PIANO DELLA SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

Il presente documento, in attuazione di quanto previsto dalle Linee guida, riporta il piano della sicurezza del sistema di gestione informatica dei documenti (SdP) elaborato nel rispetto delle:

- misure di sicurezza predisposte dall'AgID e dagli altri organismi preposti;
- disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio fatta; ● indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AGID.

1. Obiettivi del piano della sicurezza informatica dei documenti Il
piano della sicurezza è finalizzato a garantire che:

- i documenti e le informazioni trattate dal Consiglio regionale siano disponibili, integre e riservate tramite l'adozione di idonee misure di sicurezza;
- i dati personali, ivi comprese le categorie particolari di dati personali di cui agli artt. 9 e 10 del Regolamento UE 679/2016 (GDPR), vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

2. Contesto di riferimento

Le applicazioni informatiche in uso al Consiglio regionale sono le stesse in uso presso l'amministrazione regionale, ubicate in hosting presso il Data Center regionale, e pertanto possono applicarsi anche le stesse considerazioni inerenti la sicurezza fisica e logica delle informazioni

Il SdP è quindi ospitato presso il Data Center regionale, gestito dalla società in house Insiel s.p.a., nominata quale Responsabile del trattamento ex art. 28 del GDPR, pertanto il piano della sicurezza prevede due componenti, una relativa ad Insiel s.p.a., quale produttore e gestore del SdP e Responsabile del trattamento, ed una relativa al Consiglio regionale, quale Titolare del trattamento e fruitore del SdP.

A seguito infatti della deliberazione dell'Ufficio di Presidenza del Consiglio regionale n. 14 del 28 giugno 2018, è stato sottoscritto e protocollato 9483/2018 l'Atto di nomina a Insiel quale Responsabile del trattamento dei Dati Personali connesso all'erogazione dei servizi di assistenza informatica, sviluppo software, conduzione e gestione di infrastrutture, gestione documentale e forniture di beni informatici.

Il Piano della sicurezza si basa sull'analisi dei rischi a cui sono esposti i dati e i documenti trattati e rispetta le indicazioni fornite a livello nazionale dall'AgID. Nello specifico il piano della sicurezza descrive:

- le misure di sicurezza relative alle componenti organizzativa, fisica, logica e infrastrutturale adottate da Insiel s.p.a. e dal Consiglio regionale nel contesto della gestione documentale;
- le modalità di funzionamento del SdP e di accesso ai documenti in esso contenuti;
- le misure specifiche adottate in materia di protezione dei dati personali, ai sensi dell'art. 32 del GDPR, e la procedura da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del GDPR da parte di Insiel s.p.a. e della Regione;

L'allegato 1 al presente documento riporta "Analisi dei rischi e misure di sicurezza informatica adottate" mentre l'allegato 2 riporta "Analisi dei rischi nell'ambito della gestione documentale e misure organizzative e tecniche adottate"

Le misure descritte sono oggetto di monitoraggio periodico in merito alla loro efficacia ed efficienza.

Il piano della sicurezza è soggetto a revisione con cadenza almeno biennale e può essere modificato a seguito di eventi gravi.

3. Misure minime di sicurezza in ambito ICT

In attuazione di quanto previsto dalla Circolare AgID 18 aprile 2017, n. 2, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni", il Consiglio regionale, in collaborazione con Insiel s.p.a., ha approvato con Decreto n.952 di data 28/12/2017 del Direttore del Servizio sistemi informativi, comunicazione e affari generali il "Modulo di implementazione delle misure minime di sicurezza delle pubbliche amministrazioni", allegato 3 al presente documento.

Tali misure possono essere oggetto di riesame in conseguenza del verificarsi di incidenti attinenti alla sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza, che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza, portare alla modifica del livello di sicurezza complessivo o ad aggiornamenti delle prescrizioni minime di sicurezza richieste dall'AgID; il riesame può avvenire anche a seguito dei risultati delle attività di audit esterno.

Insiel s.p.a. rispetta le indicazioni contenute nella circolare AgID del 18 aprile 2017, n. 2, e il "Modulo di implementazione delle misure minime di sicurezza delle pubbliche amministrazioni" approvato dal Consiglio regionale.

4. Componente organizzativa della sicurezza

Insiel s.p.a. si avvale di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) certificato secondo la norma UNI EN ISO/IEC 27001:2017 che contiene i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni dal punto di vista della sicurezza logica, fisica/ambientale e organizzativa; inoltre il SGSI rispetta le linee guida ISO/IEC 27017, in relazione alla protezione dei servizi erogati in modalità cloud, nonché alla linea guida ISO/IEC 27018, in relazione alla protezione delle informazioni ascrivibili a dati personali, sempre nell'ottica dell'erogazione di servizi cloud; il SGSI comprende, nel suo ambito di applicazione, le infrastrutture di sicurezza fisica e logica del Data Center.

In attuazione di quanto previsto dagli standard sopra citati, Insiel s.p.a. ha individuato e definito formalmente ruoli e responsabilità che comprendono la figura del Responsabile del SGSI e diversi soggetti responsabili dell'implementazione e dell'adozione delle misure di sicurezza.

È presente un processo di governo degli eventi rilevanti per la sicurezza che prevede la rilevazione, la gestione di tali eventi, la risoluzione degli incidenti, la raccolta degli spunti per il miglioramento.

Il personale specializzato sui temi della sicurezza informatica contempla tecnici certificati ISO 27001 (Sistemi di gestione della sicurezza delle informazioni), CISSP (Certified Information Systems Security Professional) e CISM (Certified Information Security Manager).

5. Componente fisica della sicurezza

La sede che ospita il Data Center soddisfa i requisiti di cui al d.lgs. n. 81/2008 recante la "Tutela della salute e della sicurezza nei luoghi di lavoro".

L'accesso fisico è controllato, i dipendenti utilizzano badge magnetici per gli ingressi e gli ospiti devono venir identificati. Le aree esterne sono sorvegliate da un sistema televisivo a circuito chiuso mediante telecamere dislocate lungo il perimetro; le uscite di sicurezza sono controllate da sensori a contatto che rilevano intrusioni o anomalie.

È, inoltre, presente un controllo regolare di ronda notturna da parte di un servizio di Guardie Giurate che integra il presidio operativo, comunque presente 24 ore su 24; l'accesso ai locali tecnici è permesso solamente al personale autorizzato. L'intera area è protetta da un impianto automatico di controllo fumi e spegnimento automatico a gas.

L'accesso fisico alle sedi della Regione è controllato, i dipendenti utilizzano badge magnetici per gli ingressi e gli ospiti devono venir identificati; nelle sedi principali di Trieste e Udine è installato un sistema a tornelli.

La sede del Consiglio regionale è dotata di un sistema di telecamere che controlla il perimetro esterno dei due palazzi e presenta un servizio di guardiania o di portierato.

6. Componente logica della sicurezza

La componente logica della sicurezza è ciò che garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Per gli utenti interni al Consiglio regionale, l'accesso al SdP avviene, per le applicazioni di tipo web, per mezzo del trasferimento automatico delle credenziali utente acquisite al momento dell'autenticazione al dominio, mentre, per le applicazioni di tipo client / server, per mezzo di codice utente e password.

Viene richiesta la modifica della password al momento del primo accesso al sistema ed allo scadere di sei mesi dall'ultima variazione; il mancato accesso ad un sistema applicativo per un periodo superiore ai sei mesi comporta la decadenza delle credenziali dell'utente interessato che deve richiederne la riattivazione.

Nel SdP sono presenti, per ogni utente, le informazioni che determinano la disponibilità delle funzioni applicative e la possibilità di accedere ai dati ed ai documenti archiviati nel sistema.

I soggetti esterni accedono, di norma, ai servizi online di acquisizione di istanze tramite il Sistema pubblico per la gestione delle identità digitali –SPID, la Carta d'Identità Elettronica o la Carta Nazionale dei Servizi, in attuazione di quanto previsto dal d.lgs. 82/2005 recante il Codice dell'Amministrazione Digitale.

Il sistema è ospitato nel Data Center regionale dove:

- è presente una struttura di accesso ad Internet a più livelli, separati dai dispositivi firewall. Inoltre, sono implementate politiche di segmentazione delle reti in contesti logici diversi a seconda delle caratteristiche dei servizi erogati;
- sono in uso sistemi IDS (Intrusion Detection System) e IPS (Intrusion Prevention System);
- esiste un presidio attivo 24 ore su 24 che provvede alle attività necessarie a garantire la regolare operatività dei servizi;
- è presente un sistema di backup dei dati. In particolare, viene eseguito un backup completo del Database ogni settimana ed uno incrementale ogni notte; ● i sistemi utilizzano dispositivi di ridondanza.

Inoltre Insiel s.p.a. è dotata di un Sistema di Gestione della Continuità Operativa, che è oggetto di audit periodico, sia interno che di terza parte, ed è certificato secondo la norma EN ISO 22301:2012 relativa alla gestione della continuità operativa.

7. Componente infrastrutturale della sicurezza

Presso il Data Center regionale sono disponibili i seguenti impianti che costituiscono la componente infrastrutturale della sicurezza:

- uscite di sicurezza;
- luci di emergenza;
- sistema di videosorveglianza;
- guardiola all'ingresso presidiata da guardie giurate;
- sensori antintrusione;
- controllo degli accessi e dei varchi fisici;
- sistema di controllo dei fumi e spegnimento automatico a gas Inergen; ● continuità elettrica.

Gli impianti e le considerazioni precedenti valgono anche per la componente infrastrutturale della sicurezza per il Consiglio regionale, coerentemente con il livello di criticità di ciascuna sede.

8. Gestione degli accessi al SdP e al Database

Il SdP registra gli accessi da parte degli utenti e le attività riferibili all'attribuzione ed alla modifica delle password ed alla riattivazione di credenziali scadute.

Vengono altresì memorizzate le attività di aggiornamento dei dati di protocollo con evidenza dell'utente che le ha effettuate e, per quanto riguarda i dati essenziali, con registrazione della versione precedente dell'informazione.

Le registrazioni degli accessi da parte degli Amministratori di Sistema vengono effettuate con l'impiego di un'apposita infrastruttura tecnologica che garantisce l'accesso mediante credenziali di autenticazione individuali ed è volto a garantire:

- la registrazione degli accessi (access log) ai sistemi di elaborazione e agli archivi elettronici, comprendenti i riferimenti temporali e la descrizione dell'evento che le ha generate; ● che le registrazioni possiedano caratteristiche di completezza e inalterabilità; ● che le registrazioni vengano conservate per un periodo non inferiore ai sei mesi.

Con le medesime modalità vengono eseguite le registrazioni degli accessi degli Amministratori di Sistema al Database.

Viene, infine, eseguito un backup completo del Database ogni settimana ed uno incrementale ogni notte.

9. Strumenti per la trasmissione e l'interscambio dei documenti informatici

La trasmissione dei documenti informatici avviene principalmente tramite posta elettronica certificata, le caselle PEC di cui si avvale il Consiglio regionale sono rilasciate da un fornitore esterno certificato (Gestore), che fornisce garanzie che vengono considerate dall'Amministrazione idonee dal punto di vista della sicurezza.

Fra le principali misure di sicurezza che vengono adottate per garantire che le attività del Gestore si svolgano secondo i requisiti di sicurezza richiesti dalla normativa vigente, si ricordano:

- I meccanismi per il controllo dell'accesso logico e fisico alle risorse informatiche e ai sistemi del Gestore, che forniscono le seguenti funzionalità:
  - identificano ed autenticano le persone autorizzate ad accedere alle risorse informatiche; o impediscono ad una persona non autorizzata di poter accedere alle risorse informatiche; o registrano i dati significativi di tutti gli eventi di accesso in modo che si possa in ogni caso risalire alla persona che ha dato origine ad un determinato evento.
- Il controllo dell'accesso ai locali protetti adotta una politica di autorizzazioni e di procedure di registrazione e auditing:
  - l'accesso alla Sala Sistemi del Centro Servizi del Gestore è basato sul principio secondo il quale è consentito l'accesso solo a chi è esplicitamente autorizzato: o ogni persona che intende accedere alle risorse della Sala Sistemi è identificata in modo certo, mediante l'utilizzo di una smartcard o un token personale.
  - ogni operazione di firma di messaggi, avvisi e ricevute svolta dal sistema di posta certificata viene tracciata in un registro di controllo al quale viene associata con periodicità almeno giornaliera una marca temporale.

10. Accesso ai documenti informatici e gestione delle abilitazioni

L'accesso ai documenti informatici è effettuato mediante il SdP, con le modalità di seguito descritte.

10.1. Utenti interni al Consiglio regionale

L'accesso al SdP è consentito solamente agli utenti esplicitamente autorizzati e la fruizione di funzioni ed informazioni è condizionata dal tipo di abilitazione attribuita ad ogni utente.

Le abilitazioni vengono attribuite per mezzo di apposite funzioni messe a disposizione del SdP e vengono richieste e formalizzate secondo le modalità descritte di seguito.
Gli utenti vengono, di norma, associati ad uno o più gruppi funzionali ai quali sono stati attribuiti specifici diritti di accesso, registrazione, modifica, annullamento su uno o più registri di protocollo, generale o particolare. Gli utenti ereditano le caratteristiche proprie dei gruppi funzionali a cui sono associati.
In più, per ogni utente, possono essere definite specifiche abilitazioni che determinino ulteriori diritti rispetto a quelli dei gruppi funzionali di appartenenza.
La fruizione delle registrazioni di protocollo è consentita agli utenti ai quali, in modo diretto oppure in quanto appartenenti ad una struttura, sia stato attribuito uno specifico diritto di accesso. Ciò può avvenire o perché l'utente o la struttura sono gli autori del documento, oppure perché risultano essere assegnatari di un documento pervenuto, oppure perché partecipano ad un flusso di lavorazione interno.
Alle registrazioni relative a documenti con particolari caratteristiche di riservatezza sono assegnati diversi livelli di riservatezza, da 1 a 9, in modo da permetterne l'accesso solamente agli utenti in possesso di un livello di abilitazione pari o superiore.
I livelli di riservatezza sono gestiti dalla Struttura stabile inf. Serv. "Ufficio protocollo ed archivio (UPA) del Consiglio regionale e vengono assegnati dal Coordinatore della struttura su indicazione del Responsabile della gestione documentale, prima dell'attività di assegnazione di cui al paragrafo 6.1.3.2 del Manuale.
In presenza di documenti che riportino informazioni appartenenti alle categorie particolari di dati personali di cui agli artt. 9 e 10 del GDPR, alla registrazione deve essere assegnato il livello di riservatezza massimo pari a 9. È possibile definire strutture alle quali vengano assegnati utenti che, in virtù del loro ruolo istituzionale o delle loro mansioni, accedono alla totalità delle registrazioni di uno o più registri.
Le abilitazioni o disabilitazioni dei dipendenti del Consiglio regionale devono essere richieste da un funzionario responsabile (Segretario generale, Direttore di Servizio, Posizione Organizzativa) al responsabile della gestione documentale tramite l'invio di una mail.
Le richieste devono necessariamente riportare le seguenti informazioni:

A) Se richiesta di abilitazione:

- Descrizione richiesta: Abilitazione a protocollo e/o visura protocollo e/o iteratti;
- Utente: Matricola / Cognome / Nome;
- Struttura/e alla quale l'utente va assegnato: codice della struttura / descrizione della struttura così come definiti nel sistema di protocollo, con l'indicazione della struttura primaria;
- Dicitura: La presente richiesta di abilitazione sostituisce oppure integra le abilitazioni eventualmente già attribuite all'utente
- Livello di abilitazione (da 1 a 9) per consentire l'accesso a documenti caratterizzati da un livello di riservatezza superiore a "0". Se non fornito, viene attribuito il livello di abilitazione "0".

B) Se richiesta di disabilitazione:

- Descrizione richiesta: Disabilitazione a protocollo e/o visura protocollo e/o iteratti; ● Utente: Matricola / Cognome / Nome
- Struttura/e dalla quale l'utente va rimosso: codice struttura.

Il responsabile della gestione documentale provvede alla valutazione delle richieste e, in caso positivo, le approva e le inoltra all'Insiel s.p.a. per l'esecuzione.

Ogni utente abilitato ad accedere al SdP viene configurato per quanto riguarda:

- le funzioni di cui può fruire (protocollazione in arrivo/partenza, interrogazioni, firma digitale, ed altro);
- le registrazioni su cui vengono attribuiti i diritti di gestione o visibilità.

Gli utenti ereditano le abilitazioni attribuite alle rispettive strutture di appartenenza.
Nel caso in cui, a seguito di modifiche dell'organizzazione interna del Consiglio regionale, si renda necessario istituire nuove strutture o modificare la configurazione di strutture esistenti tale richiesta dovrà essere inoltrata con le medesime modalità.
Le richieste devono necessariamente riportare le seguenti informazioni:

- Creazione di una nuova struttura: o codice struttura (proposta); o denominazione struttura.
- Configurazione struttura:
  - o codice e denominazione delle strutture esistenti eventualmente collocate a livello gerarchico superiore; o codice e denominazione delle strutture esistenti o nuove eventualmente collocate a livello gerarchico inferiore;
  - o diritti di visibilità rispetto ai documenti di pertinenza di strutture di cui ai punti precedenti;
  - o Codice AOO e codice registro su cui la struttura può operare.

In alternativa, è possibile indicare codice e descrizione di una struttura la cui configurazione deve essere replicata sulla struttura interessata.
Poiché le abilitazioni di visura sono legate all'associazione ad una o più strutture, le stesse vengono meno al momento della rimozione dell'associazione del dipendente dalle strutture stesse. Restano visibili le registrazioni in cui l'utente ha avuto parte attiva (creazione, trattamento in iter).
Al fine di mantenere un controllo efficiente ed efficace in materia di accesso alle informazioni ed ai sistemi, l'UPA esegue dei controlli a campione al fine di verificare la rispondenza tra abilitazioni possedute e struttura di appartenenza e un controllo semestrale sulla disabilitazione del personale cessato.

10.2. Utenti esterni al Consiglio regionale - Amministrazioni

Sono in fase di studio funzioni che permettano l'accesso diretto ai documenti da parte di altre Amministrazioni.

10.3. Utenti esterni al Consiglio regionale - Privati

Sono in fase di studio funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti da parte di privati cittadini.

11. Protezione dei dati personali

La gestione dei flussi documentali e il SdP sono ispirati alle norme in materia di tutela dei dati personali, con particolare riferimento al concetto di accountability ed alla capacità di adottare un processo efficace per la protezione degli stessi in grado di ridurre al minimo i rischi di una loro possibile violazione.
In merito al trattamento dei dati personali, Insiel s.p.a. agisce in qualità di Responsabile del trattamento ai sensi dell'art. 28 del GDPR ed attua gli adempimenti previsti con particolare riguardo a:

- Tenuta di un registro delle attività di trattamento in qualità di Responsabile.
- Rispetto delle istruzioni ricevute dal Titolare, formulate in primis nell'atto di designazione a Responsabile del trattamento.
- Adozione delle misure di sicurezza previste sulla base dell'analisi dei rischi di cui all'allegato n. 1 tra cui: o misure per assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento tramite il SGSI di cui si è dotata la Società;
  - misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, tramite il Sistema di Gestione della Continuità operativa di cui si è dotata la Società;
  - procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento: secondo quanto previsto dallo standard internazionale ISO27001, è previsto che siano condotti, ad intervalli pianificati, audit interni per fornire

informazioni tali da permettere di riconoscere se il SGSI è conforme allo standard di riferimento adottato;

- misure di protezione dei dati durante la trasmissione: nelle reti vengono previste delle configurazioni atte a segregare gruppi di servizi, di utenti e di sistemi informativi, secondo i requisiti previsti;
- misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati, progettando e applicando la sicurezza fisica agli uffici, ai locali ed agli impianti ove avviene il trattamento di dati personali. Le apparecchiature vengono disposte e protette al fine di ridurre i rischi derivanti dalle minacce e dai pericoli ambientali, oltre alle occasioni di accesso non autorizzato;
- misure per limitare l'accesso ai dati esclusivamente al personale autorizzato, tramite sistemi di autenticazione;
- misure per garantire la registrazione degli eventi di accesso da parte degli Amministratori di Sistema, secondo quanto previsto dal Provvedimento del Garante del 27.11.2008 e in base alle istruzioni ricevute dal Titolare;
- misure per garantire la responsabilità: la Società identifica per iscritto i propri dipendenti deputati a trattare i Dati Personali tramite apposite lettere di incarico, individuando l'ambito di trattamento consentito e fornendo loro le istruzioni idonee allo scopo, in particolare vincolandoli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro. La Società ne cura la formazione, vigila sul loro operato e comunica al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi. La Società designa quali Amministratori di Sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali; predispone e conserva l'elenco contenente gli estremi identificativi degli Amministratori di Sistema e le funzioni ad essi attribuite; comunica periodicamente al Titolare tale elenco aggiornato; verifica annualmente il loro operato, informando il Titolare circa le risultanze di tale verifica. La Società, qualora si avvalga di fornitori terzi per eseguire le attività di trattamento, provvede a designarli sub-responsabili del trattamento, imponendo i medesimi obblighi cui è tenuta ad adempiere in qualità di Responsabile ex art. 28 GDPR e comunica i nominativi dei fornitori al Titolare.

- Per i trattamenti di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati (artt. 9 e 10 GDPR), adozioni di limitazioni e garanzie che tengono pienamente conto della natura dei dati e dei rischi connessi, quali il trattamento dati permesso solo per le finalità prestabilite dal Titolare, limitazioni all'accesso ai dati, limitazioni all'accesso fisico ai locali in cui i dati personali sono trattati, accesso con autenticazione, autorizzazione per iscritto del personale che accede ai dati, dotato di formazione specializzata e tenuto all'obbligo di riservatezza; registrazione degli eventi con conservazione dei log di accesso ai dati da parte degli amministratori di sistema per almeno 6 mesi; applicazione di misure per limitare trasferimenti successivi dei dati; trattamento dei dati esclusivamente nel territorio dell'Unione Europea; misure per garantire la continuità operativa al fine di assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
- In caso di violazione dei dati personali, collaborazione e supporto al Titolare nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del GDPR, tenuto conto della natura del trattamento e delle informazioni a disposizione della Società.
- In caso di una violazione dei dati personali trattati dal Titolare, collaborazione e supporto al Titolare:

1. nel notificare la violazione dei dati personali all'autorità di controllo competenti, senza ingiustificato ritardo dopo che il Titolare ne è venuto a conoscenza, se del caso (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
2. nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del GDPR, devono essere indicate nella notifica del Titolare e includere almeno:
    - la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
    - le probabili conseguenze della violazione dei dati personali; o le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

   Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo;
3. nell'adempiere, in conformità all'articolo 34 del GDPR, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

In caso di una violazione dei dati personali trattati dalla Società in qualità di Responsabile, invio di una notifica al Titolare senza ingiustificato ritardo contenente almeno:

1. una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
2. i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
3. le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Il Consiglio regionale agisce in qualità di Titolare ed attua gli adempimenti previsti dal GDPR con particolare riguardo a:

- Tenuta di un registro delle attività di trattamento.
- Nomina dei Responsabili del trattamento con indicazione precisa dei comportamenti a cui attenersi nel rispetto di quanto previsto dall'art. 28 del GDPR.

Inoltre, al fine di mitigare le minacce individuate nell'analisi dei rischi di cui all'allegato 2 e garantire la riservatezza dei dati trattati, il Consiglio regionale ha adottato, oltre alle misure già descritte nei paragrafi precedenti, i seguenti ulteriori accorgimenti:

- impartire istruzioni al personale autorizzato ad accedere al SdP quali:
    - trattare i dati personali in modo lecito e secondo correttezza; o raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
    - verificare che tali dati siano esatti e, se necessario, provvedere all'aggiornamento; o comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati a riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti;

- astenersi dal comunicare a terzi, al di fuori dell'ambito lavorativo, qualsivoglia dato personale; o informare tempestivamente il Titolare del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;
- accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni; o non fornire dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare; o non fornire dati e informazioni ai diretti interessati, senza avere la certezza della loro identità; o quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, ritirare tempestivamente i documenti stampati per evitare che soggetti non abilitati al trattamento ne prendano visione.
- non salvare documenti contenenti dati personali sulle risorse locali (hard disk della postazione pc o del notebook o comunque di qualsiasi dispositivo aziendale) o su dispositivi di memorizzazione esterni (hard disk esterni, chiavette usb) o ancora su dvd/cd-rom;
- a fine turno di lavoro, cancellare dalle risorse locali (e svuotare il cestino) eventuali file contenenti dati personali, facendo attenzione alla cartella "Download" o alla cartella dove vengono scaricati i file dal browser;
- non comunicare ad altri o dare evidenza delle credenziali di accesso al proprio computer e agli applicativi in uso;
- in caso di assenza momentanea dalla propria postazione accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone chiudendo la sessione di lavoro attraverso la disconnessione (logout) oppure, in alternativa, attivando un salvaschermo protetto dalle credenziali di autenticazione.
- spegnere il proprio computer al termine delle ore di servizio.

- impartire istruzioni specifiche al personale addetto alla protocollazione quali:
  - smistare i documenti solo al gruppo funzionale del responsabile della struttura interna alla direzione centrale o struttura direzionale equiparata competente alla trattazione del procedimento a cui il documento si riferisce;
- impartire istruzioni al personale nella gestione della documentazione cartacea quali:
  - non lasciare incustoditi i documenti contenenti dati personali nello svolgimento dell'attività lavorativa e al termine del turno di lavoro conservarli in archivi ad accesso controllato, al fine di escludere l'accesso agli stessi da parte di persone non incaricate al trattamento;
  - conservare la documentazione contenente le categorie particolari di dati personali di cui agli artt. 9 e 10 del GDPR in armadi muniti di serratura, al fine di escludere l'acquisizione o la presa visione degli stessi, da parte di persone non incaricate al trattamento;
  - qualora sia necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti" o, in assenza, sminuzzare i documenti in modo da non essere più ricomponibili;
  - nella movimentazione o trasmissione dei documenti all'interno del Consiglio regionale adottare idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in contenitori o buste chiuse).
- limitare le informazioni relative a stati, fatti e qualità personali contenute nei documenti trasmessi all'interno del Consiglio regionale o a soggetti esterni a quelle che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse;

- adozione di un sistema di sicurezza che nello svolgimento delle attività di registrazione di protocollo garantisca la protezione dei dati personali registrati in base all'architettura del sistema informativo, ai controlli sull'accesso e ai livelli di autorizzazione previsti, come descritto nei capitoli precedenti.

Inoltre, in attuazione di quanto previsto dall'art. 46 del CAD, al fine di garantire la riservatezza dei dati particolari di cui agli artt. 9 e 10 del GDPR, i documenti informatici trasmessi ad altre pubbliche amministrazioni per via digitale possono contenere soltanto i dati sensibili e giudiziari consentiti da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisiti.

In caso di violazione dei dati personali ai sensi degli artt. 33 e 34 del GDPR, il Consiglio regionale segue le procedure previste dalla normativa vigente in relazione al Data Breach.

Analisi dei rischi e misure di sicurezza informatica adottate

1. Ambito dell'analisi dei rischi – identificazione degli asset

Il focus della presente analisi dei rischi attiene ai documenti informatici ed ai rischi che insistono sulla sicurezza degli stessi (riservatezza, disponibilità ed integrità dell'informazione), rispetto ad un set di minacce identificato ed in considerazione del contesto operativo di trattamento nell'ambito delle soluzioni tecnologiche fornite da Insiel s.p.a in qualità di Responsabile del Trattamento ai sensi dell'art.28 del Regolamento UE 2016/679.

Ulteriori considerazioni rispetto ad altre tipologie di rischio possono essere derivate dalle stesse o essere ad esse collegate, in relazione al contesto di trattamento specifico operato dal Consiglio regionale in qualità di Titolare dei dati e alla natura delle informazioni presenti nei documenti stessi.

Tale contestualizzazione è in linea con quanto indicato dalla norma ISO/IEC 27005:2018, lo standard che fornisce alle organizzazioni le linee guida per la gestione efficace ed efficiente dei rischi relativi alla sicurezza delle informazioni, al fine di proteggere le proprie informazioni e quelle dei propri clienti.

Asset primario	**Asset collegati – relativi ad attività in capo al responsabile INSIEL**
Documento informatico	Sito di elaborazione dati – Data Center regionale
	Sistemi di elaborazione dati – HW/SW
	Reti di comunicazione
	Personale – Amministratori di Sistema
	Organizzazione interna - INSIEL
	Dati / file

2. Identificazione delle minacce / agenti di rischio

Gli asset considerati, collegati ai documenti informatici che costituiscono il patrimonio documentale del Titolare, sono sottoposti all'azione di diverse minacce.

Tra queste, le categorie di minacce considerate nella presente analisi del rischio rispetto all'ambito di riferimento identificato riguardano le diverse tipologie di asset considerati e sono di seguito riassunte:

Minaccia	**Asset impattati**
Danneggiamento fisico	Sito di elaborazione dati – Data Center regionale
	Sistemi di elaborazione dati – HW/SW
Eventi naturali	Sito di elaborazione dati – Data Center regionale
Perdita di servizi essenziali (alimentazione elettrica / connettività)	Sito di elaborazione dati – Data Center regionale
	Reti di comunicazione
Compromissione delle informazioni	Sistemi di elaborazione dati – HW/SW
	Dati / file
Guasti tecnici	Reti di comunicazione
	Sistemi di elaborazione dati – HW/SW

Azioni non autorizzate	Personale – Amministratori di Sistema
	Organizzazione interna - INSIEL

Attacchi informatici	Sistemi di elaborazione dati – HW/SW
	Reti di comunicazione
	Dati / file
Errori	Personale – Amministratori di Sistema
	Organizzazione interna - INSIEL

Tali minacce, nella presente analisi del rischio, sono tutte considerate come aventi alto impatto sull'asset primario oggetto della stessa, ovvero il documento informatico, e il Responsabile del Trattamento prevede quindi di adottare misure di sicurezza che vadano ad indirizzarne la totalità, nella consapevolezza che nessuna contromisura può annullare il rischio connesso ad una qualsiasi minaccia e che la sicurezza sia sempre da considerarsi come un processo continuo ed un percorso.

3. Identificazione delle contromisure

A livello generale, e nella consapevolezza che un qualsiasi rischio informatico connesso ad una specifica minaccia non potrà mai essere annullato, Insiel s.p.a. in qualità di Responsabile del Trattamento si è dotata di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI).
Scendendo a livello particolare, in considerazione delle minacce identificate al punto precedente, vengono esplicitate le seguenti misure di sicurezza. Tali contromisure sono esplicitate a livello di sintesi, richiamando il livello di dettaglio alla documentazione, ai sistemi tecnologici, alle procedure, nonché ad ogni altra evidenza riscontrabile e gestita da Insiel s.p.a. in qualità di Responsabile del trattamento.

Minaccia	**Asset impattati**	**Misure di sicurezza implementate**
Danneggiamento fisico	Sito di elaborazione dati – Data Center regionale	Controllo accessi fisici al data center regionale: sono implementate specifiche procedure per il controllo accessi, accompagnate da idoneo supporto tecnologico in relazione a: sistemi di controllo accessi/badge, servizio di guardiania, sistemi di videosorveglianza, monitoraggio e presidio 7x24.
	Sistemi di elaborazione dati – HW/SW	Controllo accessi fisici al data center regionale: sono implementate specifiche procedure per il controllo accessi, accompagnate da idoneo supporto tecnologico in relazione a: sistemi di controllo accessi/badge, servizio di guardiania, sistemi di videosorveglianza, monitoraggio e presidio 7x24.
Eventi naturali	Sito di elaborazione dati – Data Center regionale	Sistemi di protezione dei locali del data center regionale a fronte di allagamento, incendio

Perdita di servizi essenziali (alimentazione elettrica / connettività)	Sito di elaborazione dati – Data Center regionale	Ridondanza delle componenti di alimentazione nei singoli sistemi tecnologici, ridondanza dei sistemi tecnologici. Presenza di sistemi a garanzia della continuità elettrica, presenza di procedure di emergenza a supporto. Monitoraggio e presidio 7x24.
	Reti di comunicazione	Ridondanza interna delle componenti delle apparecchiature, ridondanza degli apparati e delle linee di comunicazione

Compromissione delle informazioni	Sistemi di elaborazione dati – HW/SW	I sistemi applicativi sono progettati per realizzare i requisiti funzionali richiesti dalla committenza e sono sottoposti a test funzionali specifici. Sono presenti sistemi di backup / restore volti a garantire il ripristino della disponibilità / integrità delle informazioni gestite, in base agli accordi vigenti.
	Dati / file	È presente un servizio di assistenza volto a supportare l'utente nella risoluzione di problematiche specifiche, anche connesse alla qualità del dato. Sono presenti sistemi di backup / restore volti a garantire il ripristino della disponibilità / integrità delle informazioni gestite, in base agli accordi vigenti.
Guasti tecnici	Reti di comunicazione	Ridondanza interna delle componenti delle apparecchiature, ridondanza degli apparati e delle linee di comunicazione Presenza di competenze interne specialistiche e contratti di manutenzione a copertura dei vari layer tecnologici.
	Sistemi di elaborazione dati – HW/SW	Ridondanza delle componenti di alimentazione nei singoli sistemi tecnologici, ridondanza dei sistemi tecnologici. Presenza di competenze interne specialistiche e contratti di manutenzione a copertura dei vari layer tecnologici.

Azioni non autorizzate	Personale – Amministratori di Sistema	Gli Amministratori di Sistema sono identificati e designati formalmente. Le attività ammesse sono definite da apposito regolamento reso disponibile a tutto il personale. È presente un sistema di controllo accessi fisici ai locali di INSIEL. È presente un sistema di controllo degli accessi logici ai sistemi ed alle reti accedute dal personale
	Organizzazione interna - INSIEL	Le responsabilità ed i compiti nell'ambito dell'azienda sono definite ed assegnate.
Attacchi informatici	Sistemi di elaborazione dati – HW/SW	Sono posti in essere sistemi di protezione antimalware, nei contesti previsti. Sono posti in essere apparati di sicurezza come dispositivi di firewalling, di *intrusion prevention* (IPS). Tutti i sistemi sono gestiti da personale specializzato.
	Reti di comunicazione	Le reti sono segmentate per ridurre il rischio di collegamenti non desiderati tra entità diverse. Sono posti in essere apparati di sicurezza come dispositivi di firewalling, di *intrusion prevention* (IPS)
	Dati / file	I contesti applicativi che danno accesso ad informazioni che presentano requisiti di riservatezza sono protetti da sistemi di autenticazione / autorizzazione
Errori	Personale – Amministratori di Sistema	Viene curata la formazione tecnica del personale addetto. Inoltre, nell'ambito del SGSI certificato secondo la norma ISO/IEC 27001, sono previste periodiche sessioni formative specifiche sulla sicurezza delle informazioni

	Organizzazione interna - INSIEL	Sono in atto specifici processi volti a gestire le diverse casistiche di *incident* in ottemperanza agli accordi contrattuali vigenti, nonché è incentivato il processo di miglioramento continuo anche in ossequio ai diversi *sistemi di gestione certificati* presenti in INSIEL. In caso di incidenti che implichino una violazione dei dati personali (*data breach*), INSIEL si è dotata di una specifica procedura di gestione degli stessi, che tiene conto anche dei tempi di segnalazione concordati con i Titolari.

Analisi dei rischi nell'ambito della gestione documentale e misure organizzative e tecniche adottate

Minaccia	Misura implementata	
Accesso non autorizzato ai documenti e ai dati in essi contenuti	Accesso al SdP da parte di personale non autorizzato	• L'accesso al SdP avviene, per le applicazioni di tipo web, per mezzo del trasferimento automatico delle credenziali utente acquisite al momento dell'autenticazione al dominio, mentre, per le applicazioni di tipo client / server, per mezzo di codice utente e password. • Il mancato accesso al SdP-per un periodo superiore ai sei mesi comporta la decadenza delle credenziali dell'utente interessato che deve richiederne la riattivazione. L'accesso al SdP è consentito solamente agli utenti esplicitamente autorizzati e la fruizione di funzioni ed informazioni è condizionata dal tipo di abilitazione attribuita ad ogni utente. • Le abilitazioni sono legate all'associazione ad una o più strutture pertanto le stesse vengono meno al momento della rimozione dell'associazione del dipendente dalle strutture stesse. • Sono impartite istruzioni specifiche al personale che utilizza l'SdP affinché non comunichi ad altri o dia evidenza delle credenziali di accesso al proprio computer e agli applicativi in uso.
	Accesso ai documenti contenenti dati personali da parte di personale non autorizzato	• Nel SdP sono presenti, per ogni utente, le informazioni che determinano la disponibilità delle funzioni applicative e la possibilità di accedere ai dati ed ai documenti archiviati nel sistema. • Alle registrazioni relative a documenti con particolari caratteristiche di riservatezza sono assegnati diversi livelli di riservatezza, da 1 a 9, in modo da permetterne l'accesso solamente agli utenti in possesso di un livello di abilitazione pari o superiore. • Sono impartite istruzioni specifiche al personale affinché la stampa di un documento contenente dati personali, in particolare su una

			stampante condivisa, venga ritirata tempestivamente. • Sono impartite istruzioni specifiche al personale affinché non lasci incustoditi i documenti contenenti dati personali. • Sono impartite istruzioni specifiche al personale affinché al termine del turno di lavoro conservi i documenti contenenti dati personali in archivi ad accesso controllato e quelli contenenti categorie particolari di dati personali di cui agli artt. 9 e 10 del GDPR in armadi muniti di serratura.
		Accesso ai locali fisici da parte di personale non autorizzato	• L'accesso fisico alle sedi del Consiglio regionale è controllato. • Le sedi del Consiglio regionale sono dotate di un sistema di telecamere che controlla il perimetro esterno e presentano un servizio di guardiania o di portierato. • Le stanze dell'Ufficio per la tenuta dell'Archivio e del Protocollo del Consiglio regionale, alla fine del turno di lavoro, vengono chiuse a chiave.
		Accesso alle postazioni di lavoro da parte di personale non autorizzato	• Sono impartite istruzioni specifiche al personale affinché non salvi documenti contenenti dati personali sulle risorse locali o li cancelli a fine turno di lavoro. • Sono impartite istruzioni specifiche al personale affinché non comunichi ad altri o dia evidenza delle credenziali di accesso al proprio computer e agli applicativi in uso. • Sono impartite istruzioni specifiche al personale affinché impedisca l'accesso al proprio computer in caso di assenza momentanea dalla propria postazione o al termine del turno di lavoro.

	Errato smistamento ad un ufficio del Consiglio regionale di documenti contenenti dati personali	- Sono impartite istruzioni specifiche al personale regionale addetto alla protocollazione affinché minimizzi la comunicazione di dati personali qualora non sia certo della struttura destinataria della comunicazione - Sono impartite istruzioni specifiche ai responsabili delle strutture affinché, in caso di errata ricezione di documenti contenenti dati personali, procedano alla restituzione nel più breve tempo possibile e senza conservarne copia.
	Errata assegnazione ad un funzionario del Consiglio regionale di documenti contenenti dati personali	Sono impartite istruzioni specifiche al personale regionale affinché, in caso di errata ricezione di documenti contenenti dati personali, proceda alla restituzione nel più breve tempo possibile e senza conservarne copia.
Alterazione o manomissione dei documenti o dei dati in essi contenuti	• Vengono memorizzate le attività di aggiornamento dei dati di protocollo con evidenza dell'utente che le ha effettuate. • Vengono memorizzati gli accessi e le operazioni effettuate dagli Amministratori di Sistema.	
Distruzione o perdita dei documenti o dei dati in essi contenuti	Sono presenti sistemi di backup e restore volti a garantire l'integrità e il ripristino della disponibilità dei documenti gestiti dal SdP.	
Trattamento illecito dei dati personali	- Sono impartite istruzioni specifiche al personale affinché l'accesso sia limitato ai dati strettamente necessari all'esercizio delle proprie mansioni. - Sono impartite istruzioni specifiche al personale regionale affinché raccolga e registri i dati personali solamente per scopi determinati, espliciti e legittimi.	
Trasmissione non autorizzata a soggetti terzi dei dati personali	• Sono impartite istruzioni specifiche al personale affinché comunichi, diffonda o trasferisca all'esterno i dati personali esclusivamente ai soggetti autorizzati a riceverli legittimamente. • Sono impartite istruzioni specifiche al personale affinché si astenga dal comunicare a terzi, al di fuori dell'ambito lavorativo, qualsivoglia dato personale • Sono impartite istruzioni specifiche al personale affinché fornisca dati e informazioni relativi a terzi solo dietro specifica autorizzazione del Titolare e non fornisca dati e informazioni ai diretti interessati, senza avere la certezza della loro identità. • Le informazioni relative a stati, fatti e qualità personali contenute nei documenti trasmessi all'interno del Consiglio regionale o a soggetti esterni sono limitate a quelle che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.	

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	L'inventario delle risorse hardware viene gestito da società in house Insiel con specifiche piattaforme di gestione asset e aggiornato a cura delle specifiche aree tecniche Insiel. Esportazioni periodicamente aggiornate sono condivise in apposito portale per la consultazione. E' altresì vigente un regolamento volto a vietare la connessione in rete di dispositivi personali.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Per quanto riguarda i sistemi client in gestione a Insiel l'inventario viene alimentato automaticamente attraverso lo strumento Microsoft System Center Configuration Manager (SCCM).
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Al momento tale misura non è applicata.
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Al momento tale misura non è applicata.
1	2	1	S	Implementare il "logging" delle operazionI del server DHCP.	Il logging delle operazioni del server DHCP è attivato.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Al momento tale misura non è applicata.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Il collegamento in rete dei dispositivi autorizzati comprende l'aggiornamento dell'inventario.

1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Tale contromisura è implementata a livello dei personal computer, attraverso lo strumento Microsoft SCCM.
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	È disponibile un sistema di registrazione, che raccoglie a livello degli apparati di rete i dispositivi connessi, in termini di indirizzi IP e indirizzo di rete fisica dell'hardware.
1	4	2	S	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.	Al momento tale misura non è applicata.
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	Al momento tale misura non è applicata.
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	Al momento tale misura non è applicata.
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Al momento tale misura non è applicata.

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

ABSC_ID	Livello	Descrizione	Modalità di implementazione

2	1	1	M	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.	Sono stati definiti elenchi di software autorizzato sulle postazioni di lavoro e sui server. E' altresì vigente un regolamento volto a vietare l'installazione di software non autorizzato sulle postazioni in dotazione. Ove possibile, tale requisito è garantito tecnicamente, mediante riduzione dei privilegi utente.
2	2	1	S	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.	Al momento tale misura non è applicata.
2	2	2	S	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).	Al momento tale misura non è applicata.
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Al momento tale misura non è applicata.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	La misura è attuata sulle postazioni di lavoro adottando lo strumento automatico Microsoft SCCM, che periodicamente produce l'elenco dei software rilevati, consentendo l'individuazione di eventuali software non autorizzati. Analogamente la misura è attuata con apposito sistema di rilevazione automatico sui server Languard.

2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	La misura è attuata sulle postazioni di lavoro adottando lo strumento automatico Microsoft SCCM, che mantiene l'elenco dei software rilevati. Analogamente sui server la misura è attuata con apposito sistema di rilevazione automatico Languard.
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	La misura è attuata sulle postazioni di lavoro adottando lo strumento automatico Microsoft SCCM, che mantiene l'elenco dei software rilevati.
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	Al momento tale misura non è applicata.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Le configurazioni standard di sicurezza dei sistemi operativi vengono realizzate dai gruppi tecnici Insiel e consolidate in immagini standard (template/cloni) utilizzate dal personale tecnico Insiel per le successive installazioni delle postazioni di lavoro e dei server. Le regole per l'utilizzo di strumentazioni informatiche regionali indica, per i dispositivi mobili, alcune limitazioni all'installazione di software e rende obbligatorie alcune configurazioni di sicurezza del dispositivo.

3	1	2	S	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.	Il livello di hardening di sicurezza viene definito dai gruppi tecnici Insiel anche sulla base dei vincoli di contesto; alcune misure di hardening sono demandate a componenti infrastrutturali e non vengono effettuate a livello di sistema (es. chiusura di porte di rete).
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	Attualmente tale misura è compresa nelle normali attività gestionali svolte da Insiel, limitatamente alle immagini di installazione con sistema operativo Windows. Inoltre è in progetto una attività di scansione periodica delle immagini di installazione volte a porre rimedio ad eventuali nuove vulnerabilità ed alla eventuale creazione di una versione aggiornata dell'immagine
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	L'installazione dei sistemi operativi sugli apparati viene effettuata utilizzando immagini standard ("template" per i sistemi server, "cloni" per i sistemi workstation e Laptop) Vengono definite le configurazioni standard per gli apparati di rete. .
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Il ripristino di eventuali apparati compromessi avviene imponendo nuovamente le configurazioni standard, ove possibile mediante la reinstallazione dell'apparato utilizzando immagine standard.

3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	Le modifiche delle configurazioni standard vengono definite e gestite da Insiel nell'ambito delle attività dei settori competenti secondo procedure standardizzate per la gestione del cambiamento.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini di installazione per dispositivi server (template) sono direttamente raggiungibili da personale tecnico Insiel in rete solo dai sistemi di virtualizzazione e vengono quotidianamente sottoposte a salvataggio. Le immagini di installazione per i dispositivi workstation e laptop (cloni) sono disponibili al personale tecnico Insiel sia ON-LINE sia OFF-LINE. Nel caso di corruzione dei file immagine, si procede con il loro ripristino dalle sorgenti fuori linea.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	La disponibilità delle immagini d'installazione è limitata agli amministratori di sistema Insiel, dedicati allo scopo.
3	4	1	M	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).	La connessione da e verso i sistemi indicati avviene attraverso protocolli dotati di meccanismi che garantiscono nativamente sicurezza o protezione della connessione stessa (ad es. protocolli RDP, SSH e https) o attraverso l'utilizzo di canali sicuri o reti interne. Situazioni particolari di apparati che non supportino le modalità di connessione sicure sono in corso di dismissione (es. apparati di rete).
3	5	1	S	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.	Al momento tale misura non è applicata.

3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	Al momento tale misura non è applicata.
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	Al momento tale misura non è applicata.
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Al momento tale misura non è applicata.
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Al momento tale misura non è applicata.
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Al momento tale misura non è applicata.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	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.	Visto che le modifiche significative nei sistemi in gestione da Insiel sono frequenti, si è valutato di avviare periodicamente delle ricerche di vulnerabilità. La periodicità viene concordata con il settore tecnico competente di Insiel. Sui server la ricerca delle vulnerabilità viene eseguita tramite apposito tool automatico di verifica gestito da Insiel. Nell'ambito dei sistemi distribuiti la ricerca delle vulnerabilità viene basata da un lato su una verifica degli aggiornamenti mancanti mediante il prodotto di gestione del client, dall'altro lato su una scansione a campione mediante tool automatico di verifica vulnerabilità.

4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	La ricerca delle vulnerabilità viene eseguita periodicamente mediante l'impiego di specifici tool. .
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	Al momento tale misura non è applicata.
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Al momento tale misura non è applicata.
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Al momento tale misura non è applicata.
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Al momento tale misura non è applicata.
4	3	1	S	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.	La misura è applicata nel contesto della ricerca di vulnerabilità sui sistemi client connessi alla rete.
4	3	2	S	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.	Tutti i sistemi dell'infrastruttura atta alla rilevazione delle vulnerabilità hanno indirizzi IP fissi. La ricerca delle vulnerabilità avviene solamente da questi indirizzi. Gli strumenti di ricerca sono utilizzati solamente da personale tecnico Insiel autorizzato e competente.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Tutti i sistemi dell'infrastruttura atta alla rilevazione delle vulnerabilità ricevono regolarmente gli aggiornamenti sulle vulnerabilità di sicurezza.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	E' in corso di valutazione da parte di Insiel l'abbonamento ad un servizio di alerting di terze parti ad integrazione dei canali già attivi previsti all'interno della rete dei CERT.

4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	L'attività di installazione delle patch avviene con strumenti automatici a seconda del contesto di riferimento. I sistemi server vengono aggiornati tramite il prodotto GFI Languard. I sistemi client vengono aggiornati tramite il prodotto SCCM.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non risultano presenti sistemi air-gapped separati dalla rete.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	Per le sole attività di ricerca delle vulnerabilità svolte da insiel sono seguite policy predefinite dalla Società.
4	7	1	M	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.	Il processo di gestione della vulnerabilità seguito da Insiel si articola in diverse fasi e prevede, coerentemente con il disposto delle presenti misure minime, quanto segue: - Identificazione di un criterio di classificazione delle vulnerabilità (ad esempio Low, Medium/Moderate, High/Important, Critical); - Definizione di un Risk Appetite standard (Medium/Moderate); - Indicazione di risoluzione di tutte le vulnerabilità aventi criticità superiore al Risk Appetite; - Qualora vincoli tecnico operativi impediscano il completamento della risoluzione delle vulnerabilità secondo il criterio stabilito, viene attivato un processo di escalation, che prevede l'accettazione del rischio residuo e può dar luogo ad ulteriori azioni correttive, eventualmente rivolte alla rimozione dei vincoli tecnici.

4	7	2	S	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.	Sono previste revisioni puntuali di specifici rischi connessi alle vulnerabilità, ad esempio in occasione della rimozione di obsolescenze tecnologiche o del rilascio di specifiche patch.
4	8	1	M	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.).	Il piano di gestione dei rischi definisce azioni recependo i risultati della ricerca delle vulnerabilità, assegnando dei tempi di risoluzione standard calcolati in base ai livelli di criticità delle vulnerabilità riscontrate. Specifiche vulnerabilità di notevole impatto possono venir trattate come emergency change.
4	8	2	M	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.	L'ordine di risoluzione delle vulnerabilità viene deciso in base alla loro gravità (Severity). Questa informazione viene riportata nei report degli strumenti automatici usati per la ricerca delle vulnerabilità. Il criterio di priorità per l'applicazione delle patch tiene conto della severity, come definito nel piano di gestione dei rischi.
4	9	1	S	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.	Nel caso di vulnerabilità di particolare gravità e impatto in cui non sono da subito disponibili le patch, se esistenti, vengono ricercate delle misure atte a minimizzarne l'impatto (workaround).
4	10	1	S	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.	Di norma gli aggiornamenti dei software specifici forniti da Insiel o sviluppate ad hoc vengono effettuati preliminarmente in ambienti diversi dalla produzione.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	L'assegnazione dei privilegi amministrativi in caso di necessità è riservata ai titolari in possesso di specifici requisiti e competenza tecnica, previo processo autorizzativo.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Le regole per l'utilizzo di strumentazioni informatiche regionali definiscono le modalità di utilizzo in ottemperanza al requisito indicato.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	L'assegnazione di privilegi amministrativi non standard è di norma evitata, ma possono esserci alcuni contesti in cui è prevista una profilazione puntuale dei privilegi delle utenze.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Al momento tale misura non è applicata.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Le utenze amministrative del personale tecnico Insiel sono gestite mediante una procedura standardizzata che prevede il tracciamento dell'iter di creazione delle credenziali amministrative di sistema. Le utenze amministrative del personale tecnico regionale, compreso Protezione Civile, sono espressamente autorizzate secondo le procedure autorizzative adottate. L'elenco delle utenze sono tenute dal servizio competente in materia di sistemi informativi.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Al momento tale misura non è applicata.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Le credenziali predefinite di amministrazione per i nuovi dispositivi sono sostituite da Insiel con credenziali coerenti alle utenze, in ottemperanza al regolamento adottato.

5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	L'aggiunta o la soppressione di un'utenza amministrativa di sistema viene tracciata nei log, nei sistemi che lo consentono.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Al momento tale misura non è applicata.
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Al momento tale misura non è applicata.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	I tentativi falliti di accesso con un'utenza amministrativa di sistema vengono di norma, ove possibile, tracciati nei log.
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	Al momento tale misura non è applicata.
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Tale requisito viene garantito dalle impostazioni del dominio e del sistema di accesso per gli apparati di rete adottato dal settore tecnico Insiel. È altresì disciplinato dalle regole per l'utilizzo di strumentazioni informatiche regionali.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Tale requisito viene tecnicamente garantito dalle impostazioni del dominio e del sistema di accesso per gli apparati di rete adottato dal settore tecnico Insiel. È altresì disciplinato dalle regole per l'utilizzo di strumentazioni informatiche regionali.

5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Tale requisito viene tecnicamente garantito dalle impostazioni del dominio e del sistema di accesso per gli apparati di rete adottato dal settore tecnico Insiel. È altresì disciplinato dalle regole per l'utilizzo di strumentazioni informatiche regionali.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Tale requisito viene tecnicamente garantito dalle impostazioni del dominio e del sistema di accesso per gli apparati di rete adottato dal settore tecnico Insiel. È altresì disciplinato dalle regole per l'utilizzo di strumentazioni informatiche regionali.

5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Al momento tale misura non è applicata.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Tale requisito viene tecnicamente garantito dalle impostazioni del dominio e del sistema di accesso per gli apparati di rete adottato dal settore tecnico Insiel. È altresì disciplinato dalle regole per l'utilizzo di strumentazioni informatiche regionali.
5	8	1	S	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.	Al momento tale misura non è applicata.
5	9	1	S	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.	Al momento tale misura non è applicata.

5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	L'utenza standard di dominio di cui i dipendenti dispongono per l'accesso non privilegiato non viene utilizzata per finalità amministrative. Ciò garantisce che tutti gli amministratori di sistema dispongano di un'utenza distinta per l'esecuzione delle attività privilegiate.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Tutte le utenze rilasciate sono nominative e personali.
5	10	3	M	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.	Per quanto riguarda i server le credenziali amministrative anonime sono note esclusivamente al personale tecnico Insiel che le ha memorizzate in un registro elettronico. Per accedere a questo registro gli operatori devono accedere con le proprie credenziali personali e specificare qual è il server di cui necessitano di conoscere le credenziali. Al termine dell'attività l'operatore è tenuto a cambiare sul server la password appena usata ed aggiornare la password sul registro. Il sistema traccia la richiesta.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Le regole per l'utilizzo di strumentazioni informatiche regionali disciplinano il divieto di impiego di utenze amministrative locali quando sono disponibili utenze amministrative di livello più elevato. Per gli apparati di rete, la gestione implementata da Insiel, prevede che le utenze locali non sono attive quando l'apparato è connesso in rete.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le regole per l'utilizzo di strumentazioni informatiche regionali specificano la necessità di conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.

5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non sono usati certificati per l'autenticazione. I certificati digitali qualora utilizzati sono protetti con tecniche di crittazione del File System.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	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.	L'installazione del sistema di protezione antimalware a livello di host (oggi Trend Micro OfficeScan) è obbligatoria su tutti i sistemi connessi in rete che lo supportano e viene effettuata propedeuticamente alla messa in rete da parte degli amministratori di sistema Insiel. Il sistema di protezione antimalware è mantenuto costantemente aggiornato mediante un'infrastruttura di supporto dedicata, gestita da amministratori di sistema Insiel.

8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Per tutti i server compresi nel perimetro del datacenter le funzionalità di firewall e IPS vengono gestite centralmente e si inseriscono in un contesto dove la segmentazione di rete è garantita sin dal livello progettuale. Per sistemi workstation e laptop tale misura viene applicata con l'installazione del sistema di protezione antimalware client utilizzato da Insiel (oggi Trend Micro OfficeScan). Su tutti questi dispositivi è attiva la funzionalità di "Suspicious Connection Detection", per il blocco del traffico verso sorgenti malevole ed il conseguente supporto alla prevenzione delle intrusioni. Per la funzionalità di firewall, su tutti i dispositivi workstation e laptop è installato il software disponibile nel sistema operativo Windows.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Il sistema di protezione antimalware raccoglie l'evidenza di tutte le rilevazioni su una console centralizzata gestita e monitorata da personale tecnico Insiel dedicato.
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Il sistema antimalware installato sui dispositivi è gestito e monitorato centralmente. Gli utenti non possono modificarne la configurazione se non espressamente abilitati.
8	2	2	S	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.	Il software di gestione del sistema antimalware permette l'aggiornamento manuale e il monitoraggio dello stato di aggiornamento di ciascun dispositivo.
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Al momento tale misura non è applicata.

8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Le regole per l'utilizzo di strumentazioni informatiche regionali disciplinano l'utilizzo dei supporti removibili. In particolare viene definita la natura di questi supporti, le modalità di custodia e le disposizioni da attuare per la dismissione di tali supporti. Al dipendente inoltre non è consentito collegare alla rete dispositivi non forniti dall'Amministrazione o memorizzare su di essi informazioni inerenti l'attività professionale.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Al momento tale misura non è applicata.
8	4	1	S	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.	Al momento tale misura non è applicata.
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Al momento tale misura non è applicata.
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Il servizio di connettività gestito da Insiel, prevede l'adozione di strumenti per il filtraggio del traffico di rete predisposti in vari punti dell'infrastruttura informatica. In particolare sono attivi i seguenti strumenti IPS anche con funzionalità antimalware su tutti i protocolli, gateway di navigazione Internet anche con funzionalità di protezione antimalware, gateway di posta elettronica anche con funzionalità di protezione antimalware.
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Al momento tale misura non è applicata.

8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Il monitoraggio, l'analisi e il blocco degli accessi ad indirizzi con cattiva reputazione viene effettuato da Insiel sia a livello di host sia a livello infrastrutturale. A livello di host è attuato attraverso la funzionalità di "web reputation" dal sistema antimalware installato su tutti gli host che ne supportano l'installazione mentre a livello infrastrutturale è presente tale funzionalità a livello di gateway di navigazione Internet.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Su tutti i dispositivi su cui è attivo il software antimalware è in esercizio la funzionalità che impedisce l'esecuzione automatica al momento della connessione di un dispositivo removibile. La disattivazione di tale funzionalità viene garantita anche tramite apposita configurazione a livello di dominio.

8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	La configurazione degli applicativi avviene sul clone standard e mediante l'applicazione di politiche a livello di dominio.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	La configurazione degli applicativi avviene sul clone standard e mediante l'applicazione di politiche a livello di dominio.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	La configurazione degli applicativi avviene sul clone standard e mediante l'applicazione di politiche a livello di dominio.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	A livello di sistema antimalware è attiva la funzionalità di scansione antimalware dei supporti rimuovibili al momento della loro connessione.
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Il servizio di gestione delle caselle di posta erogato da Insiel include una piattaforma perimetrale antimalware e anti-spam a protezione delle caselle di posta elettronica.

8	9	2	M	Filtrare il contenuto del traffico web.	Il servizio di connettività gestito da Insiel, comprende un sistema di protezione della navigazione Internet che prevede anche il filtro del traffico per categorie di contenuti.
8	9	3	M	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).	Il sistema di posta elettronica gestito da Insiel non consente l'invio di alcune tipologie di file ritenute pericolose ai fini della sicurezza. Il sistema di controllo del traffico web gestito da Insiel blocca i file anche in base alla tipologia del file.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Il sistema antimalware adottato da Insiel prevede oltre al riconoscimento tramite firme (pattern) anche l'utilizzo di tecnologie euristiche basate sull'analisi di comportamento.
8	11	1	S	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.	Nel processo di gestione del sistema di protezione gestito da Insiel è previsto l'invio al produttore del software antimalware di campioni di software "sospetto" per l'analisi e per l'eventuale creazione di firme personalizzate per il riconoscimento automatico di malware corrispondenti al campione inviato.

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Per tutti i sistemi server ed i sistemi di archiviazione gestiti da Insiel finalizzati all'immagazzinamento di documenti (file server, gestori documentali) è attiva una procedura di backup con periodicità almeno settimanale. E' presente un backup delle configurazioni degli apparati di rete, aggiornato a seguito di ogni modifica. E' altresì previsto nelle regole di utilizzo dei dispositivi informatici il salvataggio dei dati su servizi di memorizzazione di rete.
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	Tale misura è implementata da Insiel nel contesto del data center, ove vi siano sistemi virtuali per cui è attivo il salvataggio della "snapshot" del sistema virtuale.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Tale misura è implementata da Insiel nel contesto del data center, ove vi siano sistemi virtuali per cui è attivo sia il salvataggio della "snapshot" del sistema virtuale, sia il flusso di archiviazione verso il sistema di backup attraverso apposito software installato nel contesto del server virtuale.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Le attività di ripristino di file o sistemi viene eseguita regolarmente dagli amministratori di sistema Insiel preposti a fronte di richieste da parte di utenti. In contesti specifici sono svolte delle prove di riutilizzabilità delle copie mediante ripristini di prova.

10	3	1	M	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.	Le copie di backup sono gestite memorizzate di norma su supporti e sistemi custoditi fisicamente in locali, presso Insiel o presso i Ced regionali, ad accesso controllato.
10	4	1	M	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.	Le copie di backup sono memorizzate di norma su supporti o sistemi distinti logicamente o fisicamente e non direttamente accessibili al sistema stesso.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	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	I dati sono tutelati in conformità alla normativa in vigore. La valutazione delle informazioni con particolari requisiti di riservatezza è stata demandata agli utenti, in accordo con il Direttore di riferimento, come previsto nelle regole per l'utilizzo di strumentazioni informatiche regionali. Nel contesto dei servizi web la protezione crittografica del dato in transito avviene mediante l'uso del protocollo HTTPS. E' stato altresì commissionato uno studio volto a determinare le possibilità di crittografia del dato a riposo, nei vari contesti operativi.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	La crittografia dei dispositivi portatili è in corso di valutazione, da parte del supporto tecnico Insiel.

13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	Al momento tale misura non è applicata.
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	Al momento tale misura non è applicata.
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	Al momento tale misura non è applicata.
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	Al momento tale misura non è applicata.
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	Al momento tale misura non è applicata.
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Al momento tale misura non è applicata.
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Al momento tale misura non è applicata.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Il sistema gateway di navigazione web gestito da Insiel implementa la funzionalità richiesta, unitamente ad un blocco degli URL sulla base delle categorie.

13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	Al momento tale misura non è applicata.

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: STEFANO PATRIARCA
*CODICE FISCALE: **********
DATA FIRMA: 22/02/2023 14:24:49

NOME: PIERO MAURO ZANIN
*CODICE FISCALE: **********
DATA FIRMA: 28/02/2023 10:06:58