PROCEDURA APERTA FINALIZZATA ALL'ACQUISIZIONE DI SERVIZI, FORNITURE E ATTIVITA' ACCESSORIE NELL'AMBITO DEL PROGETTO DI IMPLEMENTAZIONE E PROSECUZIONE DEL SISTEMA REGIONALE DI RILEVAZIONE AUTOMATIZZATA DEL TRAFFICO STRADALE (SISTEMA MTS)

ALLEGATO "A"

ALL'ALLEGATO 6 (SCHEMA DI CONTRATTO)

CIG 7548358E10

Accordo per il trattamento di dati personali

Il presente accordo costituisce allegato parte integrante del contratto siglato tra la Giunta della Regione Emilia-Romagna e il Fornitore di servizi, designato Responsabile del trattamento di dati personali ai sensi dell'art. 28 del GDPR (General Data Protection – Regolamento GDPR UE 2016/679).

1. Premesse

(A) Il presente Accordo si compone delle clausole di seguito rappresentate e dai seguenti Allegati, che ne formano parte integrante e sostanziale:

- Allegato 1: Glossario
- Allegato 2: Appendice "Security"

Le Parti convengono quanto segue:

2. Trattamento dei dati nel rispetto delle istruzioni della Giunta della Regione Emilia-Romagna

2.1 Il Fornitore, relativamente a tutti i Dati personali che tratta per conto dell'Ente garantisce che:

2.1.1 tratta tali Dati personali solo ai fini dell'esecuzione dell'oggetto del contratto, e, successivamente, solo nel rispetto di quanto eventualmente concordato dalle Parti per iscritto, agendo pertanto, esclusivamente sulla base delle istruzioni documentate e fornite dall'Ente;

2.1.2 non trasferisce i Dati personali a soggetti terzi, se non nel rispetto delle condizioni di liceità assolte dall'Ente e a fronte di quanto disciplinato nel presente accordo;

2.1.3 non tratta o utilizza i Dati personali per finalità diverse da quelle per cui è conferito incarico dall'Ente, financo per trattamenti aventi finalità compatibili con quelle originarie;

2.1.4 prima di iniziare ogni trattamento e, ove occorra, in qualsiasi altro momento, informerà l'Ente se, a suo parere una qualsiasi istruzione fornita dall'Ente si pone in violazione di Normativa applicabile;

2.2 Al fine di dare seguito alle eventuali richieste da parte di soggetti interessati, il Fornitore si obbliga ad adottare:

2.2.1 procedure idonee a garantire il rispetto dei diritti e delle richieste formulate all'Ente dagli interessati relativamente ai loro dati personali;

2.2.2 procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta dell'Ente dei dati personali di ogni interessato;

2.2.3 procedure atte a garantire la cancellazione o il blocco dell'accesso ai dati personali a richiesta dall'Ente;

2.2.4 procedure atte a garantire il diritto degli interessati alla limitazione di trattamento, su richiesta dell'Ente.

2.3 Il Responsabile del trattamento deve garantire e fornire all'Ente cooperazione, assistenza e le informazioni che potrebbero essere ragionevolmente richieste dalla stessa, per consentirle di adempiere ai propri obblighi ai sensi della normativa applicabile, ivi compresi i provvedimenti e le specifiche decisioni del Garante per la protezione dei dati personali.

2.4 Il Responsabile del trattamento, anche nel rispetto di quanto previsto all'art. 30 del Regolamento, deve mantenere e compilare e rendere disponibile a richiesta della stessa, un registro dei trattamenti dati personali che riporti tutte le informazioni richieste dalla norma.

2.5 Il Responsabile del trattamento assicura la massima collaborazione al fine dell'esperimento delle valutazioni di impatto ex art. 35 del GDPR che l'Ente intenderà esperire sui trattamenti che rivelano, a Suo insindacabile giudizio, un rischio elevato per i diritti e le libertà delle persone fisiche.

3. Le misure di sicurezza

3.1 Il Responsabile del trattamento deve conservare i dati personali garantendo la separazione di tipo logico dai dati personali trattati per conto di terze parti o per proprio conto.

3.2 Il Responsabile del trattamento deve adottare e mantenere appropriate misure di sicurezza, sia tecniche che organizzative, per proteggere i dati personali da eventuali distruzioni o perdite di natura illecita o accidentale,

danni, alterazioni, divulgazioni o accessi non autorizzati, ed in particolare, laddove il trattamento comporti trasmissioni di dati su una rete, da qualsiasi altra forma illecita di trattamento.

3.3. Il Responsabile del trattamento conserva, nel caso siano allo stesso affidati servizi di amministrazione di sistema, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;

3.4 L'Ente attribuisce al Responsabile del trattamento il compito di dare attuazione alla prescrizione di cui al punto 2 lettera e) "Verifica delle attività" del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";

3.5 Il Responsabile del trattamento deve adottare misure tecniche ed organizzative adeguate per salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti all'Ente, con specifico riferimento alle misure intese a prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema.

3.6 Il Responsabile del trattamento adotta le misure di sicurezza di cui all'Appendice "Security" allegata al presente accordo. In ragione della riservatezza delle evidenze di analisi di conformità alle misure di cui alla suddetta Appendice, il Fornitore condivide con l'Ente tali informazioni solo in caso di violazione o data breach. Si sottolinea che, ad ogni buon conto, la sottoscrizione del presente accordo, e dei suoi allegati, equivale ad attestare la conformità alle misure indicate nell'appendice "Security".

3.7 Il Responsabile del trattamento dà esecuzione al contratto in aderenza alle policy dell'Ente in materia di privacy e sicurezza informatica di seguito indicate:

- Delibera di Giunta regionale n. 622 del 5/5/2017 "Approvazione della Politica generale sulla sicurezza dei dati e delle informazioni"
- Determinazione n. 6928/2009 "Disciplinare tecnico su modalità e procedure relative alle verifiche di sicurezza sul sistema informativo, ai controlli sull'utilizzo dei beni messi a disposizione dall'Ente per l'attività

lavorativa con particolare riferimento alle strumentazioni informatiche e telefoniche ed esemplificazioni di comportamenti per il corretto utilizzo di tali beni, da applicare nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna"

- Determinazione n. 4137/2014 "Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta e nell'Assemblea legislativa della Regione Emilia-Romagna".

4. Analisi dei rischi, privacy by design e privacy by default

4.1 Con riferimento agli esiti dell'analisi dei rischi effettuata dall'Ente sui trattamenti di dati personali cui concorre il Fornitore, lo stesso assicura massima cooperazione e assistenza al fine di dare effettività alle azioni di mitigazione previste dall'Ente per affrontare eventuali rischi identificati.

4.2 Il Fornitore dovrà consentire all'Ente, tenuto conto dello stato della tecnica, dei costi, della natura, dell'ambito e della finalità del relativo trattamento, di adottare, sia nella fase iniziale di determinazione dei mezzi di trattamento, che durante il trattamento stesso, ogni misura tecnica ed organizzativa che si riterrà opportuna per garantire ed attuare i principi previsti in materia di protezione dati e a tutelare i diritti degli interessati.

4.3 In linea con i principi di privacy by default, dovranno essere trattati, per impostazione predefinita, esclusivamente quei dati personali necessari per ogni specifica finalità del trattamento, e che in particolare non siano accessibili dati personali ad un numero indefinito di soggetti senza l'intervento di una persona fisica.

4.4 Il Responsabile del trattamento dà esecuzione al contratto in aderenza alle policy di privacy by design e by default adottate dall'Ente e specificatamente comunicate.

5. Soggetti autorizzati ad effettuare i trattamenti - Designazione

5.1 Il Responsabile del trattamento garantisce competenze ed affidabilità dei propri dipendenti e collaboratori autorizzati al trattamento dei dati personali (di seguito anche incaricati) effettuati per conto dell'Ente.

5.2 Il Responsabile del trattamento garantisce che gli incaricati abbiano ricevuto adeguata formazione in materia di protezione dei dati personali e sicurezza informatica, consegnando all'Ente le evidenze di tale formazione.

5.3 Il Responsabile del trattamento, con riferimento alla protezione e gestione dei dati personali, impone ai propri incaricati obblighi di riservatezza non meno onerosi di quelli previsti nel presente Accordo relativamente al trattamento dei dati personali. In ogni caso il Fornitore sarà direttamente ritenuto responsabile per qualsiasi divulgazione dei dati personali dovesse realizzarsi ad opera di tali soggetti.

6. Sub-Responsabili del trattamento di dati personali

6.1 Il Fornitore, in caso di sub-appalto occorso ai sensi della normativa in materia di appalti, imporre al Sub-Responsabile condizioni vincolanti in materia di trattamento dei dati personali non meno onerose di quelle contenute nel presente Accordo.

6.3 Su specifica richiesta dell'Ente, il Fornitore dovrà provvedere a che ogni SubResponsabile sottoscriva direttamente con l'Ente un accordo di trattamento dei dati che, a meno di ulteriori e specifiche esigenze, preveda sostanzialmente gli stessi termini del presente Accordo.

6.4 In tutti i casi, il Fornitore si assume la responsabilità nei confronti dell'Ente per qualsiasi violazione od omissione realizzati da un Sub-Responsabile o da altri terzi soggetti incaricati dallo stesso, indipendentemente dal fatto che il Fornitore abbia o meno rispettato i propri obblighi contrattuali, ivi comprese le conseguenze patrimoniali derivanti da tali violazioni od omissioni.

7. Trattamento dei dati personali fuori dall'area economica europea

7.1 L'Ente non autorizza il trasferimento dei dati personali oggetto di trattamento al di fuori dell'Unione Europea.

8. Cancellazione dei dati personali

8.1 Il Fornitore provvede alla cancellazione dei dati personali trattati per l'esecuzione del presente contratto al termine del periodo di conservazione e in qualsiasi circostanza in cui sia richiesto dall'Ente, compresa l'ipotesi in cui la stessa debba avvenire per dare seguito a specifica richiesta da parte di interessati.

8.2 Alla cessazione del presente Accordo, per qualsiasi causa essa avvenga, i dati personali dovranno, a discrezione dell'Ente, essere distrutti o restituiti alla stessa, unitamente a qualsiasi supporto fisico o documento contenente dati personali di proprietà dell'Ente.

9. Audit

9.1 Il Fornitore si rende disponibile a specifici audit in tema di privacy e sicurezza informatica da parte dell'Ente.

9.2 Il Fornitore consente, pertanto, all'Ente l'accesso ai propri locali e ai locali di qualsiasi SubResponsabile, ai computer e altri sistemi informativi, ad atti, documenti e a quanto ragionevolmente richiesto per verificare che il Fornitore, e/o i suoi Sub-fornitori, rispettino gli obblighi derivanti dalla normativa in materia di protezione dei dati personali e, quindi, da questo Accordo.

9.3 L'esperimento di tali audit non deve avere ad oggetto dati di terze parti, informazioni sottoposte ad obblighi di riservatezza degli interessi commerciali.

9.4 Nel caso in cui l'audit fornisca evidenze di violazioni alla normativa in materia di protezione dei dati personali e al presente Accordo, quali ad esempio quelle indicate all'art. 83 comma 5 (con esclusione della lett. e) l'Ente può risolvere il Contratto o chiedere una cospicua riduzione del prezzo.

9.5 Nel caso in cui l'audit fornisca evidenze di violazioni gravi, quali ad esempio quelle indicate all'art. 83 comma 4 lett. a), l'Ente può chiedere una cospicua riduzione del prezzo.

9.6 Il rifiuto del Fornitore di consentire l'audit all'Ente comporta la risoluzione del contratto.

10. Indagini dell'Autorità e reclami

10.1 Nei limiti della normativa applicabile, il Fornitore o qualsiasi SubResponsabile informa senza alcun indugio l'Ente di qualsiasi

a) richiesta o comunicazione promanante dal Garante per la protezione dei dati personali o da forze dell'ordine

b) istanza ricevuta da soggetti interessati

Il Fornitore fornisce, in esecuzione del contratto e, quindi, gratuitamente, tutta la dovuta assistenza all'Ente per garantire che la stessa possa rispondere a tali istanze o comunicazioni nei termini temporali previsti dalla normativa e dai regolamentari applicabili.

11. Violazione dei dati personali e obblighi di notifica

11.1 Il Fornitore, in virtù di quanto previsto dall'art. 33 del Regolamento, deve comunicare a mezzo di posta elettronica certificata all'Ente nel minor tempo possibile, e comunque non oltre 24 (ventiquattro) ore da quando ne abbia avuto conoscenza, qualsiasi violazione di sicurezza che abbia comportato accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, ivi incluse quelle che abbiano riguardato i propri sub-Fornitori. Tale comunicazione deve contenere ogni informazione utile alla gestione del *data breach,* oltre a

a) descrivere la natura della violazione dei dati personali

b) le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

c) i recapiti del DPO nominato o del soggetto competente alla gestione del data breach;

d) la descrizione delle probabili conseguenze della violazione dei dati personali;

e) una descrizione delle misure adottate o che si intende adottare per affrontare la Violazione della sicurezza, compreso, ove opportuno, misure per mitigare i suoi possibili effetti negativi

11.2 Il Fornitore deve fornire tutto il supporto necessario all'Ente ai fini delle indagini e sulle valutazioni in ordine alla violazione di dati, anche al fine di individuare, prevenire e limitare gli effetti negativi della stessa, conformemente ai suoi obblighi ai sensi del presente articolo e, previo accordo con l'Ente, per svolgere qualsiasi azione che si renda necessaria per porre rimedio alla violazione stessa. Il Fornitore non deve rilasciare, né pubblicare alcun comunicato stampa o relazione riguardante eventuali data breach o violazioni di trattamento senza aver ottenuto il previo consenso scritto dell'Ente.

12. Responsabilita' e manleve

12.1 Il Fornitore tiene indenne e manleva l'Ente da ogni perdita, costo, sanzione, danno e da ogni responsabilità di qualsiasi natura derivante o in connessione con una qualsiasi violazione da parte del Fornitore delle disposizioni contenute nel presente Accordo.

12.2 A fronte della ricezione di un reclamo relativo alle attività oggetto del presente Accordo, il Fornitore:

13.3.1 avverte, prontamente ed in forma scritta, l'Ente del Reclamo

13.3.2 non fornisce dettagli al reclamante senza la preventiva interazione con l'Ente

13.3.3 non transige la controversia senza il previo consenso scritto dell'Ente;

13.3.4 fornisce all'Ente tutta l'assistenza che potrebbe ragionevolmente richiedere nella gestione del reclamo.

_____, lì ___ ___ ___

LA REGIONE EMILIA-ROMAGNA

_____

L'AFFIDATARIO

_____

Allegato 1

GLOSSARIO

"**Garante per la protezione dei dati personali":** è l'autorità di controllo responsabile per la protezione dei dati personali in Italia;

"**Dati personali ":** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

"**GDPR" o "Regolamento":** si intende il Regolamento UE 2016/679 sulla protezione delle persone fisiche relativamente al trattamento dei dati personali e della loro libera circolazione (General Data Protection Regulation) che sarà direttamente applicabile dal 25 maggio 2018;

"**Normativa Applicabile":** si intende l'insieme delle norme rilevanti in materia protezione dei dati personali , incluso il Regolamento Privacy UE 2016/679 (GDPR) ed ogni guprovvedimento del Garante per la protezione dei dati personali e del WP Art. 29.

"**Appendice Security":** consiste nelle misure di sicurezza che il Titolare determina assicurando un livello minimo di sicurezza, e che possono essere aggiornate ed implementate dal Titolare, di volta in volta, in conformità alle previsioni del presente Accordo;

"**Reclamo":** si intende ogni azione, reclamo, segnalazione presentata nei confronti del Titolare o di un Suo Responsabile del trattamento;

"**Titolare del Trattamento":** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

“**Trattamento”:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

“**Responsabile del trattamento”**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

“**Pseudonimizzazione”**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile

Allegato 2

Appendice “Security”

REQUISITI ORGANIZZATIVI

ID	Descrizione
1	Designazione di un DPO o di un Responsabile della sicurezza informatica
2	Adottare un piano di Disaster recovery
3	Effettuare formazione in materia di privacy e sicurezza informatica ai dipendenti
4	Prevedere procedure per regolamentare l’accesso fisico alle aree dove vengono trattati i dati
5	Adottare un regolamento con istruzioni ai dipendenti per l’utilizzo degli strumenti informatici
6	Adottare una policy per la gestione dei data breach
7	Implementare un sistema di videosorveglianza con finalità di tutela del patrimonio aziendale

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Descrizione
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4

1	1	2	Implementare ABSC 1.1.1 attraverso uno strumento automatico
1	2	1	Implementare il "logging" delle operazione del server DHCP.
1	2	2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.
1	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.
1	3	2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.
1	4	1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.
1	4	2	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Descrizione
2	1	1	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.
2	2	1	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.
2	2	2	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).

2	2	3	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.
2	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.
2	3	2	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Descrizione
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
3	1	2	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.
3	2	1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.
3	2	2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
3	2	3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.
3	3	1	Le immagini d'installazione devono essere memorizzate offline.
3	3	2	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.

3	4	1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).
3	5	1	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Descrizione
4	1	1	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
4	1	2	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.
4	2	1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.
4	2	2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità
4	2	3	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.
4	3	1	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.
4	3	2	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.

4	4	1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
4	4	2	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione
4	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.
4	5	2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.
4	6	1	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.
4	7	1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
4	7	2	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.
4	8	1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
4	8	2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.
4	9	1	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.
4	10	1	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID	Descrizione

5	1	1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
5	1	2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
5	1	3	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.
5	2	1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
5	3	1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
5	4	1	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.
5	4	2	Generare un'allerta quando viene aggiunta un'utenza amministrativa.
5	4	3	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.
5	5	1	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.
5	7	1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
5	7	2	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.
5	7	3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).
5	7	4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
5	7	5	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.
5	7	6	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.

5	8	1	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.
5	9	1	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.
5	10	1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
5	10	2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
5	10	3	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
5	10	4	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).
5	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
5	11	2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Descrizione
8	1	1	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
8	1	2	Installare su tutti i dispositivi firewall ed IPS personali.

8	1	3	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.
8	2	1	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.
8	2	2	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.
8	3	1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
8	4	1	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.
8	5	1	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.
8	6	1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.
8	7	1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
8	7	2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
8	7	3	Disattivare l'apertura automatica dei messaggi di posta elettronica.
8	7	4	Disattivare l'anteprima automatica dei contenuti dei file.
8	8	1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
8	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.

8	9	2	Filtrare il contenuto del traffico web.
8	9	3	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).
8	10	1	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.
8	11	1	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Descrizione
10	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
10	3	1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.
10	4	1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Descrizione
13	1	1	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica
13	2	1	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti
13	7	1	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.
13	8	1	Bloccare il traffico da e verso url presenti in una blacklist.