POL-SGI Sicurezza delle informazioni, cybersecurity e protezione della privacy del Settore Innovazione Digitale, dati, tecnologia e polo archivistico

Redatto	Verificato	Approvato
Data: 14/02/2025	Data: 19/02/2025	Data: 02/04/2025
Firma: Lorenzo Pugnaghi Alessandro Landi	Firma: Stefania Papili	Firma: Francesco Raphael Frieri
Classificazione del documento:	TLP:WHITE	

INDICE

1 Introduzione

1.1 Storia del documento

Data revisione	Versione	Descrizione Modifiche	Autore
19/05/2023	1.0	Prima emissione	Lorenzo Pugnaghi Alessandro Landi
09/10/2023	2.0	Seconda emissione – modifica approvatore	Lorenzo Pugnaghi Alessandro Landi
02/04/2025	3.0	Modifica a seguto del recepimento della determina Num. 13359 del 01/07/2024 e recepimento ISO/IEC 27001:2022 - Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni - Requisiti	Lorenzo Pugnaghi Alessandro Landi

1.2 Documenti allegati

Nome documento	Contenuti
POL_POL_01_PoliticaGenerale	Politica Generale della Sicurezza delle informazioni

1.3 Glossario

Termine/Acronimo	Descrizione

2 Scopo ed obiettivi

Il Settore Innovazione Digitale, dati, tecnologia e Polo archivistico (di seguito SID) considera le informazioni gestite elemento fondamentale, a diretto supporto della propria attività istituzionale.
In tal senso, la tutela delle informazioni riveste importanza strategica per il SID.
La protezione dell'informazione attraverso lo sviluppo di una robusta strategia di sicurezza delle informazioni, unitamente all'attuazione di controlli puntuali in tal senso, rappresenta una delle responsabilità primarie dell'Ente rispetto al contesto di riferimento e ai propri stakeholder.
Di conseguenza, la Giunta Regionale si impegna a garantire la sicurezza a tutto campo in tema di Information Technology con particolare riferimento a informazioni, risorse e processi direttamente o indirettamente collegati a questo dominio. Questo impegno coinvolge, a vari livelli, l'intero personale del SID, ciascuno nell'ambito della propria Area, del proprio ruolo e delle responsabilità che ad esso afferiscono.
Quale ulteriore garanzia, Il SID adotta un Sistema di Gestione Integrato (SGI) in linea con i requisiti della ISO27001:2022, ISO27017:2015, ISO27018:2019, ISO9001:2015 e ISO37001:2016.
Il presente documento integra la *Politica per la sicurezza delle informazioni della Regione Emilia-Romagna,* dettagliando requisiti e prescrizioni specifiche delle aree del SID quali "Infrastrutture e Sicurezza"," Servizi IT" e dell' "Area Sviluppo applicazioni, Polo Archivistico e gestione documentale" (limitatamente all'erogazione del servizio di conservazione) illustrando gli elementi cardine del SGI con lo scopo di:

- chiarire la necessità di definire, diffondere e applicare idonee politiche di sicurezza;
- descrivere gli obiettivi principali e il campo di applicazione del SGI stesso;
- indicare, in termini generali, responsabilità e ruoli in materia di sicurezza delle informazioni.

3 Campo di applicazione

La politica SGI in ambito Sicurezza si applica ai:

- Servizi infrastrutturali, di sicurezza e di gestione delle postazioni di lavoro erogati dal Settore Innovazione Digitale (SID) a favore delle Direzioni e Agenzie Regionali;
- Servizio di conservazione dei documenti informatici erogato dal Settore Innovazione Digitale (SID).

Le Aree del SID che rientrano nel perimetro del Sistema di Gestione Integrato ambito Sicurezza sono:

- **Area Infrastrutture e sicurezza**, in particolare, per quanto riguarda la gestione dei Sistemi, delle Reti, della Sicurezza e delle piattaforme applicative;
- **Area Servizi IT**, in particolare per quanto riguarda la gestione delle dotazioni individuali e la gestione degli utenti (accreditamento e autorizzazioni);
- **Area Sviluppo applicazioni, Polo Archivistico e gestione documentale**, con particolare riferimento allo sviluppo del Servizio di Conservazione e al processo di conservazione dei documenti informatici della Regione e degli enti convenzionati.

In particolare, la presente Politica afferisce:

- alle informazioni trattate nell'ambito delle attività in scope, qualsiasi natura e forma esse abbiano o prendano (es. testo, immagini, audio, video, formati multimediali),
- ai sistemi IT e supporti di memorizzazione utilizzati per il loro trattamento e conservazione (cartacei o digitali che siano)
- ai servizi erogati in qualsiasi modalità (ad esempio in cloud).

4 Obiettivi del SGI di SID

4.1 Premessa

Regione Emilia-Romagna ha introdotto nel proprio ordinamento il Piano Integrato di Attività e Organizzazione (di seguito PIAO) quale misura di semplificazione e ottimizzazione della programmazione pubblica nell'ambito del processo di rafforzamento della capacità amministrativa della PA.
Tale documento pone al centro della programmazione il concetto di Valore Pubblico, ossia l'impatto generato dalle politiche dell'Ente sul livello di benessere complessivo e multidimensionale di cittadini e imprese, ottenuto indirizzando gli indirizzi di performance da raggiungere in tale direzione, a partire dalla cura della salute organizzativa e delle risorse dell'Ente.

In questo complesso contesto evolutivo Regione Emilia-Romagna sta operando un percorso di cambiamento organizzativo e tecnologico con l'obiettivo di sostenere il processo di trasformazione digitale quale leva di sviluppo del territorio e della PA, creando ulteriore Valore Pubblico.

La trasformazione digitale si sta confermando sempre più come un driver fondamentale per aumentare la resilienza delle organizzazioni, a partire dalle PA che sono anche chiamate a trainare la ripartenza economica e sociale.

In questa direzione, e con l'obiettivo di definire uno strumento di attuazione di tale strategia per la propria organizzazione, Regione Emilia-Romagna ha adottato un framework metodologico come strumento di contestualizzazione della trasformazione digitale che permette di inquadrare iniziative e percorsi di transizione digitale in modo organico e flessibile.

Tale framework è composto da "dimensioni" che non possono essere considerate in maniera isolata ed è proprio nelle intersezioni tra di esse che si manifestano le filiere di contatto e i potenziali asset per sfruttare a pieno la trasformazione digitale.
Tali "dimensioni" , presenti in dettaglio all'interno del PIAO, hanno richiesto la determinazione di una serie di linee d'intervento per indirizzare la trasformazione digitale, sia all'interno di RER sia a livello territoriale.

RER ha individuato le seguenti linee di intervento:

- Datizzazione
- Processi digitali
- **Sicurezza**
- Dotazione smart e Spazi smart
- Architettura digitale
- Postura digitale

4.2 Obiettivi

La politica di cui al presente documento richiama quanto definito all'interno del PIAO riportando sinteticamente i principali obiettivi di trasformazione digitale in ambito Sicurezza che l'amministrazione regionale intende perseguire nella sua linea d'intervento:

- RER - Garantire la sicurezza informatica del sistema informativo attraverso un'evoluzione dei servizi di cybersecurity (risk management, cyber recovery, threat hunting);
- RER - Supportare le progettualità basate sull'utilizzo e l'integrazione di fonti dati diverse, interne ed esterne, mediante verifiche e soluzioni che garantiscano la conformità alla vigente disciplina in materia di trattamento dei dati;
- Territorio - Supportare le PA del territorio regionale nella prevenzione e risposta agli incidenti di sicurezza informatica attraverso un CSIRT (Computer Security Incident Response Team) regionale;

In relazione diretta con gli obiettivi del Sistema di Gestione Integrato, il SID adotta specifici criteri nella realizzazione e nel successivo sviluppo del proprio framework di sicurezza, proprio allo scopo di trasformarlo in un insieme di pratiche pienamente integrate con l'operatività quotidiana ed i processi di lavoro.
In particolare, il SID:

- adotta un criterio di pianificazione e controllo globale per garantire che siano stati correttamente identificati e inclusi nel piano tutti gli elementi interessati dal dominio della sicurezza;
- promuove al proprio interno una diffusa cultura della sicurezza;
- effettua periodicamente attività di analisi dei rischi sulla propria infrastruttura ICT e sugli aspetti di processo e organizzazione (ivi inclusi ruoli e responsabilità in tal senso) direttamente collegati all'utilizzo delle tecnologie a supporto del trattamento di informazioni, allo scopo di selezionare coerentemente le misure da rendere esecutive;
- è consapevole del valore strategico dei servizi erogati sul territorio regionale e ne tutela la continuità operativa e il relativo patrimonio informativo attraverso l'adozione di idonee

misure tecnico-organizzative e lo sviluppo di piani specifici;

- adotta standard internazionali di riferimento ove risulti utile/opportuno;
- comunica con le parti interessate (Enti, Cittadini, Imprese, ecc.) gli elementi fondamentali del proprio Sistema di Gestione Integrato in ottica di sicurezza delle informazioni, sia per necessità dettate dagli accordi contrattuali e di servizio, sia allo scopo di recepire dagli stessi suggerimenti utili al suo miglioramento.

5 Politiche SGI

Nel presente capitolo, si riportano le Politiche relative al SGI di SID, dettagliandone, per ciascun ambito, gli obiettivi che si intendono raggiungere, regole/requisiti applicabili al SGI e riferimenti ai Disciplinari regionali (che estendono i principi descritti).

5.1 Gestione dei Cambiamenti

L'obiettivo della seguente politica è quello di garantire che i cambiamenti che coinvolgono i servizi di SID siano opportunamente gestiti al fine di evitare impatti negativi sulla sicurezza delle informazioni.
Di seguito si elencano regole e principi applicabili:

- Valutazione dell'Impatto: Prima di implementare qualsiasi cambiamento, è necessario effettuare una valutazione dell'impatto che tale modifica potrebbe avere sulla sicurezza delle informazioni.
- Pianificazione: Il cambiamento deve essere opportunamente pianificato, includendo le azioni relative all'eventuale introduzione di ulteriori controlli di sicurezza.
- Autorizzazione: Ogni cambiamento significativo deve essere approvato da personale autorizzato, assicurando che siano state prese in considerazione tutte le misure di sicurezza necessarie.
- Comunicazione: Le modifiche devono essere comunicate alle parti interessate in modo tempestivo e chiaro, per garantire che siano consapevoli delle nuove disposizioni e delle responsabilità conseguenti.
- Implementazione: Il cambiamento deve essere implementato secondo il piano definito.
- Monitoraggio e Revisione: Dopo l'implementazione, il cambiamento deve essere monitorato per garantire che non siano state introdotte nuove vulnerabilità e per verificare l'efficacia del cambiamento.

5.2 Gestione degli Asset

L'obiettivo della seguente politica è assicurare che tutti gli asset associati ai servizi erogati dalle Aree SID siano stati opportunamente identificati e inventariati e che sia stato individuato un responsabile

al fine di gestire le minacce associate alla sicurezza delle informazioni.

Sono previste le seguenti regole/requisiti:

- Ai fini della selezione e attuazione di adeguati meccanismi di controllo, gli asset gestiti devono essere identificati e classificati (anche attraverso la compilazione di uno specifico catalogo costantemente aggiornato) e per ciascun asset deve essere individuato un responsabile (asset owner).
- ogni qualvolta si dismette un dispositivo elettronico o informatico che contiene dati personali/sensibili, è necessario adottare idonei accorgimenti e misure, anche attraverso soggetti terzi, tecnicamente qualificati, che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle;
- tutti i cambiamenti, che hanno un impatto sugli utenti dei servizi erogati dalle Aree SID, devono essere comunicati tramite opportuni canali.

Relativamente alla gestione degli Asset, SID fa riferimento alla politica interna di Settore "POL_AS_03_Monitoraggio_Asset", ed alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- *"Disciplinare tecnico per gli amministratori di sistema della Giunta e dell'Assemblea Legislativa" (Determinazione n. 83 del 07/01/2021), in particolare al Capitolo 8.*

5.3 Uso Accettabile degli Asset

L'obiettivo della seguente politica è:

- *indirizzare i comportamenti degli utenti relativamente agli asset utilizzati, allo scopo di prevenire l'accesso non autorizzato ai documenti;*
- *definire le politiche per la dismissione sicura degli asset.*

Tutto il personale deve:

- Essere a conoscenza del proprio ruolo e delle responsabilità nel contribuire ad un corretto e sicuro utilizzo delle risorse informative. In particolare, ognuno è responsabile della protezione e della conservazione dei beni regionali, materiali e immateriali, avuti in affidamento per l'espletamento dei propri compiti, nonché del loro utilizzo in modo proprio e conforme ai fini regionali;
- Proteggere i computer e le altre strumentazioni informatiche, in caso di assenza, anche temporanea, dalla postazione di lavoro, tramite la sospensione o il blocco della sessione di lavoro;
- Utilizzare sulle postazioni di lavoro esclusivamente il software autorizzato e fornito dall'Ente;
- Segnalare sempre, in ogni caso e preventivamente al proprio referente informatico o all'assistenza utenti dei Servizi regionali competenti in materia di informatica, la necessità di

installare eventuale software aggiuntivo rispetto all'installazione standard, anche se gratuito e necessario per lo svolgimento dell'attività lavorativa;

- Utilizzare stampanti in cui è attiva la funzionalità di stampa riservata e il rilascio della stampa è subordinata alla presenza dell'utente presso la stampante; ciò allo scopo di mantenere la riservatezza dei documenti stampati;
- Evitare di lasciare informazioni ritenute strategiche e/o sensibili (su supporto cartaceo e/o elettronico) dove possono essere lette, copiate e sottratte da personale non autorizzato e procedere allo smaltimento sicuro (es. distruzione) dei supporti cartacei contenenti tali informazioni quando essi non siano più necessari;
- Indirizzare i comportamenti degli utenti relativamente agli asset utilizzati, allo scopo di prevenire l'accesso non autorizzato ai documenti; distinguere precisamente le informazioni di proprietà dei fruitori del servizio (clienti), da quelle da esse derivate e/o comunque ricadenti nella sfera di appartenenza dei Servizi erogati dalle Aree SID.
- Definire le politiche per la dismissione sicura degli asset. Ogni qualvolta si dismette un dispositivo elettronico o informatico che contiene dati personali/sensibili, è necessario adottare idonei accorgimenti e misure, anche attraverso soggetti terzi, tecnicamente qualificati, che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

Relativamente all'uso accettabile degli asset, SID fa riferimento alla politica interna di Settore "POL_AS_03_Monitoraggio_Asset", ed alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- "Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna" (Determina n. 8901 del 6 giugno 2017), con particolare attenzione ai Capitoli 3 e 7;
- Linee Guida per la governance del sistema informatico regionale (Delibera n. 281 del 29/02/2016) e successivi aggiornamenti, in particolare al Capitolo 14.

5.4 Risorse Umane

L'obiettivo della seguente politica è garantire che il personale di SID (dipendenti e collaboratori) abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni.

Perciò SID applica nei confronti di tutte le persone coinvolte nei processi a sostegno dei servizi erogati (personale interno, fornitori e altre terze parti) gli indirizzi generali sulla sicurezza, affinché:

- *Comprendano l'importanza degli indirizzi generali, delle politiche e delle procedure adottate da SID per assicurare la sicurezza delle informazioni;*
- *Comprendano il loro ruolo all'interno del SID, con particolare riferimento alle problematiche della sicurezza;*

- *Siano informati sui comportamenti da tenere per assicurare gli opportuni livelli di sicurezza.*

Sono previste le seguenti regole/requisiti:

- Nella fase di selezione e per tutta la durata del rapporto di lavoro:
  - devono essere valutati i livelli di affidabilità, competenza e conoscenza degli obiettivi e delle problematiche di sicurezza dell'organizzazione in funzione delle attività che dovranno essere svolte;
  - devono essere chiaramente comunicati (e sottoscritti dal soggetto) gli eventuali obblighi di riservatezza per i quali viene richiesto l'impegno; va altresì specificato se tali obblighi permangono anche a valle della cessazione del rapporto di lavoro;
  - il personale deve ricevere un'adeguata e continuativa formazione inerente alle tematiche di sicurezza e privacy dei dati, con particolare riferimento a:
    - politiche e procedure in materia di sicurezza delle informazioni;
    - principali rischi che insistono su dati e informazioni;
    - misure disponibili per prevenire eventi dannosi;
    - obblighi legislativi, regolamentari e contrattuali in materia di informazione e trattamento e protezione dei dati (con particolare riferimento ai dati dei clienti);
  - le modalità di chiusura del rapporto di lavoro con SID devono assicurare la corretta rimozione dei dritti di accesso alle risorse informative nonché la restituzione di tutti i beni forniti in uso al personale.

Il SID fa riferimento alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale; tali norme coprono l'intero percorso che un dipendente regionale compie all'interno di SID, dal momento dell'assunzione fino alla risoluzione del rapporto di lavoro:

- *"Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna" (Determina n. 8901 del 6 giugno 2017);*
- *Linee Guida per la governance del sistema informatico regionale (Delibera n. 281 del 29/02/2016) e successivi aggiornamenti;*
- *LEGGE REGIONALE 26 novembre 2001, n. 43 TESTO UNICO IN MATERIA DI ORGANIZZAZIONE E DI RAPPORTI DI LAVORO NELLA REGIONE EMILIA-ROMAGNA* e successivi aggiornamenti.

5.5 Gestione terze parti

L'obiettivo della presente politica è assicurare la conformità ai requisiti legali e ai principi legati alla

sicurezza delle informazioni nei contratti con le terze parti, in accordo con le caratteristiche specifiche della relazione che SID deve instaurare con le terze parti stesse.

Gli accordi con le terze parti e con il gestore dell'infrastruttura che accedono alle informazioni e/o agli strumenti che le elaborano:

- devono essere basati su contratti formali contenenti opportuni requisiti di sicurezza. I requisiti di sicurezza devono risultare adeguati rispetto ai rischi, accidentali e/o intenzionali, di distruzione, perdita, divulgazione, alterazione e accesso non autorizzato delle risorse informative dell'organizzazione;
- devono garantire il rispetto dei requisiti di legge in materia di protezione dei dati personali e copyright delle risorse informative accedute e utilizzate.
- devono prevedere accordi per garantire la riservatezza e la non-divulgazione delle informazioni critiche dell'organizzazione. Tali accordi devono necessariamente contemplare tutti i requisiti dell'organizzazione definiti per assicurare la protezione delle risorse informative;
- devono includere, ove possibile, la possibilità di effettuare attività di audit di II parte sui fornitori per verificare il rispetto dei requisiti di sicurezza concordati.

SID fa riferimento alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- *Linee Guida per la governance del sistema informatico regionale (Delibera n. 281 del 29/02/2016) e successivi aggiornamenti, in particolare all'Allegato 5 e 8.*

5.6 Analisi dei rischi

L'obiettivo della presente politica è assicurare che i rischi associati al SID siano identificati, valutati e trattati

Sono previste le seguenti regole/requisiti in ambito risk assessment:

- Il sistema di controllo relativo ai servizi erogati dal SID, tra cui il servizio di conservazione, deve essere risk-based: l'analisi dei Rischio è l'elemento principale da cui discendono tutte le attività di controllo, le politiche in merito alla sicurezza e le procedure operative legate alla sicurezza delle informazioni.
- I necessari controlli per la mitigazione di potenziali rischi devono essere definiti a seguito di un'attività di risk assesment;
- l'attività di risk assesment va ripetuta con cadenza periodica e regolare, a garanzia del permanere dell'efficacia delle misure di mitigazione identificate e attuate (attività svolta con cadenza annuale).

5.7 Separazione dei ruoli e degli ambienti

L'obiettivo della presente politica è garantire i necessari livelli di sicurezza nell'esercizio del SID , attraverso l'attuazione dei principi di separazione dei ruoli.

Sono previste le seguenti regole/requisiti:

- I principi di separazione dei ruoli e privilegio minimo devono prevedere, almeno, la seguente separazione dei ruoli per incompatibilità:
  - Programmatori/DBA;
  - Programmatori/Amministratori di sistema;
  - Programmatori/Collaudatori;
  - Programmatori/Responsabile della sicurezza;
  - Amministratori di sistema/Responsabile della sicurezza;
  - Chi svolge un'operazione / Chi verifica l'operazione.
- Devono essere attuate opportune misure di sicurezza a garanzia di un'adeguata separazione degli ambienti di sviluppo, test e produzione.
- I sistemi, che costituiscono l'infrastruttura ICT del SID (che consente l'erogazione dei servizi), devono essere opportunamente protetti e segregati (tra loro e dagli ambienti/sistemi/funzionalità destinati alla gestione dei servizi), in modo da minimizzare la possibilità di accessi non autorizzati.

5.8 Controllo Accessi Logici

L'obiettivo della seguente politica è garantire l'accesso sicuro alle informazioni trattate e conservate, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti (interni o esterni) che non possiedono i necessari diritti.

Sono previste le seguenti regole/requisiti:

- Il ciclo di vita delle utenze deve essere regolamentato da un'opportuna procedura, dal momento dell'assegnazione, fino alla sua dismissione;
- Personale interno e consulenti – l'accesso alle informazioni da parte di ogni singolo utente (personale SID, nonché dipendenti di imprese esterne e/o consulenti cui l'accesso

è consentito per l'esecuzione degli specifici obblighi contrattuali) deve essere subordinato ad una procedura di autorizzazione da parte di SID e limitato alle sole informazioni di cui necessita in funzione del ruolo e delle mansioni assegnate (principio del minimo privilegio);

- le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo e agli incarichi ricoperti, nel rispetto dei principi di separazione dei ruoli e devono essere sottoposte a revisione periodica, con cadenza almeno annuale. Deve essere in ogni caso prevista la tempestiva modifica/disattivazione dei diritti d'accesso in caso di revisione/sospensione/revoca dei profili autorizzativi assegnati;
- è necessario definire un processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso. Specifiche procedure devono essere definite per l'assegnazione, la gestione e il controllo dei profili associati ad elevati privilegi (es. amministratori di sistema, "*superutenti*" in genere);
- devono essere definiti standard, procedure e istruzioni per la gestione delle password in conformità alle normative vigenti, con particolare riferimento a quelle in materia di protezione dei dati personali;
- devono essere monitorati e regolarmente verificati, nel rispetto dei limiti imposti dalla vigente normativa sulla protezione dei dati personali, gli accessi da parte degli utenti alla rete, ai servizi di rete, al sistema operativo alle applicazioni e alle informazioni dell'organizzazione;
- deve essere adottata particolare attenzione al tracciamento degli accessi legati alle utenze amministrative, al fine di garantire l'inalterabilità dei log e la loro conservazione secondo le tempistiche previste e per l'espletamento degli obblighi di verifica imposti dalla vigente normativa sulla protezione dei dati personali;
- ogni utente deve custodire le proprie credenziali di accesso ai sistemi, adottando le necessarie cautele per assicurare la segretezza della componente riservata e la diligente custodia dei dispositivi in proprio possesso ed uso esclusivo.
- ogni utente deve poter accedere solo all'insieme minimo di risorse necessarie allo svolgimento del proprio lavoro. In tal senso deve essere adottata particolare attenzione al tracciamento degli accessi legati alle utenze amministrative, al fine di garantire l'inalterabilità dei log e la loro conservazione secondo le tempistiche previste e per l'espletamento degli obblighi di verifica imposti dalla vigente normativa sulla protezione dei dati personali
- l'accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati deve essere subordinato al superamento di una procedura di identificazione e autenticazione.

La comunicazione e la trasmissione di informazioni all'interno, così come verso l'esterno, deve fondarsi sullo stesso principio;

Per ciò che attiene agli Accessi Logici, si fa riferimento alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- *Determinazione n° 4137 del 28/03/2014 "Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta e nell'Assemblea legislativa della Regione Emilia-Romagna";*
- *Determina n. 8901 del 06/06/2017 "Disciplinare tecnico per utenti dei servizi informativi della Regione Emilia-Romagna: si applica a tutti, dipendenti, fornitori, politici, consulenti, stagisti e tutti coloro che si collegano alla rete regionale e utilizzano i suoi servizi (Giunta, AL, Agenzie regionali)";*
- *Determinazione n° 19529 del 23/11/2018 "Disciplinare tecnico per le verifiche di sicurezza sul sistema informativo regionale, da applicare nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna";*
- *"Linee Guida per la governance del sistema informatico regionale" (Delibera n. 281 del 29/02/2016) e successivi aggiornamenti;*
- *"Disciplinare tecnico per gli amministratori di sistema della Giunta e dell'Assemblea Legislativa" (Determinazione n. n. 83 del 07/01/2021), in particolare al Capitolo 5;*
- *Determina n. 14128 del 30/07/2019 "Disciplinare per l'esercizio diritti dell'interessato sui propri dati personali (Giunta e Assemblea)";*
- *Determina n. 12807 del 03/08/2018 "Disciplinare tecnico per la gestione degli incidenti di sicurezza e data breach".*

5.9 Sicurezza fisica

L'obiettivo della seguente politica è quello di prevenire l'accesso non autorizzato alle sedi e ai locali dell'organizzazione e garantire adeguati livelli di sicurezza alle aree e agli asset mediante i quali vengono gestite le informazioni.

L'accesso e la permanenza all'interno delle sedi delle Aree SID sono consentiti esclusivamente alle persone autorizzate. Tali aree sono protette da opportuni sistemi di controllo e tracciamento degli accessi fisici.

Sono previste le seguenti regole/requisiti a garanzia del perimetro fisico delle Aree SID:

- delimitazione e opportuna protezione del perimetro fisico relativo ai sistemi;
- isolamento/separazione delle aree di carico e scarico;
- adeguati sistemi di controllo e tracciamento degli accessi fisici;
- definizione di una adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni;

- predisposizione di idonei impianti di sicurezza fisica e ambientale;
- predisposizione di un adeguato piano di manutenzione degli impianti di sicurezza fisica e ambientale.

In merito alla sicurezza fisica dei propri ambienti SID fa riferimento al *Disciplinare Tecnico relativo al controllo degli accessi ai locali della Giunta della Regione Emilia-Romagna (Determinazione n. 1894/2018).*

5.10 Capacity management

L'obiettivo della seguente politica è quello di garantire una gestione efficace che tenga conto dei necessari livelli di disponibilità e delle performance.

Sono previste le seguenti regole/requisiti:

- devono essere attuati i necessari controlli relativi a garanzia del monitoraggio del consumo delle risorse e delle previsioni di saturazione (es. elaborazione e analisi di statistiche periodiche), al fine di intervenire con tempismo e assicurare la necessaria disponibilità degli ambienti, in coerenza con le esigenze (anche prestazionali) dei servizi erogati.

5.11 Gestione malware

L'obiettivo della seguente politica è quello di garantire un adeguato livello di sicurezza della piattaforma tecnologica a supporto del servizio (lato client e lato server), considerando opportunamente tali aspetti nelle tematiche relative alla gestione del malware.

Sono previste le seguenti regole/requisiti:

- Devono essere definite opportune politiche di protezione delle postazioni di lavoro e dei server dalla contaminazione di malware, che prevedano:
  - identificazione delle postazioni e dei sistemi operativi target, in base alle esigenze operative e alla diffusione degli attacchi;
  - selezione di opportune tecnologie anti-malware;
  - definizione di modalità di installazione delle tecnologie anti-malware;
  - definizione delle modalità di aggiornamento e verifica della corretta; configurazione;
  - definizione di meccanismi di notifica early-warning.

Il personale SID segue le norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- *"Linee Guida per la governance del sistema informatico regionale" (Delibera n. 281 del 29/02/2016) e successivi aggiornamenti;*
- *"Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna"*

(Determina n. 8901 del 6 giugno 2017).

5.12 Monitoraggio e Gestione dei Log

L'obiettivo della seguente politica è quello di garantire i livelli di sicurezza necessari nella gestione e monitoraggio degli eventi e delle attività relative alla Sicurezza Informatica sul sistema di conservazione.

Sono previste le seguenti regole/requisiti:

- Devono essere loggati gli eventi e le attività ogniqualvolta questi coinvolgano il sistema di conservazione; inoltre deve essere possibile associare i log all'utente che ha effettuato le attività;
- Il contenuto dei log può variare a seconda dei sistemi considerati e in funzione delle limitazioni tecniche presenti;
- Devono essere soggette a log le seguenti attività che vanno monitorate con regolarità:
  - tentativi di accesso (falliti e riusciti) ai sistemi più critici;
  - utenti creati o disabilitati dai sistemi;
  - assegnazione e utilizzo di particolari privilegi a sistema;
  - utilizzo di utenze di amministratore;

- devono essere ben identificate le fonti dei log (componenti infrastrutturali, applicative e le attività da monitorare);
- I dati di log raccolti devono essere adeguatamente protetti da accessi non autorizzati e preservati nella loro integrità;
- I dati di log vanno conservati per il tempo minimo necessario a rispondere alla finalità per la quale sono stati raccolti e comunque nel rispetto di quanto previsto dalle politiche regionali;
- I dati di log vanno revisionati con cadenza periodica, allo scopo di identificare eventuali anomalie e porvi rimedio;

SID fa riferimento alla Politica interna di Settore "POL_01_CentralizzazioneLOG" dove si descrive come vengono gestite le varie tipologie di log, ed alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- *Disciplinare tecnico per gli amministratori di sistema della Giunta e dell'Assemblea Legislativa" (Determinazione n. 83 del 07/01/2021), in particolare al Capitolo 6;*
- *"Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna" (Determina n. 8901 del 6 giugno 2017), in particolare al Capitolo 13.*
- *"Linee Guida per la governance del sistema informatico regionale" (Delibera n. 281 del 29/02/2016) e successivi aggiornamenti.*

5.13 Compliance e Privacy

L'obiettivo della seguente politica è quello di garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni reputazionali.

Il modello del SGI, integrato nel Sistema di Gestione adottato dal SID, è sviluppato in coerenza con la legislazione applicabile nei territori e nei settori in cui il Settore opera, oltre che in aderenza agli obiettivi istituzionali della "Direzione Generale Risorse, Europa, innovazioni e istituzioni".
In questo senso, il SGI recepisce gli elementi derivati da tutte le normative applicabili all'ambito regionale e della Giunta Regionale e dell'Assemblea Legislativa della Regione Emilia-Romagna, ivi inclusa la normativa in materia di protezione dei dati personali (Regolamento UE 2016/679; D.Lgs. 196/2003 e s.m.i., con particolare riferimento al testo emendato dal D.Lgs. 101/2018).
Con specifico provvedimento (DGR. n. 1004/2022 per la Giunta, DUP n. 29/2012) sono state disciplinate le responsabilità relative agli obblighi e agli adempimenti in materia di protezione dei dati personali, ripartendo compiti e funzioni tra i soggetti competenti tenuto conto della specifica organizzazione dell'Amministrazione. Tale articolazione di competenze è applicabile, in quanto compatibile, anche per tutte le attività che non contemplano il trattamento di dati personali.

Il SID deve garantire il rispetto dei requisiti in merito a:

- Disposizioni di legge applicabili in merito alla protezione dei dati personali e relativi Provvedimenti del garante, in riferimento ai dati trattati sia in qualità di titolare del trattamento, sia in qualità di responsabile del trattamento nell'ambito dei servizi erogati;
- Norma ISO/IEC 27001:2013, ISO27017: 2015, ISO27018: 2019 e ISO9001:2015;
- Obblighi contrattuali legati ai servizi, con particolare riferimento agli obblighi in materia di protezione dei dati.

SID, per quanto riguarda gli Aspetti legali, fa riferimento:

- Alla Politica interna di Settore "POL_AL_01_Aspetti legali" che definisce le fonti per l'aggiornamento normativo.

5.14 Gestione degli incidenti

L'obiettivo della seguente politica è quello di garantire che gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza delle informazioni dell'organizzazione siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.

Sono previste le seguenti regole/requisiti:

- Tutti i dipendenti e i collaboratori sono tenuti a rilevare e notificare, a chi di competenza e

secondo adeguate procedure, eventuali eventi rilevanti per la sicurezza delle informazioni;

- Gli incidenti rilevati devono essere comunicati a tutti i soggetti coinvolti e, ove prescritto dalla legge o dalla normativa regolamentare, alle autorità e agli enti competenti, in coordinamento con la Regione e nel rispetto delle procedure da essa previste (es. notifiche di Data Breach);
- Gli eventi/incidenti che possano avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni, potenziali e non, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure condivise con tutti i soggetti interessati
- Deve esistere un sistema di registrazione e classificazione degli incidenti per effettuare analisi volte al miglioramento dei livelli di sicurezza delle informazioni coerentemente con le reali problematiche riscontrate;
- Gli audit log inerenti alle attività degli utenti, degli amministratori di sistema e degli operatori di sistema e gli eventi che possono compromettere la sicurezza delle risorse informative devono essere tracciati, registrati e conservati per un periodo di tempo ritenuto idoneo (anche in conformità alle normative vigenti) ai fini della ricostruzione degli incidenti, e a supporto di future attività di accertamento di comportamenti illeciti.

SID, per quanto riguarda gli incidenti, fa riferimento:

- *Al Disciplinare tecnico per la gestione degli incidenti di sicurezza e data breach (Determina n. 19293 del 04/11/2020);*
- *Al Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta e nell'Assemblea legislativa della Regione Emilia-Romagna, in particolare al Capitolo 14 (Determina n. 8901 del 06/06/2017).*
- *Alla politica interna di Settore "POL_IS_01_Gestione_Incidenti" che deriva dal Disciplinare tecnico per la gestione degli incidenti di sicurezza e data breach.*

5.15 Continuità operativa

L'obiettivo della seguente politica è quello di garantire la continuità operativa del SID e l'eventuale ripristino tempestivo dei servizi erogati nel momento in cui siano stati colpiti da eventi anomali di una certa gravità, riducendo le conseguenze di tali eventi sia all'interno che all'esterno del contesto dell'organizzazione.

Sono previste le seguenti regole/requisiti:

- Deve essere sviluppato un piano di continuità operativa che si basi su un'analisi dei rischi e un'analisi degli impatti che tenga conto delle reali necessità del servizio e delle aspettative dei fruitori dei servizi;
- Il piano deve essere opportunamente comunicato e aggiornato;

- Il piano deve essere periodicamente sottoposto a test di verifica;
- Devono essere correttamente mantenuti i rapporti con tutti i soggetti interessati in caso di disastro;
- Anche in situazione di crisi e disastro, devono essere mantenuti requisiti di sicurezza delle informazioni trattate.

SID, per quanto riguarda la Continuità Operativa, fa riferimento:

- Alla Politica di Settore "POL_BC_01_Business_ContinuityICT" che definisce la Gestione della Continuità operativa.

5.16 Sicurezza delle Comunicazioni

L'obiettivo della seguente politica è quello di garantire che siano opportunamente considerati gli aspetti di sicurezza nelle tematiche relative alla sicurezza delle comunicazioni (Network security: segregazione delle reti, monitoraggio dei gateway (firewall)).

Sono previste le seguenti regole/requisiti:

- tutti i flussi contenenti pacchetti informativi in entrata e in uscita nell'esercizio dei servizi di conservazione devono essere protetti mediante opportuni protocolli di crittografia (HTTPS e FTPS) o veicolati attraverso canali di posta certificata (PEC).
- ove possibile, i flussi di traffico originati dall'utenza del servizio (interna ed esterna) sono separati da quelli legati alle attività di amministrazione e gestione (i.e. reti differenziate).

Relativamente alla gestione delle reti, il SID fa riferimento alle *Linee guida per la governance del sistema informatico regionale (Delibera n. 281 del 29/02/2016)*.

5.17 Relazioni con autorità esterne e gruppi specialistici

L'obiettivo della seguente politica è quello di garantire che siano stati identificati i referenti per mantenere le necessarie relazioni con le autorità esterne.

Sono previste le seguenti regole/requisiti:

- Devono essere identificate e assegnate le responsabilità per i contatti e le comunicazioni relative a questioni inerenti la sicurezza delle informazioni del servizio di conservazione nei confronti delle diverse autorità.

In particolare:

  - Il responsabile SID è responsabile della comunicazione alle autorità/organismi esterni (Garante della Privacy, Polizia Postale, CSIRT, etc.) in caso di incidenti di sicurezza e Data Breach.

- Il Responsabile di SID è responsabile per le comunicazioni con la Magistratura.
- Il referente sicurezza ha la responsabilità di mantenere i contatti con l'Ente di Certificazione.

- Devono essere opportunamente individuati i flussi di comunicazione verso l'interno e verso l'esterno, rilevanti per la sicurezza delle informazioni.

In particolare:

- comunicazioni legate alle funzioni di vigilanza;
- comunicazioni legate ad eventi che hanno impatto sui requisiti di disponibilità, integrità e riservatezza.

5.18 Telelavoro e attività svolte al di fuori della sede

L'obiettivo della seguente politica è quello di garantire che, nel caso di Telelavoro, Smart-working Ordinario/Straordinario ed in generale di attività svolte al di fuori delle sedi del SID, siano rispettati gli stessi requisiti di sicurezza garantiti dall'utilizzo delle postazioni di lavoro interne alla sede di SID.

Sono previste le seguenti regole/requisiti:

- Regole e principi applicabili:
  - è necessario attenersi al "Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna", con particolare attenzione al Capitolo 8;
  - è necessario rispettare quanto indicato nella presente "Politica della Sicurezza delle informazioni", con particolare attenzione al Capitolo "Uso accettabile degli asset"
- Qualora si utilizzino PC personali per lo svolgimento delle attività lavorative, sono valide le seguenti raccomandazioni:
  - i dispositivi personali utilizzati devono essere periodicamente aggiornati, tramite l'installazione dei pacchetti software resi disponibili dai Vendor;
  - i dispositivi personali utilizzati devono essere provvisti di Antivirus/Antimalware;
  - i dispositivi personali devono essere protetti tramite una password a protezione del dispositivo ed un blocca schermo che si attiva dopo 15 minuti dall'abbandono della postazione;
  - la documentazione relativa alle attività lavorative non deve essere archiviata sul dispositivo, ma deve essere memorizzata in cloud, in linea con quanto previsto dalle policy regionali;
  - in caso di furto o smarrimento, è necessario provvedere tempestivamente alla segnalazione dell'evento, secondo quanto descritto nella procedura di gestione degli incidenti di sicurezza.
- Il SID sconsiglia e limita l'utilizzo dello smartphone personale per lo svolgimento di attività

lavorative e raccomanda quanto segue:

- un costante aggiornamento del sistema operativo e delle applicazioni utilizzate nel dispositivo personale;
- il download delle applicazioni utilizzate da piattaforme sicure/certificate (quali ad esempio: Play Store o App Store);
- l'utilizzo (se possibile) di applicazioni che impongano l'uso di un canale sicuro end-to-end durante l'invio di informazioni su qualsiasi rete;
- l'utilizzo di un sistema di criptaggio del dispositivo protetto tramite password di sicurezza;
- di evitare di memorizzare mai la password e lo username dell'account lavorativo all'interno del dispositivo;
- l'installazione sul dispositivo di un Antivirus/Antimalware;
- di evitare di archiviare la documentazione relativa all'attività lavorativa nello smartphone, privilegiando l'utilizzo del cloud;
- in caso di furto o smarrimento, di provvedere tempestivamente alla segnalazione dell'evento, secondo quanto descritto nella procedura di gestione degli incidenti di sicurezza.

Il SID fa riferimento a:

- "*Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna" (Determina n. 8901 del 6 giugno 2017)* applicato al telelavoro e alle attività svolte al di fuori delle proprie sedi, sia dal personale regionale, sia da quello esterno che svolge attività connesse al SID ed ai servizi erogati.
- Alla Politica interna di Settore "POL_AS_02_Dispositivi_Mobili" Utilizzo Dispositivi mobili forniti dall'Ente.
- Alla Politica interna di Settore "POL_AS_04_Linee guida sicurezza Mobile Working".

5.19 Backup

L'obiettivo della seguente politica è quello di considerare opportunamente, gli aspetti di sicurezza relativamente all'adozione di procedure di backup e ripristino dei dati.

Sono previste le seguenti regole/requisiti:

- Devono essere garantiti adeguate misure e strumenti di backup in funzione dell'importanza dei sistemi e dei dati in essi contenuti in modo da assicurare che i dati, le configurazioni e i software possano essere ripristinati successivamente ad un malfunzionamento o un crash di sistema;

- I supporti di backup devono essere conservati in una location differente rispetto a quella in cui sono conservati i dati originari, ad una sufficiente distanza dalla location originaria e deve essere garantito un adeguato livello di protezione fisica.
- Il processo di back up e restore dei dati deve essere periodicamente testato, e gli esisti delle verifiche opportunamente documentati;
- L'eventuale affidamento della conservazione di copie di backup dei dati a terze parti va regolato attraverso opportuni accordi contrattuali, nei quali siano indicate le misure di protezione e i criteri di trasferimento delle informazioni e/o tracciamento dei relativi supporti.

SID fa riferimento alla Politica interna di Settore "POL_BCK_01_Backup", ed alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- *"Linee Guida per la governance del sistema informatico regionale" (Delibera n. 281 del 29/02/2016) e successivi aggiornamenti, in particolare al Paragrafo 6.5.*

5.20 Sicurezza dello sviluppo applicativo[1]

L'obiettivo della seguente politica è quello di assicurare che gli aspetti di sicurezza siano inclusi nelle fasi di progettazione e sviluppo del software, anche in relazione all'architettura di erogazione del servizio stesso.

SID considera lo sviluppo del software per il servizio di conservazione elemento fondamentale per garantire l'erogazione dei propri Servizi; per questo ha deciso di mantenere lo sviluppo interno.

Sono previste le seguenti regole/requisiti:

- Nelle fasi di progettazione e sviluppo del software di conservazione devono essere opportunamente considerati gli aspetti di sicurezza. In particolare, devono essere indirizzate le seguenti tematiche:
    - inclusione dei requisiti di sicurezza nelle specifiche funzionali dei servizi e dei sistemi, anche in relazione alla modalità di erogazione dei servizi prevista (es. servizi cloud-based);
    - Adozione di best practice nel rispetto dei principi fondamentali di sviluppo sicuro quali:
        - Riduzione della superficie d'attacco;
        - Security by default;
        - Privilegio minimo (Least Privilege);
        - Defence In Depth;

[1] Politica applicabile per il servizio di conservazione dei documenti informatici

        - Separazione dei ruoli (SoD);
        - Semplicità dei meccanismi di sicurezza.
    - Separazione degli ambienti di sviluppo e di test, con impiego di procedure formali di controllo e accettazione nel passaggio fra ambienti
    - Gestione controllata della documentazione.
- ogni sviluppo a sistema deve essere adeguatamente autorizzato, testato e approvato prima del suo passaggio in Produzione. Durante le fasi di test è necessario verificare che siano rispettati anche i requisiti di sicurezza delle informazioni e dei principi suddetti;
- non si effettuano attività di cancellazione dei dati personali in ambiente di test in quanto le misure di sicurezza applicate al test sono analoghe all'ambiente di produzione;
- È necessario archiviare giornalmente nei sistemi preposti tutto il codice sviluppato relativo al Sistema di Conservazione.

Al fine di includere la sicurezza nel processo di sviluppo applicativo, SID fa riferimento:

- *Alle linee guida regionali per lo sviluppo sicuro, presenti nel Disciplinare Tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna (Determinazione n. 4137 del 28/03/2014);*
- *Alle linee guida per lo sviluppo sicuro specifiche per il servizio di conservazione, contenute nel documento Sicurezza sviluppo applicativo;*
- *Alle Linee guida per la governance del sistema informatico regionale (Delibera n. 281 del 29/02/2016), per quanto riguarda le verifiche relative ai requisiti di sicurezza dei sistemi e delle informazioni.*

5.21 Crittografia

L'obiettivo della seguente politica è quello di assicurare adeguato livello di protezione ai dati e alle informazioni gestite.

Sono previste le seguenti regole/requisiti:

- Le password gestite devono essere adeguatamente protette attraverso meccanismi di crittografia; particolari accorgimenti debbono essere adottati a protezione delle password degli amministratori di sistema;
- I flussi informativi in entrata e in uscita relativi ai servizi di conservazione devono essere protetti mediante idonei protocolli di crittografia (es. HTTPS e FTPS).

SID, per quanto riguarda la crittografia, fa riferimento:

- Alla Politica Interna di Settore "POL_CONF_01_Cifratura" che definisce i requisiti per la corretta cifratura dei dati.

5.22 Verifiche di Sicurezza

Il SID effettua i controlli ritenuti opportuni per la verifica della corretta applicazione, dell'efficacia e dell'efficienza delle misure di sicurezza adottate per la protezione delle informazioni, e dei dati personali in particolare.

Sono previste le seguenti regole/requisiti:

- Devono essere pianificate attività periodiche orientate alla verifica di conformità ed efficacia del sistema di gestione della sicurezza delle informazioni, in particolare rivolte a:
  - processi di pianificazione, attuazione, controllo e miglioramento del sistema;
  - attuazione e efficacia del sistema dei controlli organizzativi;
  - attuazione e efficacia del sistema dei controlli tecnologici, anche attraverso attività di vulnerability assessment e/o penetration test
- Tali attività sono effettuate esclusivamente da personale debitamente autorizzato; le relative evidenze raccolte sono conservate solo per il periodo necessario alla valutazione indicata e alla individuazione di possibili azioni migliorative.

Per quanto riguarda:

- *le verifiche relative ai requisiti di sicurezza dei sistemi e delle informazioni, il SID fa riferimento alle Linee guida per la governance del sistema informatico regionale (Delibera n. 281 del 29/02/2016);*
- *le verifiche annuali delle attività degli amministratori di sistema effettuate dalla Regione, il SID fa riferimento al "Disciplinare tecnico per gli amministratori di sistema della Giunta e dell'Assemblea Legislativa" (Determinazione n. 83 del 07/01/2021), in particolare al Capitolo 7;*
- *le verifiche di sicurezza effettuate dalla Regione, il SID fa riferimento al Disciplinare Tecnico per le Verifiche Di Sicurezza Sul Sistema Informativo Regionale (Determinazione n. 19529 del 23/11/2018).*

5.23 Gestione della Sicurezza dei Servizi Cloud

L'obiettivo della presente politica è assicurare la conformità ai requisiti legali e ai principi legati alla sicurezza delle informazioni nei Servizi erogati in modalità Cloud, in relazione alla tipologia dei Servizi fruiti (SaaS, PaaS, IaaS) e alla criticità delle informazioni trattate.

Per la gestione dei servizi cloud, SID recepisce quanto previsto dalla Regione Emilia-Romagna all'interno del Disciplinare per la sicurezza dell'ICT nelle forniture della Giunta e dell'Assemblea legislativa della Regione Emilia-Romagna e della POL_CLD_Politica per la fornitura dei servizi cloud.

Di seguito si elencano regole e principi applicabili, in relazione alle diverse fasi del ciclo di vita del Servizio Cloud:

- **Fase di valutazione preliminare del fornitore** – effettuare una valutazione dei rischi associati ai servizi cloud, al fine di verificare le misure adottate da fornitore per la mitigazione degli stessi,
- **Fase di formalizzazione del contratto** – i contratti relativi ai servizi cloud dettagliano le responsabilità e le misure di protezione dei dati relative al servizio.
- **Fase erogazione del Servizio**:
  - la configurazione dei servizi cloud è gestita in modo sicuro, adottando misure di controllo degli accessi e protezione delle informazioni.
  - effettuare una valutazione della prestazione, con frequenza e con uno strumento di verifica dipendente dalla tipologia e criticità della fornitura, e a quanto previsto contrattualmente (ad esempio: analisi della reportistica disponibile, audit documentale /sul campo).
- **Fase cessazione del Servizio** - i dati in esso contenuti sono cancellati in modo sicuro con l'obiettivo di garantirne la riservatezza degli stessi.

6 Ruoli e Responsabilità

Per attuare una politica di Sicurezza delle Informazioni efficiente ed efficace è necessario stabilire una struttura organizzativa che sia in grado di definire, implementare e controllare l'applicazione della Politica stessa attraverso:

- la definizione degli obiettivi e delle finalità delle politiche di sicurezza identificate;
- la realizzazione del Sistema di Gestione Integrato, assicurandosi che tutti gli aspetti rilevanti per la Sicurezza delle informazioni si realizzino in conformità alle necessità dei servizi erogati dalle Aree del SID a perimetro.
- la definizione di misure coerenti e adeguate al valore del patrimonio da proteggere e all'obiettivo del monitoraggio dell'efficacia del sistema per la sicurezza delle informazioni.

Per questo motivo, a supporto del Sistema di Gestione Integrato in ambito Sicurezza, il SID si è dotato di un'adeguata struttura organizzativa in grado di definire le procedure di Gestione della Sicurezza delle informazioni, di implementare tali procedure all'interno del sistema e di mantenere adeguate misure di protezione delle informazioni, nonché di adempiere a tutti i vincoli imposti dalle normative vigenti.

7 Disposizioni Finali

Per la concreta attuazione dei principi e delle finalità indicate nel presente documento, verranno adottati uno o più disciplinari tecnici, contenenti norme di dettaglio, da portare a conoscenza dei destinatari con le modalità di volta in volta più opportune.

8 Violazioni

Qualunque violazione a queste norme deve essere individuata e gestita. Il personale che contravviene alle politiche definite in questo documento potrà essere sanzionato secondo quando definito nel contratto di lavoro con il dipendente.

9 Ciclo di revisione

Il presente documento ha il compito di provvedere all'aggiornamento del medesimo ogni qualvolta vengano riviste le strategie dell'organizzazione e gli standard/normative di riferimento.

SID, per quanto riguarda gli Aspetti legali, fa riferimento:

- Alla Politica interna di Settore "POL_AL_01_Aspetti legali" che definisce le fonti di riferimento per l'aggiornamento normativo.

Il ciclo di aggiornamento viene incluso in un ciclo di Management review del SGI al quale il SID si riferisce. Il SID gestisce e assicura il Riesame periodico da parte della Direzione del SGI stesso, effettuandone una valutazione globale sullo stato e sull'efficacia.

Allegato 1 - Regole specifiche del Servizio di conservazione

Ambito	Regole/requisiti
Gestione Asset	• In considerazione delle caratteristiche e della missione del servizio di Conservazione erogato dal SID dell'Area Sviluppo applicazioni, Polo Archivistico e gestione documentale, si stabilisce che tutte le informazioni affidate a quest'ultimo dagli Enti conservatori, abbiano tutte lo stesso livello di criticità e, pertanto, siano soggette allo stesso grado di protezione.
Backup	• Le procedure di backup/ripristino dei dati devono tener conto delle peculiarità del servizio di conservazione (i dati in conservazione non devono essere più modificati), pertanto è da preferire la modalità incrementale di backup. Per gli altri dati, invece, è possibile fare riferimento alle politiche regionali. • Risultano applicate le politiche di backup presenti all'Allegato 2.

Crittografia	• Il processo di conservazione non prevede l'utilizzo della crittografia degli oggetti conservati, in quanto:
	  • Deve assicurare la conservazione a lungo termine del documento digitale e di conseguenza la piena disponibilità nei confronti non solo dell'ente produttore, ma di tutta la comunità di riferimento (previa verifica dell'autorizzazione all'accesso ai documenti);
	  • Non deve in alcun modo alterare il documento inviato in conservazione utilizzando tecniche crittografiche proprie.

Uso Accettabile degli asset	• Evitare di archiviare nel proprio computer i documenti informatici appartenenti al polo archivistico, se non per il tempo strettamente necessario per lo svolgimento di specifiche attività di testing; • Astenersi dall'utilizzo di dispositivi mobili e supporti rimovibili (CD, hard disk, ecc.) relativamente alle attività di versamento e distribuzione di documenti in conservazione.
Compliance	• Disposizioni di legge in merito alla tutela dei beni culturali; • Normativa sulla conservazione, come descritto nell'Allegato 1 "Normativa e standard di riferimento" del Manuale di Conservazione; • I requisiti richiesti da AgID per la qualificazione dei soggetti che svolgono attività di conservazione dei documenti ("Requisiti per l'erogazione del servizio di conservazione per conto delle pubbliche amministrazioni").
Controllo accessi logici	• Personale esterno (clienti) - l'accesso alle informazioni da parte degli Utenti degli Enti Produttori deve avvenire secondo precise regole (di accesso e visibilità delle informazioni) condivise da SID con gli Enti Produttori.
Gestione incidenti	• Gli eventi/incidenti che possano avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni, potenziali e non, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure condivise con tutti i soggetti interessati (a partire dagli Enti Produttori).
Sicurezza nelle	• Non è consentito utilizzare dispositivi mobili e supporti rimovibili (CD, hard

comunicazioni	disk, ecc.) per il trasferimento relativamente alle attività di versamento e distribuzione di documenti in conservazione.
Separazione dei ruoli e degli ambienti	• devono essere adottate logiche multi-ente per il Servizio di Conservazione, garantendo un'opportuna separazione e protezione per le singole aree dedicate agli Enti.
Relazioni con autorità esterne e gruppi specialistici	• Il responsabile dell'Area Sviluppo applicazioni, Polo Archivistico e gestione documentale è responsabile per le comunicazioni con AGID e con la Soprintendenza Archivistica.
Verifiche di sicurezza	• Le attività di vulnerability assessment sono svolte da soggetti certificati ISO17025.

Allegato 2 - Servizio di conservazione – Politiche di Backup

L'Area del SID "Area Sviluppo applicazioni, Polo Archivistico e gestione documentale" adotta politiche di Backup sui sistemi coerenti con le Regole regionali (Politiche e Disciplinari) e con quanto riportato al Paragrafo 5.18 e nell'Allegato 1 del presente documento.

Nello specifico, si riportano di seguito in estrema sintesi le politiche adottate per i componenti principali del Sistema di conservazione a supporto del relativo servizio: Sistemi Operativi, Database, Oggetti Memorizzati su Nastro.

Per il Servizio di Conservazione è stata dedicata nel sistema di RER un'infrastruttura specifica per il backup, che prevede le seguenti policy:

- Sistema operativo: il backup e ripristino del sistema operativo viene gestito tramite la schedulazione di IMAGE Backup del disco di sistema operativo. Tale backup è schedulato almeno ogni 2 settimane.
- Database: il backup del database avviene con l'agente per Oracle del TSM e la retention è di 30 gg:
  - il backup FULL è schedulato una volta alla settimana
  - gli archive log sono schedulati ogni 4 ore.
- Immagini DICOM: il backup è a livello file system gestito interamente come archiviazione dal modulo applicativo TPI sviluppato da Parer che si interfaccia direttamente con il TSM server. La retention è illimitata e la schedulazione avviene giornalmente.

Inoltre, è attiva una replica della copia primaria dei documenti archiviati in locale e su diversi Siti dell'Infrastruttura SID a supporto del Servizio di Conservazione.

La cancellazione delle copie di backup è tracciata a mezzo di un sistema di Trouble ticketing.