105, comma 2, del D. Lgs. 50/2016, anche apposita dichiarazione resa ai sensi del D.P.R. n. 445/2000, attestante che nel relativo subcontratto è stata inserita, a pena di nullità assoluta, un'apposita clausola con la

quale il subcontraente assume gli obblighi di tracciabilità di cui alla Legge sopracitata. È facoltà della Agenzia e dell'Amministrazione contraente richiedere copia del contratto tra il Fornitore ed il subcontraente al fine di verificare la veridicità di quanto dichiarato.

9. Per tutto quanto non espressamente previsto, restano ferme le disposizioni di cui all'art. 3 della L. 13/08/2010 n. 136 e s.m.

Articolo 17 - Trasparenza

1. Il Fornitore espressamente ed irrevocabilmente:
   a) dichiara che non vi è stata mediazione o altra opera di terzi per la conclusione della presente Convenzione;
   b) dichiara di non aver corrisposto né promesso di corrispondere ad alcuno, direttamente o attraverso terzi, ivi comprese le imprese collegate o controllate, somme di denaro o altra utilità a titolo di intermediazione o simili, comunque volte a facilitare la conclusione della Convenzione stessa;
   c) si obbliga a non versare ad alcuno, a nessun titolo, somme di danaro o altra utilità finalizzate a facilitare e/o a rendere meno onerosa l'esecuzione e/o la gestione della presente Convenzione rispetto agli obblighi con essa assunti, né a compiere azioni comunque volte agli stessi fini.
2. Qualora non risulti conforme al vero anche una sola delle dichiarazioni rese ai sensi del precedente comma, ovvero il Fornitore non rispetti gli impegni e gli obblighi ivi assunti per tutta la durata della presente Convenzione, la stessa si intende risolta di diritto ai sensi e per gli effetti dell'articolo 1456 Cod. Civ., per fatto e colpa del Fornitore, che è conseguentemente tenuto al risarcimento di tutti i danni derivanti dalla risoluzione.

Articolo 18 - Penali

1. Intercent-ER e le Amministrazioni contraenti hanno la facoltà di effettuare tutti gli accertamenti e controlli che ritengano opportuni, con qualsiasi modalità ed in ogni momento, durante l'efficacia degli Ordinativi di Fornitura, per assicurare che da parte del Fornitore siano scrupolosamente osservate tutte le pattuizioni contrattuali. Altresì, si riservano di controllare la validità delle prestazioni eseguite, portando tempestivamente a conoscenza del Fornitore gli inadempimenti relativi all'applicazione delle penali.
2. Ove si verifichino inadempienze da parte del Fornitore nell'esecuzione delle obbligazioni previste nella Convenzione e nel Capitolato Tecnico, non imputabili all'Amministrazione Contraente ovvero a forza maggiore o caso fortuito, regolarmente contestate, Intercent-ER, la Regione per il tramite del Settore competente e le Amministrazioni contraenti, si riservano di applicare le penali di cui al presente articolo.

3. In caso di mancato rispetto dei parametri di qualità dei servizi previsti nel Capitolato, il Fornitore sarà tenuto a corrispondere all'Amministrazione Contraente e/o all'Agenzia, per quanto di propria competenza, le penali di seguito riepilogate, su richiesta delle Amministrazioni Contraenti o dell'Agenzia, a seconda delle rispettive competenze di seguito indicate.
4. L'applicazione della penale non solleva il Fornitore dalle responsabilità civili e penali, che lo stesso si è assunto con la stipulazione del contratto, e che dovessero derivare dall'incuria dello stesso Fornitore.
5. Gli eventuali inadempimenti contrattuali che danno luogo all'applicazione delle penali, vengono contestati per iscritto al Fornitore dalla Amministrazione Contraente, che inoltra la medesima contestazione anche all'Agenzia, per opportuna conoscenza, e/o dall'Agenzia stessa, per quanto di propria competenza; il Fornitore deve comunicare per iscritto in ogni caso le proprie deduzioni nel termine massimo di giorni 2 (due) dalla stessa contestazione. Qualora dette deduzioni non siano accoglibili, a insindacabile giudizio della Amministrazione e/o dell'Agenzia, ovvero non vi sia stata risposta o la stessa non sia giunta nel termine indicato, sono applicate al Fornitore le penali a decorrere dall'inizio dell'inadempimento.
6. La richiesta e/o il pagamento delle penali di cui al presente articolo non esonera in nessun caso il Fornitore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.
7. Il Fornitore prende atto che l'applicazione delle penali previste dal presente articolo non preclude il diritto delle singole Amministrazioni contraenti e/o dell'Agenzia a richiedere il risarcimento degli eventuali maggiori danni.
8. Ciascuna Amministrazione Contraente potrà applicare al Fornitore penali sino a concorrenza della misura massima pari al 10% (dieci per cento) del valore del proprio Ordinativo di Fornitura; il Fornitore prende atto, in ogni caso, che l'applicazione delle penali non preclude il diritto delle singole Amministrazioni Contraenti a richiedere il risarcimento degli eventuali maggiori danni.
9. L'Agenzia, in caso di reiterati inadempimenti del Fornitore, segnalati alla stessa dalle Amministrazioni Contraenti, salvo il diritto di risoluzione della Convenzione in relazione alla gravità ravvisata negli stessi, può applicare penali rivalendosi sulla cauzione.
10. L'Agenzia, per quanto di sua competenza, potrà applicare al Fornitore penali sino a concorrenza della misura massima pari al 10% (dieci per cento) dell'importo massimo complessivo della Convenzione, viste anche le penali applicate dalle Amministrazioni Contraenti. Resta fermo il risarcimento degli eventuali maggiori danni.
11. L'inadempimento e/o ritardo nell'adempimento, che determini un importo massimo della penale superiore all'importo sopra previsto, comporta la risoluzione di diritto dell'Ordinativo di Fornitura e/o della Convenzione per grave inadempimento. In tal caso l'Agenzia e/o l'Amministrazione

Contraente hanno facoltà di ritenere definitivamente la cauzione, e/o di applicare una penale equivalente, nonché di procedere nei confronti del Fornitore per il risarcimento del danno.

12. Tutti i tempi indicati nella presente sezione, qualora non altrimenti espressamente specificato, sono da intendersi come solari. Ogni frazione del parametro di misura (minuti, ore, giorni) sarà arrotondata nel calcolo della penale all'intero superiore.
13. L'Agenzia ovvero le Amministrazioni potranno applicare le penali di cui alle successive tabelle. Si precisa che, ove il parametro non è indicato si intende quello previsto nel Capitolato Tecnico ovvero quello indicato dalla Ditta Concorrente nell'offerta tecnica ove migliorativo.
14. L'Amministrazione si riserva di effettuare verifiche finalizzate a monitorare/controllare gli SLA previsti nel paragrafo 9.1 del Capitolato Tecnico e in generale le modalità di fornitura dei servizi. Qualora venissero confermate inadempienze rispetto al valore degli SLA minimi, l'Amministrazione, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nel Capitolato, potrà richiedere l'applicazione delle penali nelle modalità indicate nella presente Convenzione.
15. Il Fornitore sarà tenuto a corrisponderle all'Amministrazione in caso di mancato rispetto degli SLA definiti nel citato paragrafo del Capitolato.
16. È da intendersi quale ritardo nella prestazione di un determinato servizio o attività, anche il caso in cui il Fornitore presti tale servizio/attività in modo difforme dalle prescrizioni contenute nel Capitolato Tecnico. In tale circostanza, il ritardo sarà calcolato sino alla data di adeguamento del servizio/attività alle predette prescrizioni.
17. Per le penali di cui alla Tabella 2, Tabella 3, Tabella 4, Tabella 5, Tabella 6, Tabella 7 e Tabella 8 valgono le seguenti definizioni:

    - **Periodo di osservazione**: un mese;
    - **PLS**: Penale sul Livello di Servizio, relativa al periodo di osservazione;
    - **LSM**: Livello di Servizio Misurato;
    - **VUP**: Valore Unitario di Penale;
    - **FP**: Fattore di Penalità, pari a:
        - **1** nel caso in cui nel periodo di osservazione sia stato violato lo SLA_{min}
        - **2**m in caso di violazione ripetuta di SLA_{min}, dove m è il numero di periodi di osservazione consecutivi in cui si verifica la violazione di SLA_{min}, con m maggiore o uguale a 2; in caso i periodi siano superiori a 3, il valore di m rimarrà comunque pari a 3;
    - **DLS**: Differenza di Livello di Servizio, cioè la distanza percentuale tra Livello di Servizio Misurato fuori target e SLA_{min}, calcolata come segue:

$$DLS = \frac{abs(SLA_{min} - LSM)}{SLA_{min}} * 100$$

- Valorizzazione della Penale di **Tipo A**:

  In questa modalità viene misurata l'ampiezza percentuale di ciascun disservizio rispetto allo SLA_{min}. La formula di calcolo della penale viene quindi applicata per ogni prestazione in cui si registra un disservizio:

$$DLSi = \frac{abs(SLA_{min} - LSMi)}{SLA_{min}} * 100$$

  La penale sul Livello di Servizio relativa al periodo di osservazione è pari a:

$$PLS = \sum_{1}^{n} FP * VUP * DLS_i$$

  dove la sommatoria è estesa a tutte le n prestazioni fuori SLA_{min} nel singolo periodo di osservazione;

- Valorizzazione della Penale di **Tipo B**:

  In questa modalità, LSM è relativo alla qualità complessiva del servizio nel periodo di osservazione. In caso LSM sia fuori SLA_{min}, la penale applicata sul Livello di Servizio relativa al periodo di osservazione è pari a:

PLS =FP x VUP x DLS

Tabella 1 – Penali per Assessment, Piano di Esecuzione e Avvio dei Servizi (Lotti 1 e 2)

Tipologia Servizio	Descrizione KPI	Valorizzazione della Penale
Assessment e Piano Esecuzione dei Servizi	Tempo dall'invio della Richiesta di Assessment da parte dell'Amministrazione, alla conclusione delle attività di sopralluogo	0,5 per mille del valore dell'Ordinativo di Fornitura Principale, per ogni giorno di Ritardo
	Tempo dall'invio della Richiesta di Assessment da parte dell'Amministrazione, all' invio all'Amministrazione del Piano di Esecuzione dei Servizi	1 per mille del valore dell'Ordinativo di Fornitura Principale, per ogni giorno di Ritardo
	Tempo dall'invio delle richieste di modifica al Piano da parte dell'Amministrazione, all' invio all'Amministrazione del nuovo Piano di Esecuzione dei Servizi	1 per mille del valore dell'Ordinativo di Fornitura Principale, per ogni giorno di Ritardo
Avvio dei Servizi	Tempo dall'emissione dell'Ordinativo di Fornitura Principale, all'avvio dei servizi	1 per mille del valore del/dei servizio/i avviato/i in ritardo, per ogni giorno di Ritardo
Aggiornamento del Piano di Esecuzione dei Servizi	Tempo dall'invio della Richiesta di aggiornamento del Piano di Esecuzione dei Servizi da parte dell'Amministrazione, alla conclusione delle attività di sopralluogo	0,5 per mille del valore dell'Ordinativo Collegato, per ogni giorno di Ritardo
	Tempo dall'invio della Richiesta di aggiornamento del Piano di Esecuzione dei Servizi da parte	1 per mille del valore dell'Ordinativo Collegato, per ogni giorno di Ritardo

	dell'Amministrazione, all' invio all'Amministrazione del Piano di Esecuzione dei Servizi aggiornato	
	Tempo dall'invio delle richieste di modifica al Piano da parte dell'Amministrazione, all' invio all'Amministrazione del nuovo Piano di Esecuzione dei Servizi aggiornato	1 per mille del valore dell'Ordinativo Collegato, per ogni giorno di Ritardo
Avvio dei nuovi Servizi	Tempo dall'emissione dell'Ordinativo di integrazione, all'avvio dei servizi	1 per mille del valore del/dei servizio/i avviato/i in ritardo, per ogni giorno di Ritardo

Tabella 2 – Penali per Gestione Server, Rete, Sicurezza (Lotto 1)

Tipologia Richiesta Servizio	Descrizione KPI	Valorizzazione della Penale	
		Tipo	VUP
Presa in carico	Tempo di presa in carico malfunzionamento	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di gestione dell'ambito tecnologico cui il KPI si riferisce
Risoluzione Malfunzionamento nella conduzione dei sistemi	Tempo di risoluzione malfunzionamento	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di gestione dell'ambito tecnologico cui il KPI si riferisce
Intervento pianificato nell'ambito della conduzione dei sistemi	Tempo di completamento intervento	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di gestione dell'ambito tecnologico cui il KPI si riferisce

Tabella 3 – Penali per NOC (Lotto 1)

Tipologia Richiesta Servizio	Descrizione KPI	Valorizzazione della Penale	
		Tipo	VUP
Presa in carico da parte del NOC	Tempo di presa in carico malfunzionamento /segnalazione da sistema di monitoraggio	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di manutenzione dell'ambito tecnologico cui il KPI si riferisce
Risoluzione malfunzionamento da parte del NOC	Tempo di risoluzione malfunzionamento /segnalazione da sistema di monitoraggio	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di manutenzione dell'ambito tecnologico cui il KPI si riferisce

Tabella 4 – Penali Service Desk Sistemistico (Lotto 1)

Tipologia Richiesta Servizio	Descrizione KPI	Valorizzazione della Penale	
		Tipo	VUP
Richieste al Service Desk sistemistico	Tempo di gestione richieste al service desk	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di service desk sistemistico
	Tasso di risoluzione ticket al service desk (esclusi interventi che richiedono manutenzione HW)	B	2 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di service desk sistemistico

Tabella 5 – Penali Gestione Apparati e Sistemi di Sicurezza (Lotto 2)

Tipologia Richiesta Servizio	Descrizione KPI	Valorizzazione della Penale	
		Tipo	VUP
Presa in carico	Tempo di presa in carico malfunzionamento	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di gestione dell'ambito tecnologico cui il KPI si riferisce
Risoluzione Malfunzionamento nella conduzione dei sistemi	Tempo di risoluzione malfunzionamento	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di gestione dell'ambito tecnologico cui il KPI si riferisce
Intervento pianificato nell'ambito della conduzione dei sistemi	Tempo di completamento intervento	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di gestione dell'ambito tecnologico cui il KPI si riferisce

Tabella 6 – Penali per Monitoraggio in tempo reale eventi di sicurezza SOC (Lotto 2)

Tipologia Richiesta Servizio	Descrizione KPI	Valorizzazione della Penale	
		Tipo	VUP
Presa in carico di un alert e prima analisi	Tempo di prima analisi evento di sicurezza/incidente da sistema di monitoraggio indicazione prime contromisure da applicare (identificazione, verifica, notifica)	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di intervento dell'ambito tecnologico cui il KPI si riferisce
Azioni da intraprendere	Indicazione procedure operative di contenimento, gestione dell'incidente, ingaggio del Incident Response Team. Indicazione contromisure da applicare e risoluzione reattiva di incidente di sicurezza	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di intervento dell'ambito tecnologico cui il KPI si riferisce

Tabella 7 – Penali per Incident Response (Lotto 2)

Tipologia Richiesta Servizio	Descrizione KPI	Valorizzazione della Penale	
		Tipo	VUP
Presa in carico di un alert	Tempo di rilevazione e presa in carico di un alert di incidente di sicurezza (da sistema di monitoraggio e/o da segnalazione SOC)	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di intervento dell'ambito tecnologico cui il KPI si riferisce
Convalida e risoluzione	Validazione e gestione dell'incidente, Indicazione contromisure da applicare e risoluzione reattiva e proattiva di incidente di sicurezza	A	1 per mille del corrispettivo dovuto dall'Amministrazione, nel periodo di osservazione, per il servizio di intervento dell'ambito tecnologico cui il KPI si riferisce

Tabella 8 – Penali per messa a disposizione delle risorse professionali (Lotti 1 e 2)

Tipologia Servizio	Descrizione KPI	Valorizzazione della Penale
Messa a disposizione	Variazione risorse nel tempo	0,5 per cento del corrispettivo annuale dovuto dall'Amministrazione per il profilo specifico della risorsa

delle risorse		
	Tempo sostituzione / aggiunta	0,5 per cento del corrispettivo annuale dovuto dall'Amministrazione per il profilo specifico della risorsa

Tabella 9 – Penali Reportistica (Lotto 1)

Tipologia Servizio	Descrizione KPI	Valorizzazione della Penale
Report degli Asset e dei Servizi per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	0,1 per mille del valore del Contratto di Fornitura, per ogni giorno di ritardo
Report dei Livelli di Servizio conseguiti per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	0,1 per mille del valore del Contratto di Fornitura, per ogni giorno di ritardo

Tabella 10 – Penali Reportistica (Lotto 2)

Tipologia Servizio	Descrizione KPI	Valorizzazione della Penale
Report Servizi di sicurezza per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	0,1 per mille del valore del Contratto di Fornitura, per ogni giorno di ritardo
Report dei Livelli di Servizio conseguiti per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	0,1 per mille del valore del Contratto di Fornitura, per ogni giorno di ritardo

Articolo 19 - Cauzione definitiva

1. Con la stipula della Convenzione ed a garanzia degli obblighi assunti con il perfezionamento di ogni singolo rapporto di fornitura, il Fornitore costituisce una cauzione definitiva in favore della Agenzia rilasciata in data _____ dalla _____ avente n. _____ di importo pari ad Euro _____= (_____/00) del valore della fornitura eventualmente incrementata ai sensi del D.Lgs. 50 n. 2016 art. 103 (al netto degli oneri fiscali).
2. Alla garanzia di cui al presente articolo si applicano le riduzioni previste dall'art. 93, comma 7, per la garanzia provvisoria.
3. La cauzione deve essere vincolata per tutta la durata della Convenzione e comunque di tutti i contratti di fornitura da esso derivanti. In caso di risoluzione del contratto, la cauzione definitiva viene ripartita in modo proporzionale sulla base degli Ordinativi di Fornitura in corso emessi dalle Amministrazioni contraenti.
4. La cauzione definitiva si intende estesa a tutti gli accessori del debito principale ed è prestata a garanzia dell'esatto e corretto adempimento di tutte le obbligazioni del Fornitore, anche future ai sensi e per gli effetti dell'art. 1938 Cod. Civ., nascenti dall'esecuzione dei singoli Ordinativi di *F*ornitura ricevuti.

5. In particolare, la cauzione rilasciata garantisce tutti gli obblighi specifici assunti dal Fornitore, anche quelli a fronte dei quali è prevista l'applicazione di penali e, pertanto, resta espressamente inteso che le Amministrazioni contraenti/l'Agenzia, fermo restando quanto previsto nel precedente articolo "Penali", ha diritto di rivalersi direttamente sulla cauzione.
6. La garanzia opera per tutta la durata degli Ordinativi di Fornitura, e, comunque, sino alla completa ed esatta esecuzione delle obbligazioni nascenti dallo stesso; pertanto, la garanzia sarà svincolata, previa deduzione di eventuali crediti delle Amministrazioni contraenti/Agenzia verso il Fornitore, a seguito della piena ed esatta esecuzione delle obbligazioni contrattuali.
7. La cauzione può essere progressivamente e proporzionalmente svincolata, sulla base dell'avanzamento dell'esecuzione, nel limite massimo del 80%. A tal fine le Amministrazioni contraenti trasmettono all'Agenzia documenti attestanti l'avvenuta regolare esecuzione delle prestazioni, di norma semestralmente, e comunque inviano, a seguito della completa ed esatta esecuzione dell'Ordinativo di Fornitura emesso, apposita comunicazione da cui risulti la completa e regolare esecuzione delle prestazioni contrattuali.
8. In ogni caso lo svincolo definitivo della cauzione residua avviene solo previo consenso espresso in forma scritta dall'Agenzia.
9. Qualora l'ammontare della cauzione definitiva si riduca per effetto dell'applicazione di penali, o per qualsiasi altra causa, il Fornitore deve provvedere al reintegro entro il termine di 30 (trenta) giorni dal ricevimento della relativa richiesta effettuata da parte dell'Agenzia.
10. In caso di inadempimento delle obbligazioni previste nel presente articolo le Amministrazioni contraenti e/o l'Agenzia hanno facoltà di dichiarare risolto rispettivamente l'Ordinativo di Fornitura e/o la Convenzione.

Articolo 20 - 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, di non divulgarli in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione della Convenzione.
2. L'obbligo di cui al precedente comma sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione della Convenzione.
3. L'obbligo di cui al comma 1 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 anzidetti.
5. In caso di inosservanza degli obblighi di riservatezza, l'Agenzia, nonché le Amministrazioni contraenti hanno facoltà di dichiarare risolto di diritto la Convenzione ed i singoli Ordinativi di

Fornitura, fermo restando che il Fornitore è tenuto a risarcire tutti i danni che ne dovessero derivare.

6. Il Fornitore può citare i termini essenziali della Convenzione nei casi in cui sia condizione necessaria per la partecipazione del Fornitore stesso a gare e appalti, previa comunicazione all'Agenzia delle modalità e dei contenuti di detta citazione.
7. Il Fornitore si impegna, altresì, a rispettare quanto previsto dal D. Lgs.196/2003 e s.m.i. e dai relativi regolamenti di attuazione in materia di riservatezza.

Articolo 21 - Risoluzione

1. A prescindere dalle cause generali di risoluzione dei contratti di fornitura e della presente Convenzione, le Amministrazioni contraenti potrà risolvere ai sensi dell'art. 1456 Cod. Civ., previa dichiarazione da comunicarsi al Fornitore con raccomandata a/r, nel caso di mancato adempimento delle prestazioni contrattuali a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nella Convenzione e negli atti e documenti in essa richiamati.
2. In caso di inadempimento del Fornitore anche a uno solo degli obblighi assunti con la stipula della Convenzione che si protragga oltre il termine, non inferiore comunque a 20 (venti) giorni lavorativi, che verrà assegnato a mezzo comunicazione effettuata con le modalità previste dalla vigente normativa, dalle Amministrazioni contraenti e/o dalla Agenzia, per quanto di propria competenza, per porre fine all'inadempimento, le stesse Amministrazioni contraenti e/o la Agenzia hanno la facoltà di considerare, per quanto di rispettiva competenza, risolti di diritto il relativo Ordinativo di Fornitura e/o la Convenzione e di ritenere definitivamente la cauzione, e/o di applicare una penale equivalente, nonché di procedere nei confronti del Fornitore per il risarcimento del danno.
3. In ogni caso, ferme le ulteriori ipotesi di risoluzione previste dall'art. 108 del D. Lgs. n. 50/2016, le Amministrazioni contraenti potrà risolvere di diritto ai sensi dell'art. 1456 Cod. Civ., previa dichiarazione da comunicarsi al Fornitore nel rispetto delle modalità previste dalla vigente normativa, senza necessità di assegnare alcun termine per l'adempimento, i singoli Ordinativi di Fornitura nei seguenti casi:
   a) Nel caso in cui almeno 3 (o numero diverso se del caso) Amministrazioni contraenti abbiano risolto il proprio Ordinativo di Fornitura ai sensi dei precedenti commi 1 e 2;
   b) mancata reintegrazione della cauzione eventualmente escussa entro il termine di cui all'articolo "Cauzione definitiva";
   c) mancata copertura dei rischi durante tutta la vigenza di ogni singolo Ordinativo di Fornitura, ai sensi dell'articolo "Danni, responsabilità civile e polizza assicurativa";

d) azioni giudiziarie per violazioni di diritto di brevetto, di autore ed in genere di privativa altrui, intentate contro le Amministrazioni contraenti, ai sensi dell'articolo "Brevetti industriali e diritti d'autore";
e) mancata rispondenza tra i servizi erogati e quelli offerti in gara;
f) nei casi di cui all'articolo "Tracciabilità dei flussi finanziari e clausola risolutiva espressa";
g) nei casi di cui all'articolo "Riservatezza";
h) nei casi di cui all'articolo "Subappalto";
i) nei casi di cui all'articolo "Trasparenza";
j) qualora disposizioni legislative, regolamentari ed autorizzative non ne consentano la prosecuzione in tutto o in parte.

4. La risoluzione della Convenzione legittima la risoluzione dei singoli Ordinativi di Fornitura a partire dalla data in cui si verifica la risoluzione della Convenzione stessa. In tal caso, il Fornitore si impegna comunque a porre in essere ogni attività necessaria per assicurare la continuità del servizio in favore delle Amministrazioni contraenti.
5. In tutti i casi di risoluzione della Convenzione e/o del/degli Ordinativo/i di Fornitura, l'Agenzia e/o le Amministrazioni contraenti hanno diritto di escutere la cauzione prestata rispettivamente per l'intero importo della stessa o per la parte percentualmente proporzionale all'importo del/degli Ordinativo/i di Fornitura risolto/i.
6. Ove non sia possibile escutere la cauzione, sarà applicata una penale di equivalente importo, che sarà comunicata al Fornitore con lettera raccomandata A/R. In ogni caso, resta fermo il diritto del medesimo le Amministrazioni contraenti e/o della Agenzia al risarcimento dell'ulteriore danno.
7. Si precisa che, le cause di risoluzione di cui sopra possono riguardare la Convenzione e/o l'Ordinativo di Fornitura. In tal caso l'Agenzia e/o le Amministrazioni contraenti, per le parti di loro rispettiva competenza, possono risolvere la Convenzione e/o l'Ordinativo di Fornitura.
8. Nel caso di risoluzione degli Ordinativi di Fornitura, il Fornitore ha diritto soltanto al pagamento delle prestazioni relative ai servizi regolarmente eseguiti, decurtato degli oneri aggiuntivi derivanti dallo scioglimento dell'Ordinativo di Fornitura.

Articolo 22 - Recesso

1. Fermo restando quanto previsto dagli articoli 88, comma 4-ter, e 92, comma 4, del decreto legislativo 6 settembre 2011, n. 159, le Amministrazioni contraenti e/o l'Agenzia, per quanto il proprio interesse, hanno diritto, nei casi di giusta causa, di recedere unilateralmente dai singoli Ordinativi di Fornitura e/o dalla Convenzione, in tutto o in parte, in qualsiasi momento, con un preavviso di almeno 30 (trenta) giorni solari, da comunicarsi al Fornitore con lettera raccomandata a/r.

2. Si conviene che per giusta causa si intende, a titolo meramente esemplificativo e non esaustivo:
   i) qualora sia stato depositato contro il Fornitore un ricorso ai sensi della legge fallimentare o di altra legge applicabile in materia di procedure concorsuali, che proponga lo scioglimento, la liquidazione, la composizione amichevole, la ristrutturazione dell'indebitamento o il concordato con i creditori, ovvero nel caso in cui venga designato un liquidatore, curatore, custode o soggetto avente simili funzioni, il quale venga incaricato della gestione degli affari del Fornitore;
   ii) qualora il Fornitore perda i requisiti minimi richiesti per l'affidamento di forniture ed appalti di servizi pubblici e, comunque, quelli previsti dal Bando di gara e dal Disciplinare di gara relativi alla procedura attraverso la quale è stato scelto il Fornitore medesimo;
   iii) qualora taluno dei componenti l'Organo di Amministrazione o l'Amministratore Delegato o il Direttore Generale o il Responsabile tecnico del Fornitore siano condannati, con sentenza passata in giudicato, per delitti contro la Pubblica Amministrazione, l'ordine pubblico, la fede pubblica o il patrimonio, ovvero siano assoggettati alle misure previste dalla normativa antimafia.
   iv) Si conviene altresì che le singole Amministrazioni Contraenti, in coincidenza con la scadenza del proprio bilancio triennale, potranno recedere in tutto o in parte dal proprio Ordinativo di Fornitura nell'ipotesi in cui, in ottemperanza alla normativa vigente in materia di impegni pluriennali di spesa, le risorse stanziate nel proprio bilancio annuale o pluriennale non risultino sufficienti per la copertura degli impegni di spesa derivanti dall'ulteriore durata del medesimo Ordinativo di Fornitura. Tale ipotesi integra e sostanzia a tutti gli effetti una ulteriore giusta causa di recesso.
   v) L'Amministrazione Contraente, in caso di mutamenti di carattere organizzativo interessanti la stessa Amministrazione, che abbiano incidenza sull'esecuzione della prestazione dei servizi, può altresì recedere unilateralmente, in tutto o in parte, dall'Ordinativo di Fornitura, con un preavviso di almeno 30 (trenta) giorni solari, da comunicarsi al Fornitore con lettera raccomandata a/r.
   vi) Nei casi di cui ai commi precedenti il Fornitore ha diritto al pagamento delle prestazioni eseguite, purché correttamente ed a regola d'arte, secondo il corrispettivo e le condizioni contrattuali rinunciando espressamente, ora per allora, a qualsiasi ulteriore eventuale pretesa, anche di natura risarcitoria, ed a ogni ulteriore compenso o indennizzo e/o rimborso delle spese, anche in deroga a quanto previsto dall'articolo 1671 Cod. Civ.
   vii) L'Amministrazione Contraente può altresì recedere, per motivi diversi da quelli elencati, da ciascun singolo Ordinativo di Fornitura, in tutto o in parte, avvalendosi della facoltà consentita dall'articolo 1671 c.c. con un preavviso di almeno 30 (trenta) giorni solari, da

comunicarsi al Fornitore con lettera raccomandata a/r, purché tenga indenne lo stesso Fornitore delle spese sostenute, delle prestazioni rese e del mancato guadagno.

viii) In ogni caso, dalla data di efficacia del recesso, il Fornitore deve cessare tutte le prestazioni contrattuali, assicurando che tale cessazione non comporti danno alcuno per le Amministrazioni Contraenti.

Articolo 23 – Eventi di forza maggiore

1. Si intende per forza maggiore il verificarsi di un evento o circostanza che impedisca al Fornitore di adempiere ad una più obbligazioni contrattuali, se, e nella misura in cui, provi:
   [a] che tale impedimento è fuori dal suo ragionevole controllo; e
   [b] che l'evento non avrebbe potuto ragionevolmente essere previsto al momento della conclusione della Convenzione; e
   [c] che gli effetti dell'impedimento non avrebbero potuto ragionevolmente essere evitati o superati dal Fornitore stesso.
2. In assenza di prova contraria, si presume che gli eventi seguenti soddisfino le condizioni (a) e (b) del comma 1 del presente articolo, mentre resta a carico del Fornitore provare la sussistenza della condizione (c):

(i) guerra (dichiarata o meno), ostilità, invasione, atti di un nemico straniero, estesa mobilitazione militare;

(ii) guerra civile, sommossa, ribellione, rivoluzione, forza militare o usurpazione di potere, insurrezione, atti di terrorismo, sabotaggio o pirateria;

(iii) restrizioni valutarie o agli scambi commerciali, embargo, sanzioni;

(iv) atti dell'autorità, legittimi o illegittimi, osservanza di leggi o ordini governativi, norme, espropriazione, confisca di beni, requisizione, nazionalizzazione;

(v) peste, epidemia, catastrofi naturali o eventi naturali estremi;

3. Il Fornitore è tenuto a comunicare senza ritardo all'Agenzia il verificarsi dell'evento che inibisce l'adempimento degli obblighi contrattuali. L'Agenzia valuta il sussistere delle condizioni di cui al comma 1 del presente articolo.
4. Il Fornitore che si trovi in tali condizioni è esonerato dall'obbligo di adempiere alle proprie obbligazioni contrattuali e da responsabilità per danni o inadempimento, a partire dal momento in cui comunica l'evento all'Agenzia.
5. Ove l'effetto dell'impedimento o dell'evento invocato sia temporaneo, le conseguenze sopraddette si produrranno solo nella misura in cui e fino a quando l'impedimento o l'evento invocati inibiscano al Fornitore l'adempimento degli obblighi contrattuali.
6. Il Fornitore deve informare l'Agenzia non appena tali eventi cessino e lo stesso può riprendere l'adempimento delle proprie obbligazioni.

7. Qualora la durata dell'impedimento invocato sia, o diventi, insostenibile, sulla base delle esigenze della Agenzia e delle amministrazioni contraenti, le stesse avranno il diritto di risolvere la Convenzione e/o gli Ordinativi di Fornitura.
8. Le parti convengono che, in assenza di diverso accordo, la Convenzione e gli Ordinativi di Fornitura potranno comunque essere risolti ove la durata dell'impedimento superi i 120 giorni.

Articolo 24 - Danni, responsabilità civile e polizza assicurativa

1. Il Fornitore assume in proprio ogni responsabilità per infortunio o danni eventualmente subiti da parte di persone o di beni, tanto del Fornitore stesso quanto di terzi, in virtù dei servizi oggetto della presente Convenzione, ovvero in dipendenza di omissioni, negligenze o altre inadempienze relative all'esecuzione delle prestazioni contrattuali ad esso riferibili, anche se eseguite da parte di terzi.
2. Il Fornitore, inoltre, dichiara di essere in possesso di un'adeguata polizza assicurativa a beneficio anche delle Amministrazioni contraenti, per l'intera durata della Convenzione, a copertura del rischio da responsabilità civile del medesimo Fornitore in ordine allo svolgimento di tutte le attività di cui alla stessa Convenzione. In particolare, detta polizza tiene indenne le Amministrazioni contraenti, ivi compresi i loro dipendenti e collaboratori, nonché i terzi per qualsiasi danno il Fornitore possa arrecare alla stessa, ai loro dipendenti e collaboratori, nonché ai terzi nell'esecuzione di tutte le attività di cui alla Convenzione. Resta inteso che l'esistenza e, quindi, la validità ed efficacia della polizza assicurativa di cui al presente articolo è condizione essenziale per le Amministrazioni contraenti, e, pertanto, qualora il Fornitore non sia in grado di provare in qualsiasi momento la copertura assicurativa di cui si tratta la Convenzione si risolve di diritto con conseguente ritenzione della cauzione prestata a titolo di penale e fatto salvo l'obbligo di risarcimento del maggior danno subito.

Articolo 25 - Subappalto

1. Il Fornitore, conformemente a quanto dichiarato in sede di offerta, affida in subappalto, l'esecuzione delle seguenti prestazioni:

   _____

   _____

2. Il Fornitore è responsabile dei danni che dovessero derivare alle Amministrazioni contraenti, all' Agenzia o a terzi per fatti comunque imputabili ai soggetti cui sono state affidate le suddette attività.
3. I subappaltatori dovranno mantenere per tutta la durata della Convenzione e dei singoli Ordinativi di Fornitura, i requisiti richiesti dalla normativa vigente in materia per lo svolgimento delle attività agli stessi affidate.
4. Il subappalto è autorizzato dalla Agenzia. Il Fornitore si impegna a depositare presso la Agenzia medesima, almeno venti giorni prima dell'inizio dell'esecuzione delle attività oggetto

del subappalto, la copia del contratto di subappalto e la documentazione prevista dalla normativa vigente in materia, ivi inclusa la dichiarazione attestante il possesso da parte del subappaltatore dei requisiti, richiesti dalla vigente normativa, per lo svolgimento delle attività allo stesso affidate. Copia del contratto di subappalto deve essere inviata anche alle Amministrazioni contraenti. In caso di mancata presentazione dei documenti sopra richiesti nel termine previsto, la Agenzia non autorizzerà il subappalto.

5. Il subappalto non comporta alcuna modificazione agli obblighi e agli oneri del Fornitore. Il fornitore e il subappaltatore sono responsabili in solido nei confronti della Agenzia e/o delle Amministrazioni contraenti, in relazione alle prestazioni oggetto del contratto di subappalto.
6. Il Fornitore si obbliga a manlevare e tenere indenne la Agenzia e/o le Amministrazioni contraenti da qualsivoglia pretesa di terzi per fatti e colpe imputabili al subappaltatore o ai suoi ausiliari.
7. Ai sensi dell'art. 105, comma 14, del D. Lgs. n. 50/2016, il subappaltatore per le prestazioni affidate in subappalto, deve garantire gli stessi standard qualitativi e prestazionali previsti nel contratto di appalto e riconoscere ai lavoratori un trattamento economico e normativo non inferiore a quello che avrebbe garantito il contraente principale, inclusa l'applicazione dei medesimi contratti collettivi nazionali di lavoro qualora le attività oggetto di subappalto coincidano con quelle caratterizzanti l'oggetto dell'appalto ovvero riguardino le lavorazioni relative alle categorie prevalenti e siano incluse nell'oggetto sociale del contraente principale.
8. L'esecuzione delle prestazioni affidate in subappalto non può formare oggetto di ulteriore subappalto.
9. Fuori dai casi di cui all'art. 105 comma 13, il Fornitore si obbliga a trasmettere alla all'Amministrazione contraente entro 20 (venti) giorni dalla data di ciascun pagamento effettuato nei suoi confronti, copia delle fatture quietanzate relative ai pagamenti da esso corrisposti al subappaltatore con l'indicazione delle ritenute di garanzia effettuate.
10. Qualora il Fornitore non trasmetta le fatture quietanzate del subappaltatore nel termine di cui al comma precedente, le Amministrazioni contraenti sospende il successivo pagamento a favore del Fornitore.
11. In caso di cessione in subappalto di attività senza la preventiva approvazione ed in ogni caso di inadempimento da parte del Fornitore agli obblighi di cui ai precedenti commi, la Agenzia potrà risolvere la Convenzione e le Amministrazioni contraenti l'Ordinativo di Fornitura, fatto salvo il diritto al risarcimento del danno.
12. Per tutto quanto non previsto si applicano le disposizioni di cui all'art. 105 del D. Lgs. n. 50/2016 ss.mm.

    ovvero nel caso sia vietato il subappalto (qualora il Fornitore non l'abbia richiesto in offerta)

Non essendo stato richiesto in sede di gara, è fatto divieto al Fornitore di subappaltare le prestazioni oggetto della presente Convenzione.

Articolo 26 - Divieto di cessione del contratto e dei crediti

1. È fatto assoluto divieto al Fornitore di cedere, a qualsiasi titolo, la Convenzione e i singoli Ordinativi di Fornitura, a pena di nullità delle cessioni stesse, salvo quanto previsto dall'art. 106, comma 1, lett. d, punto 2, del D. Lgs. 50/2016 e ss.mm.
2. È fatto assoluto divieto al Fornitore di cedere a terzi i crediti della fornitura senza specifica autorizzazione da parte dell'Amministrazione contraente debitrice, salvo quanto previsto dall'art. 106, comma 13 del D. Lgs. 50/2016 e ss.mm.
3. Anche la cessione di credito soggiace alle norme sulla tracciabilità dei flussi finanziari di cui alla L. 136/2010 e s.m.
4. In caso di inadempimento da parte del Fornitore degli obblighi di cui ai precedenti commi, le Amministrazioni contraenti hanno facoltà di dichiarare risolti di diritto i singoli Ordinativi di Fornitura, per quanto di rispettiva ragione.

Articolo 27 - Brevetti industriali e diritti d'autore

1. Il Fornitore assume ogni responsabilità conseguente all'uso di dispositivi o all'adozione di soluzioni tecniche o di altra natura che violino diritti di brevetto, di autore ed in genere di privativa altrui.
2. Qualora venga promossa nei confronti delle Amministrazioni contraenti una azione giudiziaria da parte di terzi che vantino diritti su beni acquistati, il Fornitore si obbliga a manlevare e tenere indenne le Amministrazioni contraenti, assumendo a proprio carico tutti gli oneri conseguenti, inclusi i danni verso terzi, le spese giudiziali e legali a carico del medesime.
3. Le Amministrazioni contraenti si impegnano ad informare prontamente il Fornitore delle iniziative giudiziarie di cui al precedente comma; in caso di difesa congiunta, il Fornitore riconosce allo stesso la facoltà di nominare un proprio legale di fiducia da affiancare al difensore scelto dal Fornitore.
4. Nell'ipotesi di azione giudiziaria per le violazioni di cui al comma precedente tentata nei confronti delle Amministrazioni contraenti, lo stesso, fermo restando il diritto al risarcimento del danno nel caso in cui la pretesa azionata sia fondata, ha facoltà di dichiarare la risoluzione di diritto degli Ordinativi di Fornitura, per quanto di rispettiva ragione, recuperando e/o ripetendo il corrispettivo versato, detratto un equo compenso per i servizi erogati.

Articolo 28 - Responsabile del Servizio e Referente del Fornitore

1. Con la stipula del presente atto il Fornitore individua nel Sig._____ il Responsabile del Servizio, con capacità di rappresentare ad ogni effetto il Fornitore, il quale è Referente nei confronti dell'Agenzia e delle Amministrazioni contraenti.
2. I dati di contatto del Responsabile del servizio sono: numero telefonico _____, numero di fax _____, indirizzo e-mail _____.
3. Il Fornitore deve inoltre comunicare alle Amministrazioni contraenti il nominativo del Responsabile dell'esecuzione del contratto che svolgerà il ruolo di interfaccia con l'Amministrazione contraente per tutte le attività ed eventuali problematiche inerenti il servizio.

Articolo 29 - Foro competente

Per tutte le questioni relative ai rapporti tra il Fornitore e la Agenzia, è competente in via esclusiva il Foro di Bologna.

Per tutte le controversie relative ai rapporti tra il Fornitore e le Amministrazioni contraenti, la competenza è determinata in base alla normativa vigente.

Articolo 30 - Trattamento dei dati, consenso al trattamento

1. Con la sottoscrizione della presente Convenzione, le parti, in relazione ai trattamenti di dati personali effettuati in esecuzione della Convenzione medesima, dichiarano di essersi reciprocamente comunicate tutte le informazioni previste dal Regolamento UE 2016/679 (GDPR), ivi comprese quelle relative alle modalità di esercizio dei diritti dell'interessato.

   In particolare, il Fornitore dichiara di aver ricevuto, prima della sottoscrizione della presente Convenzione, le informazioni di cui all'art. 13 del Regolamento UE/2016/679 circa la raccolta ed il trattamento dei dati personali conferiti per la sottoscrizione e l'esecuzione della Convenzione stessa e degli Ordinativi di Fornitura, nonché di essere pienamente a conoscenza dei diritti riconosciuti ai sensi della predetta normativa.

   L'informativa è contenuta al paragrafo 28 del Disciplinare di Gara che deve intendersi integralmente trascritto in questa sede.
2. L'Agenzia, oltre ai trattamenti effettuati in ottemperanza ad obblighi di legge, esegue i trattamenti dei dati necessari alla esecuzione della Convenzione e dei singoli Ordinativi di Fornitura, in particolare per finalità legate al monitoraggio dei consumi ed al controllo della spesa delle Amministrazioni contraenti, nonché per l'analisi degli ulteriori risparmi di spesa ottenibili.
3. Con la sottoscrizione della Convenzione il rappresentante legale del Fornitore acconsente espressamente al trattamento dei dati personali e si impegna ad adempiere agli obblighi di rilascio dell'informativa e di richiesta del consenso, ove necessario, nei confronti delle persone fisiche interessate di cui sono forniti dati personali nell'ambito dell'esecuzione della Convenzione e dei contratti attuativi, per le finalità descritte nel Disciplinare di gara in precedenza richiamate.

4. In ogni caso le Amministrazioni contraenti, aderendo alla Convenzione con l'emissione dell'Ordinativo di Fornitura, dichiarano espressamente di acconsentire al trattamento ed alla trasmissione all'Agenzia, da parte del Fornitore, anche per via telefonica e/o telematica, dei dati relativi alla fatturazione, rendicontazione e monitoraggio, per le finalità connesse all'esecuzione della Convenzione e dei singoli Ordinativi di Fornitura ed ai fini del monitoraggio dei consumi e del controllo della spesa totale, nonché dell'analisi degli ulteriori risparmi di spesa ottenibili.
5. I trattamenti dei dati sono improntati, in particolare, ai principi di correttezza, liceità e trasparenza ed avvengono nel rispetto delle misure di sicurezza previste dall' art 32 Regolamento UE 2016/679. Ai fini della suddetta normativa, le parti dichiarano che i dati personali forniti con il presente atto sono esatti e corrispondono al vero, esonerandosi reciprocamente da qualsivoglia responsabilità per errori materiali di compilazione ovvero per errori derivanti da una inesatta imputazione dei dati stessi negli archivi elettronici e cartacei, fermi restando i diritti dell'interessato di cui agli artt. 7 e da 15 a 22 del Regolamento UE 2016/679.
6. Qualora, in relazione all'esecuzione della presente Convenzione, vengano affidati al Fornitore trattamenti di dati personali di cui l'Agenzia risulta titolare, il Fornitore stesso è da ritenersi designato quale Responsabile del trattamento ai sensi e per gli effetti dell'art. 28, Regolamento UE 2016/679 (GDPR). In coerenza con quanto previsto dalla normativa richiamata, il Fornitore si impegna ad improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza nel pieno rispetto di quanto disposto dall'art. 5 del Regolamento UE 2016/679 e dalle ulteriori norme regolamentari in materia, limitandosi ad eseguire i soli trattamenti funzionali, necessari e pertinenti all'esecuzione delle prestazioni contrattuali e, in qualsiasi caso, non incompatibili con le finalità per cui i dati sono stati raccolti.
7. Il Fornitore qualora venga nominato "Responsabile del trattamento" si impegna inoltre a:
   a) adempiere all'incarico attribuito adottando idonee e preventive misure di sicurezza, con particolare riferimento a quanto stabilito dall'art. 32 Regolamento UE 2016/679;
   b) tenere un registro del trattamento conforme a quanto previsto dall'art. 30 del Regolamento UE/2016/679 ed a renderlo tempestivamente consultabile dal Titolare del trattamento. Il Fornitore dovrà consentire alle Amministrazione contraenti di eseguire, anche tramite terzi incaricati, le verifiche sulla corretta applicazione delle norme in materia di trattamento dei dati personali;
   c) predisporre, qualora l'incarico comprenda la raccolta di dati personali, l'informativa di cui all'art 13 del Regolamento UE 2016/679 e verificare che siano adottate le modalità operative necessarie affinché la stessa sia effettivamente portata a conoscenza degli interessati;

d) dare direttamente riscontro orale, anche tramite propri incaricati, alle richieste verbali dell'interessato;

e) trasmettere all'Agenzia, con la massima tempestività, le istanze dell'interessato per l'esercizio dei diritti di cui agli artt. 7 e da 15 a 23 del Regolamento UE 2016/679 che necessitino di riscontro scritto, in modo da consentire all'Agenzia stessa di dare riscontro all'interessato nei termini; nel fornire altresì all'Agenzia tutta l'assistenza necessaria, nell'ambito dell'incarico affidato, per soddisfare le predette richieste;

f) individuare gli incaricati del trattamento dei dati personali, impartendo agli stessi le istruzioni necessarie per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;

g) consentire all'Agenzia, in quanto Titolare del trattamento, l'effettuazione di verifiche periodiche circa il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, fornendo alla stessa piena collaborazione.

8. Ove applicabile, in ragione dell'oggetto della Convenzione, ove il Fornitore sia chiamato ad eseguire attività di trattamento dei dati personali, il medesimo potrà essere nominato Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento UE; in tal caso, il Fornitore si impegna ad accettare la designazione a Responsabile del trattamento da parte dell'Azienda Sanitaria/Amministrazione Contraente relativamente ai dati personali di cui la stessa è titolare e che potranno essere trattati dal Fornitore nell'ambito di erogazione dei servizi contrattualmente previsti. In tal caso, il Fornitore si obbliga ad adottare le misure di natura fisica, logica, tecnica e organizzativa idonee a garantire un livello di sicurezza adeguato al rischio, ivi comprese quelle specificate nell' Ordinativo di Fornitura, unitamente ai suoi allegati.
9. Il Fornitore si impegna ad adottare le misure di sicurezza di natura fisica, tecnica e organizzativa necessarie a garantire un livello di sicurezza adeguato al rischio, nonché ad osservare le vigenti disposizioni in materia di sicurezza e privacy ed a farle osservare ai propri dipendenti e collaboratori, opportunamente autorizzati al trattamento dei dati personali.

Articolo 31 - Oneri fiscali e spese contrattuali

1. La presente Convenzione viene stipulata nella forma della scrittura privata con firma digitale.
2. Sono a carico del Fornitore tutti gli oneri anche tributari e le spese contrattuali relative alla Convenzione e agli Ordinativi di Fornitura ivi incluse, a titolo esemplificativo e non esaustivo, quelle notarili, bolli, carte bollate, tasse di registrazione, ecc. ad eccezione di quelle che fanno carico alle Amministrazioni contraenti per legge.

Articolo 32 – Verifiche sull'esecuzione della Convenzione

1. Anche ai sensi degli artt. 101 e 103 del D.Lgs. n. 50/2016 e ss.mm., il Fornitore si obbliga a consentire alle Amministrazioni Contraenti e all'Agenzia, per quanto di propria competenza, di procedere, in qualsiasi momento e anche senza preavviso, alle verifiche della piena e corretta esecuzione delle prestazioni oggetto degli Ordinativi di fornitura, nonché a prestare la propria collaborazione per consentire lo svolgimento di tali verifiche.
2. Le Amministrazioni/Aziende Sanitarie Contraenti nominano da uno a tre componenti incaricati di norma in contraddittorio con il Referente del Fornitore, in qualsiasi momento e senza preavviso, di effettuare controlli sulle modalità operative e sulle attrezzature utilizzate per lo svolgimento del servizio, in tutte le sue fasi.
3. Al termine delle verifiche è redatto un verbale, firmato dai presenti e consegnato in copia alla Ditta, che si impegna a risolvere le eventuali non conformità riscontrate e, su richiesta dei Referenti delle Amministrazioni contraenti a comunicare quali azioni correttive intende porre in atto per evitare il ripetersi delle non conformità dallo stesso giudicate gravi.
4. Nel caso siano contestate al Fornitore non conformità nell'esecuzione del servizio, le stesse devono essere risolte in via bonaria tra le parti, mantenendo comunque le Amministrazioni Contraenti la facoltà di richiedere la ripetizione delle attività non correttamente svolte e la sostituzione dei prodotti non conformi senza ulteriori addebiti economici. In attesa della risoluzione della non conformità, la fattura riferita al prodotto o servizio contestato non deve essere emessa e, se già emessa non sarà liquidata. Qualora le contestazioni non vengano risolte in via bonaria, le Amministrazioni Contraenti procedono ad applicare le penalità previste al precedente Articolo.
5. Il Fornitore, in ogni caso, si obbliga a rispettare tutte le indicazioni relative alla buona e corretta esecuzione contrattuale che dovessero essere impartite dalle Amministrazioni Contraenti.

Articolo 33 - Clausola finale

1. Il presente atto costituisce manifestazione integrale della volontà negoziale delle parti che hanno altresì preso piena conoscenza di tutte le relative clausole, avendone negoziato il contenuto, che dichiarano quindi di approvare specificamente singolarmente nonché nel loro insieme e, comunque, qualunque modifica al presente Atto non può aver luogo e non può essere provata che mediante Atto scritto; inoltre, l'eventuale invalidità o l'inefficacia di una delle clausole della Convenzione e/o dei singoli Ordinativi di Fornitura non comporta l'invalidità o inefficacia dei medesimi atti nel loro complesso.
2. Qualsiasi omissione o ritardo nella richiesta di adempimento della Convenzione e/o dei singoli Ordinativi di Fornitura da parte delle Amministrazioni contraenti non costituisce in nessun caso rinuncia ai diritti spettanti che le medesime parti si riservano di far valere nei limiti della prescrizione.

3. Con il presente Atto si intendono regolati tutti i termini generali del rapporto tra le parti; in conseguenza esso non viene sostituito o superato dagli eventuali accordi operativi attuativi o integrativi, quali ad esempio gli Ordinativi di Fornitura, e sopravvive ai detti accordi continuando, con essi, a regolare la materia tra le parti; in caso di contrasti le previsioni del presente Atto prevalgono su quelle degli Atti di sua esecuzione, salvo diversa espressa volontà derogatoria delle parti manifestata per iscritto.

L'AGENZIA*	IL FORNITORE*
_____	_____

*Sottoscritto con firma digitale ai sensi del D. Lgs. 82/05 e s.m.i.

ALLEGATO 1 ALLA CONVENZIONE PER L'ACQUISIZIONE DI SERVIZI DI IT SYSTEM MANAGEMENT (LOTTO 1)

ALLEGATO 1 ALLA CONVENZIONE PER L'ACQUISIZIONE DI SERVIZI DI SICUREZZA INFORMATICA (LOTTO 2)

TRA

Agenzia Regionale Intercent-ER, C.F. 91252510374 con sede legale a Bologna, Via dei Mille n.21, in persona del Direttore e legale rappresentante, Dott. Adriano Leli (di seguito nominata, per brevità, anche Agenzia)

E

Società _____ sede legale in _____ via_____, iscritta al Registro delle Imprese presso il Tribunale di _____ al n. _____ , P. IVA/C.F. _____ domiciliata ai fini del presente atto in _____, via _____, in persona del Direttore/Procuratore/Legale Rappresentante, nato/a a _____ il _____ , e residente a in Via _____ , giusti poteri allo stesso conferiti da (di seguito nominato, per brevità, "Fornitore");

CLAUSOLE VESSATORIE

Il sottoscritto _____, quale procuratore/legale rappresentante del Fornitore, dichiara di avere particolareggiata e perfetta conoscenza di tutte le clausole contrattuali e dei documenti ed atti ivi richiamati; ai sensi e per gli effetti di cui agli artt. 1341 e 1342 Cod. Civ., dichiara altresì di accettare tutte le condizioni e patti ivi contenuti e di avere particolarmente considerato quanto stabilito e convenuto con le relative clausole; in particolare dichiara di approvare specificamente le clausole e condizioni di seguito elencate: Articolo 3 (Norme regolatrici e disciplina applicabile), Articolo 4 (Oggetto), Articolo 7 (Durata), Articolo 8 (Condizioni della fornitura e limitazione di responsabilità), Articolo 9 (Obbligazioni specifiche del Fornitore), Articolo 11 (Modalità e termini di esecuzione della fornitura), Articolo 12 (Livelli di Servizio), Articolo 13 (Corrispettivi), Articolo 14 (Adeguamento dei prezzi), Articolo 15 (Fatturazione e pagamenti), Articolo 16 (Tracciabilità dei flussi finanziari), Articolo 18 (Penali), Articolo 19 (Cauzione definitiva), Articolo 20 (Riservatezza), Articolo 21 (Risoluzione), Articolo 22 (Recesso), Articolo 24 (Danni, responsabilità civile e polizza assicurativa), Articolo 25 (Subappalto), Articolo 26 (Divieto di cessione del contratto e dei crediti), Articolo 27 (Brevetti industriali e diritti d'autore), Articolo 28 (Responsabile del servizio), Articolo 29 (Foro competente), Articolo 30 (Trattamento dei dati, consenso al trattamento), Articolo 31 (Oneri fiscali e spese contrattuali), Articolo 33 (Clausola finale).

IL FORNITORE*

_____

*Sottoscritto con firma digitale ai sensi del D. Lgs. 82/05 e s.m.i.