INFORMATION SECURITY POLICY DOCUMENT - POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

Gestione e supporto per la Sicurezza delle Informazioni, in conformità con i requisiti aziendali, le leggi e i regolamenti pertinenti.

REDAZIONE, VERIFICA, APPROVAZIONE

Azione	**Data**	**Nominativo**	**Funzione**
Redazione	09/03/2018	Filippo del Prete	*Comitato Scientifico*
Verifica	09/03/2018	Cinzia Amici	*Responsabile dei sistemi informativi per la conservazione*
Approvazione	03/09/2018	Serenella Carota	*Responsabile del servizio di conservazione*

STATO DELLE REVISIONI

N°Ver/Rev/Bozza	**Data emissione**	**Modifiche apportate**	**Osservazioni**
Vers. 1.0 / Rev. 01	03/09/2018	Emissione documento	
Vers. 1.0 / Rev. 02	02/12/2019	Aggiornamento	

Acronimi e definizioni

Acronimo	Descrizione
DigiP	Polo regionale di conservazione digitale denominato Marche DigiP
GDPR	General Data Protection Regulation
ISO	International Standard Organization
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
PASS	Trouble ticket system
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
SOA	Statement of Applicability

Diffusione & Riservatezza del documento

Il presente documento è considerato "Pubblico" in quanto contiene informazioni che possono essere comunicate liberamente senza che vi possano essere conseguenze negative per DigiP ad eccezione delle informazioni contenute nei capitoli da 6 a 12 che, proprio per la loro natura, non possono essere diffuse senza limitazioni o preclusioni. Il documento completo è pubblicato nell'apposito Sistema di Gestione Documentale ad accesso riservato all'indirizzo https://progetti.regione.marche.it

Sommario

1 DICHIARAZIONE DI PRINCIPIO

La Politica di Sicurezza delle Informazioni nel Polo regionale di conservazione digitale denominato Marche DigiP (DigiP d'ora in avanti) ha l'obiettivo di proteggere le risorse informative da tutte le minacce, siano esse organizzative o tecnologiche, interne o esterne, accidentali o intenzionali.

Il presente documento descrive la Governance adottata da DigiP al fine di garantire gli obiettivi relativi alla Sicurezza delle Informazioni, in conformità anche con i requisiti e le strategie aziendali. Il documento è dunque finalizzato a:

- garantire la riservatezza delle informazioni;
- mantenere l'integrità delle informazioni;
- assicurare la disponibilità dei servizi informatici;
- rispettare i requisiti normativi, legislativi e le regole interne;
- formare il personale alla sicurezza delle informazioni;
- tenere traccia e studiare qualsiasi incidente, reale o presunto, che interessi la sicurezza delle informazioni;
- stabilire regole, elaborare piani e adottare misure per attuare la migliore politica di sicurezza delle informazioni;

ed inoltre di:

- indicare il "Responsabile del servizio di conservazione" quale responsabile della attuazione della Politica di sicurezza delle informazioni;
- stabilire che i Dirigenti ed i Responsabili di Posizioni Organizzative (P.O.) sono responsabili nei rispettivi servizi e funzioni, della applicazione e del rispetto della Politica di sicurezza delle informazioni;
- assegnare ad ogni operatore di DigiP, dipendente e/o collaboratore, la responsabilità per il rispetto della politica di sicurezza delle informazioni.

2 ASPETTI GENERALI

La Politica di sicurezza delle informazioni di DigiP è attuata per proteggere, per quanto possibile e comunque ad un livello ottimale e ad un costo compatibile con le specificità delle attività connesse a DigiP, il Sistema di gestione delle informazioni da eventi intesi come minacce o incidenti, esterni e/o interni, oggettivi e/o soggettivi, che possono compromettere l'erogazione dei servizi.
Lo scopo di questo documento è indicare le esigenze, gli obiettivi, le finalità, ed i modelli organizzativi della strategia di sicurezza che DigiP intende perseguire, al fine di orientare lo sviluppo, la gestione, il controllo e la verifica dell'efficacia della sua attuazione.
Pertanto, la definizione di una Politica di Gestione della Sicurezza delle Informazioni è un punto strategico per supportare e garantire gli obiettivi che possono essere raggiunti.

2.1 Esigenza di una politica della sicurezza delle informazioni

DigiP, istituito con Deliberazione della Giunta Regionale n. 265 del 10 marzo 2014, ha come "mission" la fornitura di servizi tecnologici, organizzativi, giuridici ed archivistici per la gestione e la conservazione di archivi digitali della Amministrazione regionale marchigiana e degli enti locali del proprio territorio. Stante la sua missione, è fondamentale per DigiP fare continuo riferimento agli standard per la tutela del patrimonio informativo proteggendolo da accessi non autorizzati e manomissioni.
DigiP per supportare in modo efficiente e tempestivo il complesso delle azioni connesse alla sua missione, oltre ad avvalersi dei servizi informatici e di rete della Regione Marche, ha commissionato a terzi la progettazione, la realizzazione, lo sviluppo e il mantenimento tecnologico del proprio polo archivistico. La regione Marche ha acquisito con DDPF 128/INF del 18/09/2015 (contratto rep. n. 61337 del 01/12/2016), specifici servizi di gestione del Polo di conservazione Marche DigiP ed in particolare:

A – Servizi tecnologici, di un conservatore accreditato, a supporto del processo di conservazione

B1 - Servizi di presidio ed assistenza dal punto di vista archivistico ed informatico agli "enti produttori" (Unità di Gestione) ed al Comitato Regionale Utilizzatori

C.1 - Servizi di manutenzione evolutiva e adeguativa del software di conservazione DigiP

C.2 - Servizi di assistenza e manutenzione correttiva del software di conservazione DigiP

D - Produzione documentazione per l'accreditamento presso AgiD e l'audit del Comitato Scientifico regionale

DigiP svolge per conto degli enti convenzionati il servizio di conservazione dei documenti e degli archivi informatici, con la finalità principale di garantirne la validità giuridica, attivando i trattamenti previsti dalla normativa in vigore. Allo scopo di garantire tale servizio DigiP si avvale di un sistema applicativo e di un'apposita organizzazione con personale altamente qualificato e del supporto di esperti esterni di comprovata esperienza in materia, dotati di competenze specializzate.

2.2 Scopo

DigiP considera il sistema di gestione e le informazioni gestite, per il particolare rilievo che hanno assunto per il perseguimento dei propri fini istituzionali, parte integrante del proprio patrimonio. È obiettivo di assoluta priorità per DigiP, salvaguardare la sicurezza del proprio sistema informativo e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni prodotte, raccolte o comunque trattate, da ogni minaccia intenzionale o accidentale, interna o esterna.
DigiP si impegna a implementare la strategia per la Sicurezza delle Informazioni per tutte le risorse informative fisiche e logiche dell'azienda, al fine di garantire il rispetto dei requisiti normativi, operativi e contrattuali.
In particolare, gli obiettivi principali della Sicurezza delle Informazioni da affrontare sono:

- **Riservatezza:** la garanzia che una determinata informazione sia preservata da accessi impropri e sia utilizzata esclusivamente dai soggetti autorizzati (le informazioni devono essere accessibili solo a coloro che sono autorizzati ad accedervi).

- **Integrità:** la garanzia che ogni informazione sia realmente quella originariamente inserita nel sistema informatico e sia stata modificata in modo legittimo da soggetti autorizzati, salvaguardando l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione.

- **Disponibilità:** la garanzia di reperibilità dell'informazione in relazione alle esigenze di continuità di erogazione del servizio e di rispetto delle norme che ne impongono la conservazione sicura, assicurando che gli utenti autorizzati abbiano accesso alle informazioni quando necessario.

- **Autenticità:** la garanzia che l'informazione ricevuta corrisponda a quella generata dal soggetto o entità che l'ha trasmessa.

DigiP pone a base della politica di tutela delle informazioni, una idonea Analisi dei Rischi di tutte le risorse (asset) che costituiscono il sistema di gestione delle informazioni, al fine di comprendere le vulnerabilità, di valutare le possibili minacce e di predisporre le necessarie contromisure.
La consapevolezza che non è possibile ottenere, in ambito informatico come del resto in natura, una condizione di sicurezza assoluta, comporta che lo scopo della politica di sicurezza delle informazioni è quello di gestire il rischio ad un livello accettabile attraverso la progettazione, l'attuazione ed il mantenimento di un "Sistema di Gestione della Sicurezza delle Informazioni" (SGSI).

2.3 Campo di applicazione e destinatari

La politica di sicurezza delle informazioni è valida per l'intero DigiP, con riferimento principale alla funzione di Polo archivistico regionale.
La politica si applica a tutte le informazioni trattate nell'ambito sopra definito, qualsiasi natura e forma esse abbiano o prendano, e a tutti i sistemi di gestione e supporti di memorizzazione utilizzati per il loro

trattamento e conservazione.
I destinatari della politica sono tutti i collaboratori di DigiP dipendenti o consulenti, a tempo pieno e a tempo determinato. Sono tenuti al rispetto della politica tutti i soggetti che a vario titolo fruiscono dei servizi informativi di DigiP, nonché i visitatori e gli ospiti.
In particolare, sono tenuti al rispetto della politica di sicurezza, i fornitori di servizi informatici per la loro tipica condizione di operare direttamente sui sistemi di gestione delle informazioni.
A tal proposito, nei contratti con tutti fornitori di servizi vengono inserite apposite clausole di riservatezza e di sicurezza delle informazioni.

2.4 Obiettivi

Gli obiettivi generali della Sicurezza delle Informazioni includono quanto segue:

- Garantire la conformità con le attuali leggi nazionali, i regolamenti (ad esempio Regolamento generale sulla protezione dei dati UE 679/2016 - da ora GDPR) e le linee guida nonché le politiche interne di DigiP;
- Garantire al personale e a tutti i collaboratori la conoscenza delle norme sul trattamento dei dati personali menzionate al punto precedente e delle relative implicazioni, nonché delle modalità di applicazione delle misure previste;
- Garantire al personale e ai collaboratori una adeguata conoscenza e grado di consapevolezza dei problemi connessi con la sicurezza dell'informazione, al fine di acquisire sufficiente coscienza delle loro responsabilità in merito al suo trattamento;
- Garantire che tutto il personale e i collaboratori di DigiP abbiano consapevolezza delle regole tecniche ed organizzative nell'utilizzo dei sistemi informativi del Polo contenute nel "Manuale di conservazione" e nel "Piano della sicurezza";
- Garantire che tutto il personale e i collaboratori di DigiP siano consapevoli delle prescrizioni del SGSI nella gestione delle informazioni stesse;
- Accertare che tutti i fornitori esterni abbiano consapevolezza dei problemi di sicurezza delle informazioni di DigiP e rispettino la politica di sicurezza adottata dal Polo;
- Stabilire dei controlli per proteggere i sistemi informativi e le informazioni di DigiP da furti, abusi e altre forme di danno e perdita;
- Stabilire delle linee guida per l'applicazione di standard, procedure e sistemi per realizzare il Sistema di Gestione della Sicurezza dell'Informazione (SGSI);
- Motivare tutti i dipendenti a migliorare la loro consapevolezza della sicurezza al fine di proteggere e salvaguardare i dati di DigiP e dei suoi clienti;

- Assicurarsi che DigiP sia in grado di dare continuità ai propri servizi, anche se si verificano incidenti di sicurezza importanti;
- Garantire la disponibilità e l'affidabilità dell'infrastruttura di rete e dei servizi forniti e gestiti da DigiP;
- Rispettare le metodologie degli standard internazionali per la Sicurezza delle Informazioni, ad es. ISO/IEC 27001;
- Garantire flessibilità e un adeguato livello di sicurezza per l'accesso ai sistemi di informazione.

2.5 Strategia per la sicurezza delle informazioni

La visione della sicurezza di DigiP si basa sulla protezione delle risorse informative, sulla gestione dei rischi per la sicurezza, sull'attuazione delle strategie di business in modo efficace ed efficiente, supportata da una leadership operativa e sostenuta da tutti i dipendenti e collaboratori del Polo.

I principali driver coinvolti in una definizione del piano strategico di sicurezza sono:

- **Aspettative di sicurezza di DigiP:** l'aspettativa e l'ambizione del Polo che sono l'input principale per definire il piano di sicurezza e l'investimento in una visione a lungo termine;
- **Gestione del rischio:** i risultati dal punto di vista della gestione del rischio per quanto riguarda i principali rischi per la sicurezza di DigiP in termini di Sicurezza delle Informazioni;
- **Regolamentazione e conformità:** influenza esterna attraverso esigenze normative e di conformità;
- **Esigenze e aspettative delle altre parti interessate.**
- **Posizionamento rispetto alla sicurezza:** la posizione di sicurezza risultante da una valutazione tecnica (ad esempio un vulnerability assessment) interna/esterna e da valutazione (ossia l'assicurazione di gruppo) che può influenzare le priorità sulle attività aziendali;
- **Campagne di sensibilizzazione:** i risultati delle campagne di sensibilizzazione che sono un indicatore della prontezza dei dipendenti in materia di sicurezza.

Questi driver e i relativi obiettivi devono essere stabiliti e rivisti ogni anno, al fine di considerarli come la base per una strategia a livello organizzativo e per impostare un corretto livello corretto per la Sicurezza delle Informazioni.

Devono essere noti sia la natura sensibile delle informazioni che il Polo memorizza e processa che il grave danno potenziale che potrebbe essere causato da incidenti di sicurezza che interessano tali informazioni, così come la violazione dei dati personali.

Ciò significa che la questione della sicurezza sarà considerata un'alta priorità nel prendere qualsiasi decisione commerciale. Ciò consentirà a DigiP di allocare risorse umane, tecniche e finanziarie sufficienti alla gestione

della Sicurezza delle Informazioni e di intraprendere azioni appropriate in risposta a tutte le possibili violazioni alla Sicurezza.

Gli impegni e gli sforzi aziendali per la sicurezza saranno:

- **Coordinati:** saranno prese misure di sicurezza basate su un quadro comune e tutto il personale sarà coinvolto nel mantenimento della conformità con esso;
- **Proattivi:** le minacce e le lacune di sicurezza saranno rilevate, identificate e gestite al fine di prevenire incidenti di sicurezza;
- **Supportati al massimo livello:** la sicurezza delle informazioni sarà supportata pienamente dal management per implementare i controlli di sicurezza identificati attraverso un processo di valutazione del rischio continuo.

2.6 Revisione, controllo e gestione dei cambiamenti

Il "Responsabile del servizio di conservazione" è responsabile della revisione periodica della politica affinché sia allineata agli eventuali e significativi cambiamenti intervenuti nell'organizzazione e/o nelle tecnologie utilizzate per la protezione delle informazioni.
La revisione sarà fatta secondo necessità, in occasione di significative modifiche organizzative e/o tecnologiche rilevanti per la gestione delle informazioni.
Nel caso di cambiamenti significativi, questi vengono gestiti a livello progettuale, con dei progetti specifici, documentati a cura di un Responsabile definito, secondo l'ambito di competenza.

2.7 Livelli di servizio garantiti

I livelli minimi di servizio garantiti a livello di tempo massimo di ripristino (RTO), di tempo massimo di recupero dati (RPO) e di tempo massimo di messa a disposizione delle postazioni di lavoro in caso di non agibilità della sede DigiP, sono conformi alle specifiche elencate nel documento "Piano della Sicurezza", disponibile nel repository documentale accessibile al seguente URL: http://progetti.regione.marche.it.

2.8 Riferimenti normativi

DigiP è stato istituito con Deliberazione della Giunta Regionale n. 265 del 10 marzo 2014.
La materia della sicurezza delle informazioni è disciplinata dalla legislazione comunitaria e dalla legislazione italiana.
Le norme e i documenti più importanti sono:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le

imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis;

- Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Regolamento generale per la protezione dei dati personali n. 2016/679 (GDPR);
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- Deliberazione della Giunta Regionale n. 1039 del 30 luglio 2008 - Modalità Attuative del Programma Operativo (MAPO) della Regione Marche - POR-FESR - Competitività regionale e occupazione 2007-2013";
- Deliberazione del Consiglio Regionale n. 95 del 15 luglio del 2008 - Piano Telematico Regionale per lo sviluppo della banda larga ed il superamento del digital divide;
- Deliberazione della Giunta Regionale 1759 del 1° dicembre 2008 - Avvio della sperimentazione e dell'analisi finalizzata alla definizione del sistema di conservazione dei documenti cartacei e digitali della Regione Marche;
- Deliberazione della Giunta Regionale n. 252 del 23 febbraio 2009 - Programma Attuativo Regionale PAR FAS 2007-2013;
- Deliberazione della Giunta Regionale n. 1925 del 17 novembre 2009 - Partecipazione al

partenariato interregionale con le Regioni Liguria, Piemonte, Lombardia, Emilia-Romagna, Marche, Abruzzo, Campania, Puglia, Sicilia e la Provincia Autonoma di Trento ed il CISIS per la cooperazione nella realizzazione del progetto interregionale "PRODE-PROGETTO Dematerializzazione;

- Deliberazione della Giunta Regionale n. 167 del 14 febbraio 2010 - Definizione delle modalità operative di attuazione del polo di conservazione digitale della Regione Marche;
- Decreto della P.F. Sistemi informativi e telematici n. 213/INF_02 del 30 novembre 2010 - Procedura aperta per l'acquisizione di beni e servizi per la creazione e gestione del Polo regionale di conservazione degli archivi digitale;
- Decreto della P.F. Sistemi informativi e telematici n. 119/INF del 22 agosto 2012 – Aggiudicazione della procedura aperta e costruzione dell'infrastruttura organizzativa, tecnologica e giuridica per l'avvio dei servizi di archiviazione digitale a norma;
- Deliberazione della Giunta Regionale n. 265 del 10 marzo 2014 - Avvio dei servizi del Polo di conservazione digitale Marche DigiP.

2.9 Standard e norme di riferimento

Gli standard citati di seguito sono da intendersi nella loro ultima versione pubblicata e reperibile sul sito www.iso .org.

- Standard ISO/IEC 27000: Sistemi di gestione della sicurezza delle informazioni - Panoramica e vocabolario.
- Standard ISO/IEC 27001: Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni – Requisiti.
- Standard ISO/IEC 27002: Codice di condotta per i controlli di sicurezza delle informazioni.
- Standard ISO/IEC 27005: Tecnologia delle informazioni - Tecniche di sicurezza – Gestione del rischio per la sicurezza delle informazioni

3 PROCESSO DI GOVERNANCE DELLA SICUREZZA DELLE INFORMAZIONI

Il framework adottato in DigiP e descritto in questo capitolo è ispirato al modello descritto nello standard internazionale ISO/IEC 27001:2013 (da ora come generico ISO27001) "... per stabilire, implementare, operare, monitorare, revisionare, mantenere e migliorare un sistema di gestione della Sicurezza delle Informazioni (ISMS)".

Il modello descrive un approccio top-down che separa gli aspetti di governance (dichiarazioni, politiche e principi definiti dal Polo) dalla componente di management che riguarda il controllo dei rischi di sicurezza; il modello include un quadro di politiche e procedure che comprende tutti i controlli legali, fisici e tecnici coinvolti nei processi di gestione del rischio delle informazioni di un'azienda.

La struttura del processo adottata in DigiP segue l'approccio di stabilire, attuare, mantenere e migliorare continuamente un sistema di gestione della Sicurezza delle Informazioni per supportare la decisione strategica del Polo di preservare la riservatezza, l'integrità e la disponibilità delle informazioni in base alla struttura della norma ISO/IEC 27001.

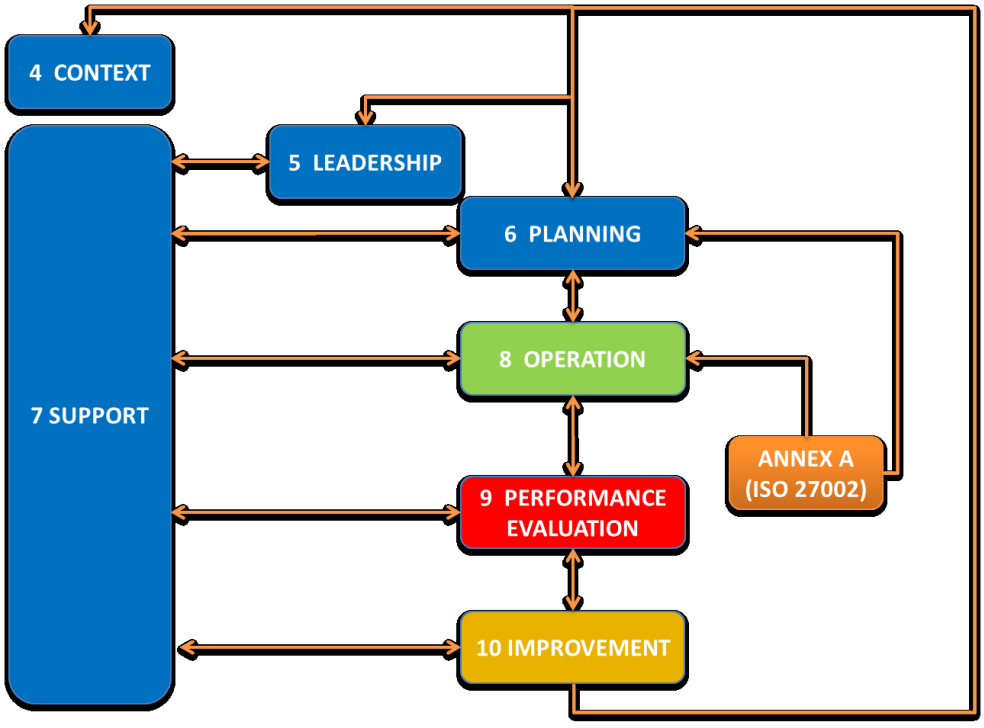

Figura 1 - capitoli della ISO/IEC 27001 e relazioni con SGSI (ISMS)

3.1 Contesto dell'organizzazione

3.1.1 Comprensione dell'organizzazione e del suo contesto

Con Delibera di Giunta n. 167 del 01/02/2010 la Regione Marche ha deliberato la costituzione del Polo regionale di conservazione digitale denominato Marche DigiP, inteso come struttura che fornisce una soluzione tecnologica, organizzativa, giuridica ed archivistica per la gestione e conservazione di archivi digitali dell'Amministrazione regionale e degli enti locali del proprio territorio. Il Polo, in qualità di conservatore accreditato, è progettato per gestire gli archivi digitali delle citate amministrazioni nonché, in prospettiva, gli archivi digitali di soggetti privati e di altri soggetti pubblici come le aziende sanitarie.

Il Polo Marche DigiP si avvale inoltre di un Comitato Scientifico formato da soggetti altamente qualificati che ha lo scopo di indirizzare e supervisionare le attività del Polo, in particolare:

- definisce gli indicatori e gli strumenti per assicurare la qualità dei servizi erogati;
- approva la documentazione elaborata dall'Unità di Progettazione, il piano di audit e monitoraggio;
- assicura il monitoraggio dell'evoluzione tecnologica, normativa e degli standard, fornendo all'Unità di Porgettazione il know how per l'aggiornamento del modello conservativo e tecnologico.

Ulteriori informazioni reperibili sul sito del Polo:

http://www.regione.marche.it/Regione-Utile/Agenda-Digitale/Polo-di-conservazione-regionale

3.1.2 Comprensione delle necessità e delle aspettative delle parti interessate

DigiP determina:

- Le parti interessate pertinenti alla governance della Sicurezza delle Informazioni;
- i requisiti di queste parti interessate rilevanti per la Sicurezza delle Informazioni.

Al fine di comprendere e comunicare le esigenze e le aspettative delle parti interessate, DigiP ha identificato i dipendenti in relazione agli accordi contrattuali, i fornitori e clienti; i contratti con i fornitori e i clienti prendono in considerazione gli accordi per la Sicurezza delle Informazioni. Pertanto, le parti esterne influenzate dai requisiti di legge e la conformità in materia di Sicurezza delle Informazioni sono gestite, tra l'altro e non solo, secondo le regole GDPR, ISO 27001 e le norme cogenti.

3.2 Leadership (Plan)

3.2.1 Leadership e impegno

Il Top Management di DigiP dimostra leadership e impegno nel rispetto della Sicurezza delle Informazioni attraverso:

- Le politiche per la Sicurezza delle Informazioni;
- La struttura organizzativa formalizzata, con compiti e responsabilità definiti per quanto riguarda la gestione della sicurezza;
- La comunicazione al personale relativa alla necessità di soddisfare gli obiettivi, le politiche, i requisiti normativi e regolamentari applicabili (leggi, regolamenti), lo stimolo al miglioramento continuo;
- La pianificazione e la fornitura di risorse (materiale umano in termini di quantità e competenza);
- La definizione e la formalizzazione del livello di rischio di accettazione;
- La valutazione delle prestazioni della sicurezza e l'efficacia della governance;
- Le attività di audit interno;
- L'implementazione di riesami periodici.

3.2.2 Politica

La politica generale per la Sicurezza delle Informazioni è riportata nel presente documento, che è dettagliato in altre politiche per aspetti più specifici; il presente documento include i requisiti ISO/IEC 27001:2013.

3.2.3 Ruoli organizzativi, responsabilità ed autorità

Come riportato negli standard di DigiP, le attività di Sicurezza delle Informazioni devono essere coordinate e gestite da vari ruoli funzionali aziendali.

Uno degli argomenti principali relativi alla Sicurezza delle Informazioni è rappresentato dai modelli organizzativi e di governance adottati dal Polo.

Le responsabilità, le autorità e i compiti relativi ai ruoli rilevanti per la Sicurezza delle Informazioni sono identificati all'interno della struttura aziendale. Questo modulo include la definizione dei ruoli in termini di unità organizzative e persone.

I ruoli, le responsabilità e le autorità formalizzate in questo documento ed in allegato sono rivisti almeno una volta l'anno, nell'ambito del riesame del sistema, o secondo necessità.

3.3 Pianificazione (Plan)

3.3.1 Azioni per indirizzare i rischi e le opportunità

DigiP definisce le sue priorità di governance della sicurezza attraverso un approccio di gestione del rischio (Risk Management): una visione di alto livello dell'approccio adottato è descritto nella sezione seguente. I dettagli sono riportati nel documento di Metodologia Risk Assessment e i risultati di ogni singola valutazione sono riportati nei documenti previsti dal processo.

3.3.1.1 Obiettivi

L'approccio di gestione del rischio è fondamentale per l'identificazione, la valutazione e la definizione delle priorità dei rischi. Gli obiettivi principali del metodo di Risk Management sono:

- Condurre un'appropriata analisi del rischio per valutare e identificare il livello di rischio delle attività del Polo;
- Assicurare che il rischio residuo delle soluzioni di Sicurezza delle Informazioni sia coerente con il livello di rischio definito dalla direzione;
- Ridurre la probabilità e/o l'impatto di eventuali minacce su servizi/asset.

3.3.1.2 Descrizione

Il Risk Management si basa su un framework che consente di identificare, valutare, notificare e monitorare il rischio delle informazioni in azienda attraverso l'attività di valutazione del rischio.

Le valutazioni del rischio devono identificare, quantificare e dare priorità ai rischi in base a criteri di accettabilità ben definiti e devono essere approvati dalla direzione di DigiP.

Se una valutazione del rischio rivela rischi inaccettabili, sono implementate misure appropriate per ridurre il rischio a un livello accettabile. Tale situazione deve essere segnalata dal responsabile della sicurezza alla Direzione.

3.3.2 Obiettivi della Sicurezza delle Informazioni e pianificazione per raggiungerli

In base ai risultati provenienti dalla governance e management della Sicurezza delle Informazioni, gli obiettivi specifici di Sicurezza delle Informazioni devono essere identificati e pianificati; il raggiungimento di questi obiettivi è monitorato periodicamente e rivisto durante il riesame della direzione.

Il piano può includere obiettivi e attività (iniziative di sicurezza) pianificate per raggiungerli. Devono essere indicate le attività, il proprietario e il manager, il risultato previsto, le risorse, i tempi e i metodi di misurazione

dei risultati.

Tra gli altri, il piano può prendere in considerazione iniziative di sicurezza per: formazione e sensibilizzazione, analisi delle vulnerabilità tecniche, miglioramento dei controlli e dei relativi processi, aggiornamento della documentazione e delle procedure. In ogni caso, la definizione di questi obiettivi deve essere allineata con gli obiettivi strategici del Polo.

Un'attenzione specifica deve essere applicata per la conformità al GDPR e alla famiglia delle norme ISO/IEC 2700x, attraverso l'approccio basato sul rischio che dimostra la responsabilità del titolare del trattamento dei dati nel supportare, in modo proattivo, la protezione dei dati personali.

3.3.3 Risorse

La disponibilità delle risorse è importante per garantire il raggiungimento degli obiettivi, pertanto è necessario che siano definiti piani opportuni per supportare la gestione della Sicurezza delle Informazioni. In particolare, DigiP considera:

- una pianificazione generale delle risorse;
- la coerenza tra pianificazione delle risorse in termini di quantità e piani di abilità/formazione;
- la tempestività nella disponibilità di risorse.

3.3.4 Competenze

Per gli aspetti di formazione e competenza si devono impostare le seguenti:

- Definire le competenze richieste per i ruoli relativi ai processi di Sicurezza delle Informazioni e agli aspetti di protezione dei dati;
- Definire ed erogare formazione al fine di garantire le competenze necessarie e in particolare a qualsiasi persona che agisca sotto l'autorità di DigiP (anche quando opera come titolare del trattamento dei dati), che ha accesso a dati personali;
- Verificare l'efficacia della formazione.

3.3.5 Consapevolezza

I principi, le politiche e gli aspetti generali dichiarati dalle politiche di Sicurezza delle Informazioni di DigiP devono essere comunicati e condivisi con tutto il personale, utilizzando gli strumenti istituzionali, in modo che essi siano consapevoli dell'importanza del loro contributo e delle implicazioni della mancata conformità ai requisiti di Sicurezza delle Informazioni.

3.3.6 Comunicazione

I documenti e le procedure relativi alla Sicurezza delle Informazioni, laddove appropriato, forniscono istruzioni e criteri per comunicare, sia all'interno che all'esterno di DigiP, i risultati di varie attività utilizzando la matrice RACI (Responsible, Accountable, Consulted, e Informed).

3.4 Operation (Do)

Le attività operative sono orientate all'attuazione, all'applicazione di controlli specifici per identificare i rischi e mitigarli secondo le procedure e gli obiettivi di sicurezza definiti dalla direzione.

Le attività sono definite in specifici obiettivi di controllo e relative politiche e procedure atte ad indicare come tali obiettivi possono essere soddisfatti; analogamente sono fornite indicazioni sugli strumenti adottati da DigiP.

Tali obiettivi sono strettamente allineati con lo standard internazionale ISO/IEC 27001: 2013 e in particolare con il Codice di Prassi ISO/IEC 27002:2013; lo standard è organizzato in 14 sezioni corrispondenti alle aree di controllo chiave del framework delle politiche. Il documento "SOA - Statement of applicability" (successivamente referenziato come SOA) riporta per ogni obiettivo di controllo definito nella ISO/IEC 27002:2013, la sua applicabilità per DigiP e le modalità con le quali tale obiettivo viene indirizzato (riferimenti ai processi, politiche e procedure). Eventuali obiettivi aggiuntivi che dovessero essere utili per il mantenimento della sicurezza delle informazioni saranno riportati nella SOA. Nello specifico, alcuni di essi rientrano anche nel raggiungimento della conformità GDPR: ad esempio il controllo degli accessi per gestire l'autorizzazione al trattamento dei dati personali, la gestione del rapporto con i fornitori per affrontare l'attribuzione delle responsabilità per i responsabili del trattamento e la gestione degli incident per identificare, registrare e gestire le violazioni dei dati personali. Un elenco completo dei documenti applicati agli obiettivi è comunque riportato anche nella SOA.

3.5 Valutazione delle performance (Check)

Il monitoraggio delle attività di governance è orientato a valutare e misurare le prestazioni rispetto alla politica, agli obiettivi e all'esperienza pratica. I risultati del monitoraggio sono uno degli input del riesame della direzione, nonché una dimostrazione di responsabilità nel fornire un'adeguata protezione delle informazioni e dei dati personali.

La principale fonte delle attività di monitoraggio è la misurazione dell'efficacia dei controlli di sicurezza, i report degli audit interni, gli incidenti di sicurezza (compresa la violazione dei dati personali), le valutazioni del rischio. A tal proposito devono essere definiti specifici indicatori di prestazione (KPI - Key Performance Indicator). La revisione degli indicatori KPI viene eseguita durante il riesame della direzione.

3.5.1 Monitoraggio, misura, analisi e valutazione

Deve essere implementato uno specifico processo per valutare le performance dei processi e identificare le opportunità per il miglioramento della Sicurezza delle Informazioni.

Il risultato delle attività di monitoraggio, in particolare quelle sugli indicatori, deve essere riportato ai Manager di competenza.

3.5.2 Audit interno

DigiP, su base regolare, esegue audit sul Sistema di Gestione della Sicurezza delle Informazioni (SGSI) per valutare l'effettiva attuazione e conformità. La pianificazione e la programmazione degli audit interni sono fornite su base annuale e riviste in base ai risultati di eventuali attività di monitoraggio. La frequenza degli audit interni è stabilita considerando il livello di rischio e le attività operative più critiche. A tale proposito, Digip ha formalizzato il processo attraverso la apposita procedura di gestione.

3.5.3 Riesame della Direzione

DigiP esegue un regolare Riesame della Direzione per garantire l'adeguatezza e la correttezza del sistema implementato. I risultati del riesame includono tra gli altri: revisione degli obiettivi di sicurezza, conferma del contenuto di questa politica di governance della Sicurezza delle Informazioni in base alla visione strategica aziendale.

3.6 Miglioramento (ACT)

3.6.1 Non conformità ed azioni correttive, miglioramento continuo

Secondo i principi definiti da DigiP in questa politica, l'attenzione al miglioramento è dimostrata dal riesame di tutte le attività di monitoraggio (misurazione e audit interno) durante il Riesame della Direzione e l'analisi dei risultati conseguiti; per risolvere formalmente qualsiasi non conformità devono essere implementate opportune azioni correttive.

Il Polo ha definito un processo per il miglioramento continuo a partire dai risultati del monitoraggio e delle misurazioni. Mediante l'uso di uno specifico strumento di Service Desk per registrare incidenti, le richieste di assistenza, le richieste di modifica (change) e problemi relativi al sistema di gestione, possono emergere statistiche e proposte per aumentare l'efficacia della gestione della sicurezza. Devono essere definiti gli obiettivi per migliorare la governance della sicurezza e le relative operazioni devono essere monitorate.

4 POLITICA DI PROTEZIONE DEI DATI PERSONALI A LIVELLO IT

La politica di protezione dei dati è un punto importante per le attività di trattamento dei dati personali direttamente correlata alla sicurezza delle informazioni; DigiP sta pianificando, identificando, implementando e gestendo attività specifiche al fine di dimostrare la sua responsabilizzazione ed il suo approccio.

Lo scopo di questa sezione della Politica sulla sicurezza delle informazioni e sulla protezione dei dati IT è di delineare gli standard di conformità, i processi, le organizzazioni e le misure di controllo per il Polo.

Questa politica è progettata per raggiungere i seguenti obiettivi:

- adottare un modello globale di protezione dei dati al fine di gestire correttamente i dati personali nel loro intero ciclo di vita;
- consentire a DigiP di far fronte alle responsabilità commerciali, legali e normative relative ai dati personali;
- aumentare la consapevolezza dei requisiti normativi, legali e aziendali per il trattamento e la protezione dei dati personali;
- stabilire una pratica aziendale chiara e completa per la gestione dei dati personali;
- stabilire la responsabilità per tutte le persone che gestiscono i dati personali;
- facilitare e consolidare pratiche comuni di gestione della privacy su base globale;
- mitigare i rischi (operativi, reputazionali e di conformità) relativi alla gestione e alla violazione dei dati personali;
- gestire correttamente la condivisione dei dati all'interno del Polo e l'accesso/trasferimento dei dati a terze parti.

Al fine di raggiungere gli obiettivi sopra definiti, DigiP adotta almeno i seguenti principi:

- trattare i dati personali in modo lecito, equo e trasparente (liceità, correttezza e trasparenza);
- trattare i dati personali in modo compatibile con finalità definite (limitazione delle finalità);
- elaborare i dati personali minimi necessari per scopi definiti (minimizzazione dei dati);
- elaborare dati personali aggiornati (esattezza);
- conservare i dati personali memorizzati per il tempo minimo necessario (limitazione della conservazione);
- elaborare i dati personali in modo tale da consentire al soggetto interessato di esercitare i propri diritti (efficacia);
- trattare i dati personali in modo tale da proteggere le informazioni (integrità e riservatezza);
- trattare i dati personali sotto la responsabilità e le disposizioni del titolare del trattamento dei dati (responsabilizzazione);
- consentire la rettifica o la cancellazione dei dati personali in risposta alla richiesta del soggetto a cui i dati fanno riferimento;
- considerare la privacy e la protezione dei dati dalla fase di progettazione (data protection by design) per la tecnologia, i sistemi e le attività operative al fine di garantire la privacy complessivamente;

- adottare un approccio basato sul rischio, considerando eventuali rischi per i diritti e le libertà dei soggetti a cui i dati fanno riferimento dovuti alle attività di trattamento dei dati svolte.

5 USO DEI SISTEMI DI ELABORAZIONE DELL'INFORMAZIONE

DigiP considera i sistemi di elaborazione delle informazioni come strumenti di lavoro ed il loro uso, da parte di coloro che vi operano a qualunque livello e a qualsiasi rapporto, è regolato dal "*Manuale della conservazione DigiP*", dal "*Manuale di utilizzo DigiP*" e dalle *"Procedure di esercizio"*, disponibili nel repository documentale accessibile al seguente URL: http://progetti.regione.marche.it.

Gli strumenti messi a disposizione devono essere utilizzati per lo svolgimento dell'attività lavorativa in modo strettamente pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi stessi e della rete e tenendo sempre presente l'interesse collettivo al risparmio delle risorse pubbliche.

DigiP perseguirà a norma di legge e del vigente contratto di lavoro, il collaboratore che utilizza in modo non appropriato i sistemi di elaborazione delle informazioni, poiché l'eventuale esposizione al rischio impedirebbe a DigiP lo svolgimento dei compiti istituzionali.

6 ORGANIZZAZIONE E RESPONSABILITÀ DELLA SICUREZZA [Contenuto ad accesso riservato]

7 TRATTAMENTO DEI DATI PERSONALI [Contenuto ad accesso riservato]

8 CONTINUITÀ OPERATIVA [Contenuto ad accesso riservato]

9 INVENTARIO DELLE RISORSE INFORMATICHE [Contenuto ad accesso riservato]

10 SICUREZZA FISICA E LOGICA [Contenuto ad accesso riservato]

11 SICUREZZA DELLE RETI E DELLE COMUNICAZIONI [Contenuto ad accesso riservato]

12 GESTIONE DEGLI INCIDENTI [Contenuto ad accesso riservato]