Phone +39(0)966 585637
info@portodigioiatauro.it
autoritaportuale@pec.portodigioiatauro.it

Autorità di Sistema Portuale
dei Mari Tirreno Meridionale
e Ionio

Contrada Lamia, snc
89013 Gioia Tauro (RC) - Italy
C.F. 91005020804

AUTORITA' DI SISTEMA PORTUALE
DEI MARI TIRRENO MERIDIONALE E IONIO

Piano della Sicurezza dei Documenti Informatici

Firmato digitalmente dal
Dirigente Area Pianificazione Sviluppo

Giovanni Piccolo
03.11.2023 13:25:47
GMT+01:00

Versione	1.0	Data versione:	Novembre 2023
Descrizione modifiche	Prima emissione		
Motivazioni	Adeguamento alle disposizioni legislative e regolamenti tecnici di riferimento		

Sommario

1. INTRODUZIONE AL DOCUMENTO

Il presente piano di sicurezza, adottato ai sensi delle Linee guida AgID sul documento informatico, descrive le politiche adottate dall'Autorità di Sistema Portuale dei Mari Tirreno Meridionale e Ionio in seguito denominata ADSP, descrive l'implementazione del Sistema di Gestione della Sicurezza Informatica (SGSI) dell'Ente esclusivamente per quanto attiene le attività di conservazione documentale ex DPCM 3 dicembre 2013 e, quindi, inerenti quanto definito nell'ambito del Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82 e successive modificazioni). Pertanto, ogni indicazione contenuta nel PdS è da intendersi riferita, ove altrimenti non indicato, esclusivamente alle predette attività di conservazione documentale.
Il PdS fa riferimento ad una serie di documenti e procedure che devono essere utilizzate all'interno della organizzazione stessa. Nel seguito, si fa riferimento agli aspetti della norma ISO/IEC 27001:2013, la cui certificazione è obbligatoria per l'accreditamento alla conservazione documentale e alle norme ISO/IEC 27002 e lo ETSI TS 101 533-01.Si considerano inoltre, a puro titolo di esempio, aspetti contemplati nella norma ISO 9001:2008, oltre che ad altre eventuali norme e/o dispositivi legislativi.

1.0 Scopo e campo di applicazione del documento

Il presente Piano per la Sicurezza del Sistema di Gestione Informatica dei documenti ai sensi della vigente normativa, riprende e integra le misure di sicurezza contenute nei documenti di politiche e piani della sicurezza delle informazioni previsti dai Fornitori di tecnologie coinvolti.
Il Piano garantisce che i dati siano disponibili, integri, riservati e che per i documenti informatici sia assicurata l'autenticità, l'integrità, la validità temporale.

Il patrimonio informativo gestito dell'Ente, regolato secondo i principi dell'organizzazione amministrativa in settori, servizi, e uffici (come da organigramma approvato), è custodito in modo da ridurre al minimo i rischi di perdita, anche accidentale, distruzione, accesso non autorizzato, trattamento non consentito o non conforme.

Le soluzioni di sicurezza adottate hanno l'obiettivo di:
- assicurare la protezione degli interessi dei soggetti pubblici e privati;
- evitare eventi di pericolo che possano compromettere l'accessibilità, la riservatezza e l'integrità dei dati dei sistemi informatici e tramite sistemi di comunicazioni adottati.

Il presente Piano di Sicurezza prende in considerazione i seguenti aspetti principali:
- la competenza dell'infrastruttura fisica e logica e le politiche di sicurezza adottate per l'erogazione del Sistema di Gestione Documentale;
- la competenza dell'Ente e le politiche generali e particolari di sicurezza adottate;
- il risultato dell'analisi dei rischi a cui sono esposti i dati (personali e non), e i documenti trattati, nei locali dove risiedono i sistemi fisici e logici e nei locali dove si usufruisce del servizio;
- le modalità di accesso e l'adeguata disponibilità del servizio di protocollo, di gestione documentale ed archivistico (anche definito "Sistema di Gestione Documentale");

- piani di formazione del personale riguardo la sicurezza;
- le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure
- di sicurezza applicate.

1.1 Modifiche al documento

Il presente documento è di proprietà dell'Ente, ADSP ed è compito del Responsabile per la Transizione al Digitale provvedere all'aggiornamento puntuale del medesimo ogni qualvolta vengano:

- riviste le strategie organizzative dell'Ente;
- introdotte modifiche applicative, funzionali e procedurali che hanno impatti architetturali, infrastrutturali e organizzativi sulla gestione sicura del servizio;
- riviste le politiche di sicurezza dei Fornitori interessati;
- adeguamenti a standard le normative di riferimento.

1.2 Livello di riservatezza

Livello	Ambito di diffusione consentito
○ **Pubblico**	Il documento può essere diffuso all'esterno dell'Ente.
✓ **Uso interno**	Il documento può essere diffuso solo all'interno dell'Ente. E' consentito darne comunicazione a terzi con clausola di non diffusione
○ **Riservato**	Il documento non può essere diffuso all'interno dell'Ente. La sua visibilità è limitata ad un gruppo ristretto di persone. L'indicazione "Riservato" DEVE essere riportata anche nel Piè-di-pagina del documento.

1.3 Precedenti emissioni

Prima emissione

Versione	1.0	Data versione:	Novembre 2023
Descrizione modifiche	Prima emissione		
Motivazioni	Adeguamento alle disposizioni legislative e regolamenti tecnici di riferimento		

1.4 Normativa e Standard di riferimento

Alla data di redazione, l'elenco dei principali riferimenti normativi, regolamenti, standard e linee guida in materia è costituito da:

CAD	Codice dell'Amministrazione Digitale, Decreto legislativo 7 marzo 2005, n. 82 e s.m.i.
Linee guida AGID Disaster Recovery	Linee Guida AgID per il Disaster Recovery delle pubbliche amministrazioni CAD
Linee guida per la sicurezza nel procurement ICT	Linee guida AgID aprile 2020: indicazioni tecnico-amministrative per garantire, all'interno delle procedure per l'approvvigionamento di beni e servizi informatici delle pubbliche amministrazioni, la rispondenza di questi ad adeguati livelli di sicurezza.
Linee guida AgID	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici AgID del 09 settembre 2020 (data di attuazione entro il 7 giugno 2021) – *con riferimento alle misure di sicurezza*
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.
Circolare AgID 18 aprile 2017, n. 2	Misure minime di sicurezza ICT per la PA
Reg. UE 679/2016 (GDPR)	Reg. UE 679/2016 (General Data Protection Regulation GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
Codice della Privacy	Codice per la protezione dei dati personali emanato con il Decreto legislativo 30 giugno 2003, n. 196 e s.m.i.
DPCM 13 novembre 2014	DPCM 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici (a partire dalla data di applicazione delle Linee Guida infra, sono abrogati) – *con riferimento alle misure di sicurezza.*
Garante privacy	Parere sullo schema di "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" – 13 febbraio 2020
D.Lgs 8 giugno 2001, n. 231	Decreto legislativo 8 giugno 2001, n. 231 e s.m.i. che disciplina la responsabilità amministrativa delle persone giuridiche e delle associazioni

Piano triennale per l'informatica nella PA	Piano Triennale 2020-2022, licenziato dal Ministro per l'innovazione tecnologica e la digitalizzazione e in corso di registrazione presso la Corte dei conti
ISO/IEC 27001	Standard internazionale che descrive le best practice per un sistema di gestione della sicurezza delle informazioni, anche detto SGSI
ISO/IEC 20000-1	Standard internazionale per la gestione dei servizi IT
ISO/IEC 22301	Standard internazionale relativa alla gestione della continuità operativa
ISO 9001	Standard internazionale che definisce i requisiti di un sistema di gestione per la qualità per un'organizzazione

1.5 Documenti di riferimento

Di seguito sono elencati i principali documenti ed i riferimenti tecnico-operativo collegati al presente Piano della Sicurezza dei Documenti Informatici.

AOO	(Area Organizzativa Omogenea) Struttura Organizzativa di riferimento
Nomine	Riferimenti a Ruoli e Responsabilità
SGCO	Sistema di Gestione Continuità Operativa
SIEM	Security Information and Event Management (Sistema di gestione delle informazioni e degli eventi di sicurezza)
SLA	Service Level Agreement - Livelli di Servizio garantiti
SGSI	Sistema di Gestione della Sicurezza delle Informazioni - Politiche di Sicurezza adottate dal fornitore Co.el.da
MANUALE	Manuale di Gestione documentale
MCF CLIENT	Manuale di configurazione della postazione di lavoro client

1.6 Terminologia

Ai fini dell'interpretazione del presente documento, sono di seguito indicati alcuni acronimi dei termini utilizzati.

Asset	Rappresentano qualunque cosa di valore che necessita di essere protetto o salvaguardato (in questo contesto: postazione di lavoro, altre dotazioni informatiche, server ed altri apparati, patrimonio informativo, etc.). Sono amministrati mediante un sistema gestione dei beni di proprietà dell'organizzazione
AdS	Amministratore di Sistema
AUDIT	Processo di valutazione e verifica (interna o di terze parti)
BC	Business Continuity
BCP	Business Continuity Plan?
CMDB	Gestione delle Configurazioni
DR	Disaster Recovery
DPO	Data Protection Officer
Sistema di Gestione Documentale	Inteso come categoria di piattaforme applicative utilizzate per organizzare e facilitare la creazione collaborativa di documenti elettronici e di altri contenuti digitali, di proprietà di Co.el.da
GEDOC	Un'applicazione di Gestione Documentale, di proprietà di Co.el.da
GDPR	General Data Protection Regulation
ICT	ICT Information and Communications Technology
Malware	Software dannoso utilizzato per compromettere sistemi informatici
RPO	Recovery Point Objective, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso (tolleranza ai guasti di un sistema)
RTO	Recovery Time Objective, si riferisce al tempo che intercorre tra il disastro e il completo ripristino dei sistemi
Patching	Programma strutturato che preveda l'applicazione sicura degli aggiornamenti di sicurezza
PdL	Postazioni di Lavoro (fisse e mobili)
PdS	Piano della Sicurezza
Spamming	Invio massiccio e indiscriminato di messaggi di posta elettronica, generalmente di tipo promozionale

1.7 Informazioni che rientrano nel concetto di dato personale

I dati sono classificabili in varie tipologie che, a seconda della loro delicatezza, devono essere trattati con cautele e regole diverse. Per trattamento s'intende "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*".

Dato Personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Dati relativi alla salute	Dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute
Dati Genetici	Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione
Dati Biometrici	Dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici
Categorie particolari di dati personali	Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
Dati personali relativi a condanne penali e reati	Dati personali che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato

2. ORGANIZZAZIONE DELLA SICUREZZA PER LA GESTIONE DOCUMENTALE

La sicurezza delle informazioni (intesa come il patrimonio informativo gestito) è ottenuta realizzando una serie idonea di controlli che comprendono politiche, procedure, istruzioni e raccomandazioni, strutture organizzative, strumenti e meccanismi tecnologici di tipo fisico e logico. I controlli rispondono ai requisiti di sicurezza che possono essere rilevati dall'analisi dei rischi oltre che da requisiti legislativi e regolamentari di riferimento.
Nelle sezioni successive si rappresenta, il Sistema di Governo della Sicurezza delle Informazioni, organizzato e documentato, mediante: i processi di gestione della sicurezza, i soggetti coinvolti ed ogni altra informazione utile alla gestione e alla verifica del funzionamento delle architetture e delle infrastrutture utilizzate.
Il sistema include aspetti che riguardano componente:

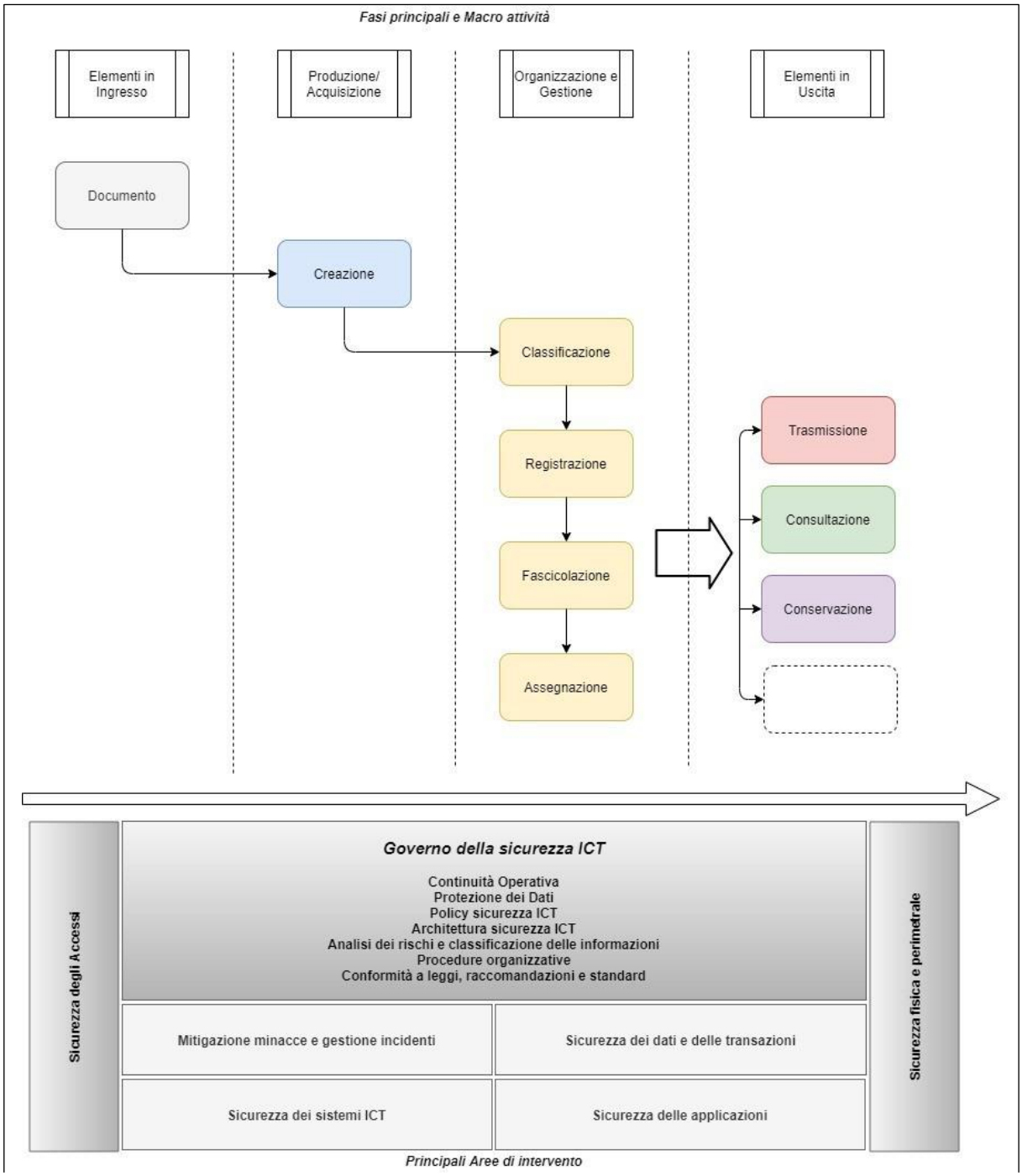
- Organizzativa
- Tecnologica, che a sua volta riguarda aspetti di sicurezza logica e sicurezza fisica.

2.1 Sistemi di Gestione Documentale

Le piattaforme applicative utilizzate per la gestione informatica dei documenti sono di proprietà di fornitori, ai quali l'ADSP si è rivolta, sviluppate internamente secondo gli standard qualitativi e di sicurezza, tra i quali quelli dettati dalle normative ISO 9001 e ISO/IEC 27001.
Sono piattaforme applicative, usufruibili da interfaccia web, che consentono l'automazione dell'intero ciclo di vita del documento sia in entrata che in uscita, a partire dall'assegnazione del numero di protocollo e delle informazioni identificative minime sino alla classificazione e all'assegnazione alle unità operative o ai soggetti responsabili e alla successiva fascicolazione e consultazione.
L'attività di acquisizione a protocollo dei documenti ne comporta l'immodificabilità, garantendo l'accesso esclusivamente ai soggetti in possesso di adeguate abilitazioni. Qualora richiesto, i documenti formati all'interno dell'Ente vengono firmati digitalmente (verificata la necessità di conversione in un formato standard, solitamente un PDF) prima della registrazione di protocollo. La firma digitale assicura l'inalterabilità del documento e ne attribuisce in modo certo la paternità e il non ripudio (salvo prova contraria).
Il sistema è progettato per fornire il servizio alle Aree Organizzative interessate, al fine di consentire una gestione efficace e razionale della struttura organizzativa di riferimento.
L'accesso alle funzionalità di sistema è determinato dal ruolo applicativo o dall'insieme di ruoli applicativi associati all'utente. I ruoli, a loro volta, si articolano in un insieme di permessi funzionali, che possono essere attivati o disattivati in funzione delle specifiche attività che dovranno essere eseguite dall'utente, cui il ruolo è assegnato.
È possibile modificare l'attivazione dei permessi in funzione delle attività che dovranno essere eseguite. Per soddisfare qualsiasi esigenza organizzativa, è possibile la creazione di nuovi ruoli per implementare nuove funzioni.

2.2 Aree di intervento della sicurezza

Di seguito è riportato il flusso rappresentativo delle macroattività del Sistema di Gestione Documentale, le aree di intervento della sicurezza condivise con i Fornitori dei Servizi e delle Infrastrutture su cui sono ospitati le piattaforme applicative di gestione documentale.



2.3 Analisi dei rischi operativi e di sicurezza inerenti il sistema di gestione documentale

L'Ente, con il contributo delle Società Co.el.da e Kibernetes (in qualità di Fornitori del Servizio di Gestione Documentale riguardante il protocollo e la creazione degli atti Amministrativi) in seguito chiamati anche "Fornitori", durante tutto il periodo di utilizzo è aderente a leggi, norme e regolamenti di riferimento; mette in atto misure tecniche ed organizzative idonee a garantire elevati livelli di qualità, sicurezza e protezione del patrimonio informativo gestito, di seguito elencate e successivamente descritte nelle sezioni del presente documento o con riferimento alla consultazione di specifiche Politiche di Sicurezza adottate internamente dall'Ente a dai Fornitori.

Il framework di riferimento per la gestione dei rischi operativi e di sicurezza, approvato e riesaminato almeno con cadenza annuale della dirigenza dell'Ente, d'intesa con i Fornitori di tecnologia (Co.el.da e Kibernetes) dell'ambito individuato, stabilisce e rende operativo:

- adeguata Struttura Organizzativa, Politiche di Sicurezza e di Gestione del Rischio;
- adeguata modalità di Acquisizione, Amministrazione e Configurazione sicura degli Asset;
- gestione degli Incidenti di sicurezza e di Violazione dei Dati Personali (Data breach);
- sistemi a Protezione di Malware/Virus periodicamente aggiornati;
- definizione e attuazione di meccanismi di backup/ripristino per garantire un'adeguata continuità operativa;
- adeguata protezione dei dati in termini di riservatezza, integrità e disponibilità;
- monitoraggio e Controllo delle attività;
- formazione e consapevolezza del personale;
- adeguata sicurezza delle postazioni di lavoro anche considerando modalità di lavoro flessibile o decentrato;
- politica di controllo degli accessi fisici e logici;
- gestione delle modifiche apportate alle risorse, agli apparati ed ai sistemi IT;
- gestione operativa di sviluppo software sicuro;
- gestione degli aggiornamenti e dell'obsolescenza tecnologica;
- sicurezza della rete e delle infrastrutture di comunicazione;
- cancellazione/eliminazione dei dati (quando necessario).

Nella tabella di seguito si riportano i principali eventi di rischio che potrebbero manifestarsi singolarmente oppure in forme sofisticate di minacce, applicabili al processo di formazione e gestione documentale, utilizzati come base per decidere azioni e contromisure tecniche ed organizzative.

Sono identificati gli eventi probabili (le minacce conosciute che possono sfruttare vulnerabilità) che nel verificarsi possono produrre effetti indesiderati rilevanti (in particolare: incidenti di sicurezza, violazione dei dati) e le eventuali principali azioni di mitigazione adottate.

Questa lista non costituisce un elenco esaustivo e fa riferimento agli argomenti trattati nelle prossime sezioni del presente documento e nei suoi riferimenti collegati.

Responsabilità	**Principali Categorie di Asset coinvolti**	**Principali eventi di rischio** [*Descrizione del rischio, inteso come esposizione alle minacce ricorrenti e più diffuse*]	**Probabilità di insorgenza** [*Analisi*]	**Impatto** [*Valutazione potenzialità danno*]	**Livello di Rischio**	**Azioni di trattamento** [*Principali strategie e contromisure messe in atto per ridurre il rischio, agendo su quei fattori che ne aumentano/diminuiscono la probabilità con cui la minaccia può manifestarsi sfruttando le vulnerabilità. Fare riferimento alle sezioni successive del presente documento ed ai riferimenti indicati*]
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Struttura Organizzativa	Accesso logico non autorizzato (es violazione dell'account con furto credenziali e Cracking delle password)	Moderata	Critico	Non accettabile	Dotazione di un sistema di controllo accessi centralizzato e policy password L'accesso degli utenti ai servizi erogati avviene in modalità autenticata. I diritti di accesso vengono riesaminati regolarmente e sono registrati gli eventi di accesso e le risorse. Sono presenti sistemi di filtraggio per bloccare l'accesso a risorse critiche.
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Infrastrutture e altre dotazioni informatiche	Accesso fisico non autorizzato	Improbabile	Critico	Non accettabile	Sono messe in atto procedure adeguate per garantire la sicurezza fisica necessaria per proteggere le aree, i sistemi e le persone che operano sui sistemi informativi (postazioni di lavoro e infrastrutture server) e le informazioni raccolte, trattate e conservate (aree presidiate, supervisione del lavoro, uso di dispositivi non autorizzati, formazione-informazione, regolamenti e buone pratiche)
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Applicazioni	Configurazione errata delle autorizzazioni	Improbabile	Alto	Non accettabile	Uso di strumenti di gestione della configurazione predefiniti, regolando automaticamente le impostazioni quando necessario

Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Struttura Organizzativa	Abuso di privilegi da parte di utenti	Rara	Critico	Non accettabile	È definito un processo che amministra l'assegnazione e la revoca dei diritti di accesso dell'utente, identificato con credenziali personali. La gestione dei profili consente di applicare il principio del minor privilegio. Tale principio richiede che gli utenti ricevano i privilegi minimi richiesti per svolgere il proprio lavoro, in modo che non ricevano tutti i privilegi di amministratore.
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Patrimonio Informativo	Copia o Trasferimento/Divulgazione di informazioni senza autorizzazione	Moderata	Alto	Accettabile	Misure implementate per assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.). Politica qualità, Codice condotta, piano di formazione e sensibilizzazione del personale e procedure di controllo logiche e fisiche. Il personale autorizzato e debitamente istruito sulle operazioni di diffusione di dati, da parte di soggetti pubblici, che è ammessa solo quando prevista da una norma di legge o, nei casi previsti dalla legge
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Patrimonio Informativo	Alterazione delle informazioni contenute nei documenti	Rara	Critico	Non accettabile	Apposizione della firma digitale ai documenti per garantirne l'autenticità e l'inalterabilità nel tempo. Sistema di validazione delle firme digitali.
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Patrimonio Informativo	Cancellazione o furto di informazioni (accidentale o intenzionale)	Rara	Critico	Non accettabile	Installazione sui dispositivi di antivirus con estensioni anti-malware, backup regolari, valutazione protezione, se necessario, mediante cifratura o altri meccanismi. Il personale autorizzato è debitamente istruito.
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Risorse Umane	Comportamenti sleali o fraudolenti del personale	Rara	Alto	Accettabile	È definito e diffuso un Codice di comportamento e di regolamentazione. Tracciabilità degli accessi alle risorse e audit log applicativi

Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Risorse Umane	Errori accidentali da parte di personale (varie tipologie di utenze) che possono comportare l'esposizione di dati personali	Moderata	Basso	Minimo	Pianificazione ed esecuzione di percorsi formativi in materia di protezione per il trattamento dei dati. Messa a punto di procedure/istruzioni che descrivono la gestione degli incidenti che possono comportare violazione di dati personali (data breach)
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Struttura Organizzativa	Non adeguamento a leggi, normative e standard di riferimento	Rara	Alto	Non accettabile	Piano operativo per la Qualità, e aggiornamento continuo su leggi e regolamenti di riferimento
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Struttura Organizzativa	Violazioni rispetto alla politiche di sicurezza dell'Ente	Moderata	Medio	Accettabile	Sono attivate procedure automatiche e manuali (audit e verifiche) per consentire un adeguato e costante utilizzo delle dotazioni informatiche strettamente legate alle finalità dell'Ente
Fornitori di Servizi/Applicazioni	Infrastrutture e Applicazioni	Inaffidabilità delle infrastrutture, Servizi e Applicazioni	Improbabile	Alto	Non accettabile	Il Fornitore predispone e attua piani di manutenzione e monitoraggio con misure necessarie a garantire la sicurezza informatica, fisica e logica. Si assicura la Business Continuity e Disaster Recovery per garantire sicurezza, ridondanza ed efficienza. Lo sviluppo e il test del sw vengono eseguiti in ambienti protetti e applicando le migliori pratiche di sviluppo sicuro e attività di VA e PT (Vulenrability Assessment e Penetration Testing)
Fornitori di Servizi/Applicazioni	Infrastrutture e Applicazioni	Servizi Informatici non disponibili e/o con prestazioni gravemente degradate	Improbabile	Medio	Minimo	Sono definite le principali procedure e meccanismi di controllo (anche con firewall) per garantire il necessario livello di continuità e disponibilità del Servizio, tenendo sempre presente le possibili esposizioni ad attacchi tipo DoS (Denial of Service), volumi di traffico e corretto dimensionamento delle risorse.

Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Struttura Organizzativa	Carenza - Violazione o inosservanza di obblighi di Responsabilità delle terze parti coinvolte	Rara	Alto	Non accettabile	Affidamento a fornitori di infrastrutture e servizi riconosciuti e qualificati. Formalizzato accordo al trattamento dei dati con i responsabili del trattamento prima di iniziare attività di trattamento
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Applicazioni	Introduzione di codice malevole	Moderata	Alto	Non accettabile	I Sistemi sono protetti con rischio di intrusione e malware mediante attivazione di idonei strumenti aggiornati tempestivamente. Sono attivati percorsi di sensibilizzazione periodica degli utenti in base al ruolo
Fornitori di Servizi/Applicazioni	Infrastrutture e Applicazioni	Monitoraggio non adeguato del Servizio	Rara	Medio	Minimo	SLA contrattualizzati e disponibilità Audit presso fornitore del Servizio. Codice di Condotta del Fornitore e aderenza agli standard di riferimento, verifica periodica del corretto dimensionamento del sistema in termini di risorse utilizzate BCP, la disponibilità di un piano di dismissione, la capacità di monitorare adeguatamente le risorse esternalizzate
Fornitori di Servizi/Applicazioni	Infrastrutture e Applicazioni	Obsolescenza tecnologica	Improbabile	Alto	Minimo	Conduzione, Manutenzione ed Evoluzione del Sistema di Gestione Documentale da parte del Fornitore. Sistematico adeguamento all'innovazione tecnologica, considerando il livello di maturità tecnologica tipicamente richiesto per realizzare le attività documentali
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Infrastrutture e altre dotazioni informatiche	Danneggiamento, perdita o furto di risorse informatiche	Rara	Critico	Non accettabile	Sono stabilite e divulgate procedure di gestione e regole chiare per il corretto utilizzo delle risorse informatiche (sono compresi i dispositivi mobili usati per attività lavorative). Per risorse critiche, sono previsti sistemi di controllo automatici e meccanismi di riservatezza.

Fornitori di Servizi/Applicazioni	Patrimonio Informativo	Dati e Documenti non consultabili (disponibilità)	Rara	Alto	Non accettabile	Il fornitore del servizio adotta meccanismi tecnologici e misure di sicurezza, che garantiscono la disponibilità del Servizio secondo gli SLA contrattualizzati
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Struttura Organizzativa	Flusso delle comunicazioni tra le parti coinvolte non adeguato (segnalazioni incidente e richieste di assistenza)	Rara	Basso	Minim	Identificato la figura e lo strumento che mantiene costante il flusso delle informazioni seguendo la procedura definita
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Infrastrutture e altre dotazioni informatiche	Uso di strumenti non autorizzati	Moderato	Medio	Accettabile	Sono stabilite e divulgate procedure di gestione e regole chiare per il corretto utilizzo delle risorse informatiche (sono compresi i dispositivi mobili usati per attività lavorative). Per risorse critiche, sono previsti sistemi di controllo automatici
Responsabilità condivisa tra Ente e Fornitori di Servizi/Applicazioni	Infrastrutture e Applicazioni	Invio fraudolento/falsificazione di email	Rara	Medio	Minimo	Sono adottate, d'intesa con il Fornitore del servizio qualificato, misure di filtraggio della posta e configurazioni di sicurezza sul server di posta. Il personale autorizzato é debitamente istruito sulle buone pratiche di utilizzo sicuro della email e altri servizi internet.
Fornitori di Servizi/Applicazioni	Infrastrutture e Applicazioni	Compromissione/Intercettazione dei dati trasmessi	Rara	Critica	Non accettabile	Utilizzo di standard aperti di comunicazione sicura (ad esempio utilizzando il servizio di PEC); applicazione di canale cifrato per le comunicazioni mediante utilizzo di protocolli SSL/TLS.

Probabilità di accadimento	***Frequenza con cui la specifica minaccia può verificarsi nel tempo***	**Impatto**	***Entità del danno conseguente al verificarsi della minaccia sull'operatività e sugli asset utilizzati***
4 – Frequente (può accadere regolarmente, almeno una volta l'anno)		1 – Basso (irrilevante)	
3 – Moderata (frequenza compresa tra 2-4 anni)		2 – Medio (senza conseguenze)	
2 – Rara (frequenza compresa tra 1-5 anni)		3 – Alto (importante ma riparabile)	
1 – Improbabile (superiore a 5 anni)		4 – Critico (visibile sui risultati dell'Ente)	

Rischio minimo (*valore PxI≤4*), nessun provvedimento necessario, controllare evoluzione; **Rischio accettabile** (*valore PxI>4*), verificare i provvedimenti (adozione di strategie e/o contromisure) necessari per il trattamento del rischio; **Rischio non accettabile** (*valore PxI≥8*), provvedimenti (adozione di strategie/contromisure) urgentemente necessari per il trattamento del rischio.

L'Ente ed i Fornitori di tecnologie coinvolti, sono consapevoli che i meccanismi di attacco/pericoli sono sempre in evoluzione, spesso sfruttando vulnerabilità/debolezze non ancora catalogate.
Entrambi provvedono, per quanto di competenza, ad effettuare verifiche e controlli costanti sul Servizio erogato al fine del continuo miglioramento dello standard di qualità e sicurezza di utilizzo.

Nelle prossime sezioni sono descritte le azioni messe in atto dall'Ente in accordo con i Fornitori, secondo il principio di responsabilità condivisa, realizzando una serie di controlli che rispondono ai requisiti di sicurezza identificati (dall'analisi di rischio, dalla legislazione, dai regolamenti di riferimento, altre fonti) e che comprendono politiche, procedure, istruzioni, responsabilità, meccanismi e strumenti hardware e software.

3. MISURE DI SICUREZZA ORGANIZZATIVE

Di seguito sono descritti i provvedimenti adeguati a trattare rischi operativi e di sicurezza derivanti da criticità organizzative in termini gestionali e operativi tra cui: insufficiente formazione e sensibilizzazione del personale, mancata o poco chiara attribuzione di responsabilità, mancanza o inefficacia di procedure specifiche, carenza nella comunicazione e nell'analisi del rischio, inefficacia gestione delle relazioni, altro.

3.1 Ruoli e Responsabilità

Secondo quanto previsto dalla Regole Tecniche di supporto al CAD, il presente Piano per la Sicurezza Informatica (relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso; la fase della conservazione dei documenti informatici è gestita dal Soggetto Conservatore accreditato) è organizzato e predisposto dal Responsabile della Gestione Documentale d'intesa con il Responsabile dei Sistemi Informativi, sentito il Responsabile della Protezione dei Dati che, se richiesto, fornisce consulenza al trattamento e al controllo dei dati. In aggiunta, si richiede il supporto dei Fornitore di tecnologia, servizi di sicurezza e data protection.

Co.el.da e Kibernetes, in qualità di Fornitori di infrastruttura IT e piattaforma applicativa della soluzione di gestione documentale, si impegnano a garantire la massima sicurezza delle infrastrutture fisiche e logiche, in particolare implementando una politica di sicurezza dei sistemi informativi ed in aderenza alla legislazione vigente ed alle certificazioni mantenute.

3.1.1 Elenco utenti incaricati

Il Responsabile della Gestione Documentale predispone e mantiene aggiornato l'elenco degli utenti incaricati/autorizzati all'accesso al Sistema di Gestione Documentale, con le relative abilitazioni che dispone mediante ordine di servizio e lo comunica. Sono descritte eventuali particolarità sulle modalità di individuazione dei soggetti o sul conferimento delle abilitazioni.

I Fornitori di tecnologia, in qualità di Responsabile Esterno al Trattamento, predispongono e mantengono aggiornato al proprio interno un elenco di soggetti autorizzati alle operazioni di trattamento: Incaricati al trattamento, Amministratori di Sistema, altre tipologie che possono essere individuate (ad esempio, altri soggetti esterni che effettuano il trattamento dei dati) e tutti inquadrati in base alle attività assegnate. In particolare gli Amministratori di Sistema (AdS) sono figure professionali "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

3.2 Formazione e Sensibilizzazione del personale

In conformità a quanto disposto dall'art. 13 del CAD (D.lgs. 82/2005 e s.m.i), ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla loro formazione fino alla loro trasmissione al sistema di conservazione, l'Ente predispone adeguate attività formative e informative per il personale coinvolto, con particolare riferimento ai seguenti temi:

- utilizzo del Sistema di Gestione Informatica dei Documenti; organizzazione sicura del lavoro a distanza;
- fascicolazione dei documenti informatici;
- politiche e aspetti organizzativi previsti nel manuale di gestione; legislazione e tematiche relative alla gestione documentale;
- riferimenti privacy e sicurezza informatica;
- aggiornamento continuo sui temi indicati.

La pianificazione della formazione è coordinata dal Responsabile della Gestione Documentale, tenendo conto dei seguenti aspetti:

- analisi dei bisogni formativi;
- programmazione dei percorsi formativi;
- diffusione delle informazioni sui corsi;
- effettuazione degli interventi formativi;
- valutazione degli interventi.

3.3 Continuità Operativa del Servizio

Scopo della continuità operativa è la protezione dell'Ente, per garantire e migliorare la capacità di reagire agli incidenti, rispondere alle emergenze e alle calamità (resilienza organizzativa).

Con l'obiettivo di ridurre la probabilità che tali eventi negativi avvengano, oltre a quello di permettere all'Ente di prepararsi ad essi e rispondere in modo adeguato, per ripristinare l'operatività nel più breve tempo possibile, le azioni di prevenzione intraprese sono indicate nel Piano di Continuità Operativa e di Disaster Recovery d'intesa con Co.el.da. e Kibernetes.

3.3.1 Continuità Operativa del Sistema di Gestione Documentale

Il Sistema di Gestione Documentale è ospitato su infrastruttura IT di proprietà dei Fornitori.
Sono adottate tutte le iniziative volte a ridurre, a un livello ritenuto accettabile, i danni conseguenti incidenti/disastri che colpiscono direttamente o indirettamente l'Infrastruttura IT dei servizi erogati. Co.el.da e Kibernetes sono consapevoli che le misure di BC e DR sono misure di sicurezza fondamentali per garantire la disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali, e nel contempo garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico, come richiesto dall'art. 32 del Regolamento UE 2016/679 (GDPR).

Tutto ciò premesso, il Sistema di Gestione Documentale è incluso:

- nell'ambito del Sistema di Gestione della Continuità Operativa di Co.el.da e Kibernetes;
- nell'ambito della soluzione tecnologica di Disaster Recovery di Co.el.da e Kibernetes; tale soluzione costituisce l'insieme delle misure per garantire alle strutture di Co.el.da e Kibernetes di gestire il ripristino del Servizio di Gestione Documentale a fronte di eventi disastrosi che rendano indisponibile per periodi prolungati il Sito principale, attraverso l'attivazione del Sito secondario predisposto in Sito alternativo (ridondanza geografica).

È attuata una politica di Backup e Ripristino sui server e apparecchiature utilizzate per l'erogazione del servizio. Sono pianificate procedure di gestione, esecuzione e manutenzione dei meccanismi di Backup e Ripristino per tutti i sistemi e dati necessari alla continuità operativa, alla ricostruzione del sistema, all'analisi degli incidenti. Le frequenze e i metodi di archiviazione sono definiti a seconda dell'esigenza e il processo di backup è soggetto a monitoraggio e alla gestione degli errori delle informazioni e delle applicazioni, sottoposti a verifiche periodiche.

3.3.2 Attivazione del Registro di emergenza del protocollo

In casi di indisponibilità, a livello centralizzato del Sistema di Gestione Documentale, ad esempio ogni qualvolta per cause tecniche non sia possibile utilizzare la procedura ordinaria, il Responsabile del Sistema di Gestione Documentale autorizza lo svolgimento delle operazioni di registrazione di protocollo tramite procedura di emergenza, su registri presso specifiche e protette postazioni, secondo quanto riportato nel Manuale di gestione. Si applicano le modalità di registrazione dei documenti sul registro di emergenza e di recupero delle stesse nel sistema di protocollo informatico di cui all'articolo 63 del DPR 445/2000.

Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, seguendo le istruzioni del Responsabile della Gestione Documentale.
Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema di gestione documentale ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

3.4 Gestione incidenti di sicurezza e violazione dei dati personali

L'incidente di sicurezza informatica è qualsiasi evento o insieme di eventi che sottintendono una violazione delle politiche di sicurezza ICT, fonte di danno per gli asset ICT ovvero per il patrimonio informativo dell'organizzazione e per il quale si rende necessaria l'applicazione di misure di contrasto e/o contenimento da parte delle strutture preposte. Alcuni possibili esempi:

- accesso non autorizzato agli asset IT;
- diffusione non autorizzata di informazioni riservate provenienti dagli asset IT;
- impersonificazione (sostituzione) di utenti, tramite la compromissione delle credenziali personali di autenticazione;
- perdita o modifica delle configurazioni di sistema;
- degradamento dei livelli di servizio standard;
- interruzione di servizi ICT;
- constatazione di illeciti o azioni criminose apportate con l'ausilio delle risorse IT all'Ente ai danni della PA o di terzi.

Una violazione di sicurezza comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione o accesso non autorizzati ai dati personali trasmessi, conservati o comunque trattati. Sono alcuni possibili esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

È compito dei servizi competenti in materia di sistemi informativi dell'Ente e di quelli dei Fornitori procedere ad attivare il processo risposta agli incidenti e data breach, alla comunicazione, al riesame e alla verifica delle politiche di sicurezza, ciascuno per quanto di propria pertinenza.

Di regola, a seguito del verificarsi di un incidente, si procede con le macro-attività di seguito riportate:

- Rilevazione, identificazione e classificazione degli incidenti;
- Gestione degli incidenti;
- Chiusura degli incidenti.

Il piano di risposta agli incidenti, in particolare nel caso di perdita, uso improprio o acquisizione non autorizzata di dati personali viene comunicato a tutte le parti coinvolte tra cui:

- gli utenti degli aggiornamenti e delle procedure di sicurezza in cui sono coinvolti;
- notifica tempestiva alle autorità competenti (vale a dire alle autorità di vigilanza e alle autorità preposte alla protezione dei dati), laddove esistano, in caso di gravi incidenti che coinvolgono dati personali.

Nei casi in cui l'incidente consista in una violazione di dati personali (data breach) e si ritiene probabile che la violazione dei dati personali presenti effettivamente un rischio per i diritti e le libertà delle persone fisiche l'Ente provvede, ove necessario, consultato il DPO, alla notifica al Garante privacy e/o comunicazione agli interessati (secondo le modalità e i tempi prescritti dal Regolamento UE 2016/679 e come previsto dal Provvedimento del Garante per la protezione dei dati personali del 30 luglio 2019, sulla notifica delle violazioni dei dati personali (data breach).

Per indicazioni, si rimanda alle procedure adottate dall'Ente, Titolare del trattamento e da ogni Fornitore, Responsabile Esterno del trattamento (in qualità di Fornitore del Servizio di Gestione Documentale).

3.4.1 Tempistiche e modalità con cui vengono gestite violazioni dati da Co.el.da e Kibernetes

Il Fornitore del Servizio di Gestione Documentale, e Protocollo, in caso di violazione di sicurezza (ad esempio consistente nella perdita, modifica, accesso e divulgazione non autorizzata) dei dati personali, tale da mettere in pericolo i diritti e le libertà degli individui, i cui dati è autorizzato a trattare in qualità di Responsabile del trattamento, per conto dell'Ente Titolare, agisce secondo quanto prescritto dalla normativa in materia di protezione dei dati personali:

- informando tempestivamente l'Ente Titolare
- fornendo assistenza per far fronte alla violazione e alle conseguenze
- proponendo azioni per mitigare gli effetti delle violazioni, seguendo le indicazioni del Titolare

3.5 Gestione segnalazioni anomalie e richieste di supporto

Di norma, il personale che riscontri un problema e/o un disservizio che impedisca il normale svolgimento dell'attività lavorativa, deve segnalarlo al Responsabile del Servizio di Gestione Documentale o suo delegato per attivare la procedura di richieste di assistenza e gestione incidenti. Il processo di intervento adottato a fronte di anomalie riscontrate a seguito del monitoraggio delle funzionalità del Sistema di Gestione Documentale o di segnalazioni di utenti autorizzati dell'Ente, viene condotto secondo quanto indicato nel presente documento e in accordo con eventuali altre indicazioni formalizzate e adottate dall'Ente.
L'assistenza ed il supporto tecnico alla piattaforma applicativa di Gestione Documentale e protocollo è gestito da un sistema di gestione delle richieste di assistenza adottato dai Fornitori; consente una gestione completa delle anomalie, tracciando l'incaricato alla risoluzione, le azioni intraprese e lo stato del problema fino alla completa risoluzione.

Le strutture e gruppi di lavoro, preposti al mantenimento della continuità del Servizio di Gestione Documentale, individuate, dovranno seguire le procedure specificate nel Sistema di Governo della Sicurezza delle Informazioni dei fornitori, classificando le anomalie per tipologia, gravità e priorità.

3.5.1 Tempistiche per la presa in carico e risoluzione anomalie

Le tempistiche per la presa in carico, gestione delle segnalazioni di malfunzionamento e le richieste di assistenza e supporto, dipendono dalle diverse priorità assegnate.
Generalmente, in base ai diversi livelli di segnalazione, il tempo massimo impiegato per prendere incarico una segnalazione ed il tempo massimo di risoluzione, dipendono dalla criticità rilevata.

3.6 Gestione Terze Parti coinvolte

Al fine di assicurare il rispetto dei requisiti previsti dall'art. 28 Regolamento UE 2016/679 (GDPR), è previsto l'obbligo di individuare soggetti esterni (fornitori di servizi e tecnologie) quali Responsabili del Trattamento, ricorrendo, peraltro, "unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato", anche in considerazione dei rischi per i diritti e le libertà degli interessati e della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento effettuato.
In tal senso, le clausole contrattuali sono redatte in conformità ai requisiti ed ai principi previsti dal Regolamento UE 2016/679, anche con riferimento alla corretta ripartizione delle responsabilità circa i rischi e la conformità dei trattamenti al Regolamento stesso.
Sotto il profilo della sicurezza, il Servizio di Gestione Documentale è organizzato nel rispetto dei principi e dei requisiti previsti in materia di sicurezza dei dati e dei sistemi dal Regolamento (artt. 32 - 34), tenendo conto anche dell'attività di notifica delle violazioni dei dati personali di cui all'art. 33 del Regolamento stesso.

4. MISURE DI SICUREZZA FISICHE E LOGICHE

Di seguito si presentano i provvedimenti messi in atto per trattare rischi operativi e di sicurezza derivanti da criticità di tipo tecnico, implementando un sistema che garantisce tanto la sicurezza fisica quanto la sicurezza logica.
Sono adottate soluzioni di protezione e di sicurezza fisica per:

- i datacenter che ospitano il Sistema di Gestione Documentale, localizzati in Italia;
- gli ambienti dell'Ente dove viene utilizzato il Servizio di Gestione Documentale.

Sono adottate soluzioni di protezione e di sicurezza logica di:

- autenticazione e autorizzazione dell'utente che vuole accedere al sistema;
- tracciamento, tramite registrazioni delle operazioni che l'utente compie nel sistema.

Le due componenti che riguardano gli aspetti di sicurezza tecnica, lavorano in sinergia per implementare un sistema efficiente che garantisca la sicurezza del patrimonio informativo. Tipicamente, la sicurezza fisica rappresenta il primo livello di tale sistema, mentre la sicurezza logica ne rappresenta il secondo.

4.1 Sicurezza fisica dell'Infrastruttura per l'erogazione del servizio

L'architettura del Sistema di Gestione Documentale è costituita da risorse realizzate su Sistema Pubblico di Connettività (SPC) in CLOUD localizzato in Italia, ed utilizzato anche come soluzione di Disaster Recovery.
La sicurezza, la connettività ed i collegamenti alla rete sicuri ed affidabili nonché la disponibilità di banda sufficiente, sistemi di riconoscimento del personale, sono affidati ai Fornitori proprietari e gestori dei data center.

4.1.1 Piani di manutenzione

Le apparecchiature e gli impianti sono oggetto di manutenzione programmata e continuativa per garantirne la corretta funzionalità ed efficienza gestita da Co.el.da e Kibernetes. È attiva una procedura operativa per la gestione degli interventi in emergenza.
Le attività di pianificazione e controllo sono gestite e registrate da Co.el.da e Kibernetes.

4.2 Patching e aggiornamento dei sistemi

A livello di Infrastruttura server ed altri apparati, le configurazioni di sicurezza e la gestione degli aggiornamenti segue le indicazioni descritte da apposita procedura prevista da Co.el.da. e Kibernetes.
A livello di Postazione di Lavoro (sistemi client), la gestione della sicurezza logica sui dispositivi fissi e mobili è implementata attraverso strumenti e meccanismi, amministrati dalla struttura di competenza dell'Ente, seguendo le buone pratiche di approccio di policy di dominio, possibilmente con aggiornamenti automatici e centralizzati.

4.3 Configurazione standard sicura

Le configurazioni delle Postazioni di Lavoro, tipicamente utilizzate per usufruire del servizio di Gestione Documentale, sono gestite secondo le procedure specificate dall'Ente e dalla struttura preposta.
Le regole adottate fanno riferimento alle migliori pratiche conosciute e sono riassunte nella sezione "3.7 *Sicurezza delle postazioni di lavoro e comportamento degli utenti*" del presente documento.

Per i sistemi di tipo server e apparati di rete coinvolti nel servizio di Gestione Documentale, sono sottoposti ad un processo di configurazione di sicurezza, seguendo le direttive ben documentate dalla struttura preposta di Co.el.da, in accordo alle migliori raccomandazioni internazionali ed in aderenza al Sistema di

Governo della Sicurezza delle Informazioni periodicamente aggiornato. Sono considerati i seguenti elementi di base:

- eliminazione dei servizi e dei componenti non necessari;
- configurazione delle regole di routing;
- costante e tempestivo aggiornamento del sistema operativo e delle applicazioni di sicurezza, per minimizzare il rischio legato alle nuove vulnerabilità;
- attivazione di meccanismi di raccolta degli eventi;
- policy delle password;
- restrizione degli accessi a risorse critiche.

4.4 Inventario degli asset hardware e software

La gestione degli asset avviene mediate l'utilizzo di meccanismi e strumenti che permettono sia un monitoraggio delle risorse per l'erogazione e la fruizione del servizio di Gestione Documentale all'interno dell'Ente, che l'attività di distribuzione software.

- Le Postazioni di Lavoro ed altri dispositivi collegati sono censiti e amministrati dalla struttura preposta dell'Ente.
- Analogamente, l'Ente e cataloga tutti gli asset (di tipo fisico e logico) necessari ad erogare servizi, utilizzando un sistema di CMDB/Asset Management che permette la gestione amministrativa dell'intero ciclo di vita dell'asset o elementi di configurazione, dall'approvvigionamento alla sua dismissione e le relazioni fra i vari elementi.

I criteri di valutazione degli asset si riferiscono al valore economico, ai processi/servizi in cui sono coinvolti, alle normative cui sono assoggettati, ai requisiti di riservatezza, integrità e disponibilità, alla criticità per l'organizzazione dell'Ente.

4.5 Politica di controllo degli accessi

Obiettivo della seguente politica è garantire l'accesso sicuro alle informazioni trattate, 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.
L'accesso fisico e logico ai sistemi IT è permesso soltanto al personale autorizzato. L'autorizzazione viene rilasciata tenendo conto dei compiti e delle responsabilità del personale e soltanto alle persone adeguatamente addestrate e controllate.
I Fornitori pongono molta attenzione nella gestione delle utenze e dei profili di accesso e si impegna a garantire che i suoi sistemi IT siano sicuri, dati e applicazioni sono protetti e sono accessibili solo agli utenti autorizzati.
Le sedi dell'Ente e i data center dispongono di misure avanzate di protezione, attiva e passiva. In particolare i siti dove sono ospitati i data center hanno idonei livelli di protezione.
L'integrità di rete è protetta con firewall di rete e altre funzionalità avanzate per creare reti private e per controllare l'accesso a istanze e applicazioni. Se necessario sono disponibili opzioni di connettività che supportano connessioni private o dedicate.

L'Ente, d'intesa con il Fornitore, ha istituito controlli per limitare in modo affidabile l'accesso al Sistema di Gestione Documentale solo alle persone in possesso di un legittimo requisito nel rispetto dell'approccio che l'accesso ai dati e ai sistemi per mezzo di applicazioni informatiche dovrebbe essere limitato a quanto strettamente necessario per la prestazione delle attività richieste. Le identità e le credenziali di accesso per gli utenti autorizzati sono gestite, periodicamente verificate e revocate. I diritti di accesso e le autorizzazioni sono gestite secondo il principio del privilegio minimo e separazione delle funzioni.
Sono controllati rigorosamente gli accessi privilegiati alle risorse informatiche, limitando strettamente e sorvegliando attentamente il personale in possesso di estese autorizzazioni di accesso. I diritti di accesso vengono sottoposti a revisioni periodiche.
In particolare, per gli utenti che operano in qualità di Amministratori di Sistema (AdS – sia nell'organizzazione del Fornitore che in quella dell'Ente), di cui vale ancora la definizione presente nel provvedimento del Garante del 2008 (applicabile in quanto non incompatibile con il GDPR), è mantenuto un elenco aggiornato e le funzioni attribuite sono opportunamente definite in appositi atti di nomina, predisposti a seguito di valutazione delle caratteristiche soggettive degli amministratori. Come prescritto dal provvedimento, l'operato degli AdS è sottoposto ad attività di controllo periodico ed è previsto un sistema di log management finalizzato al tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio e controllo.

La strumentazione e le istruzioni per il controllo degli accessi sono mantenute costantemente adeguate alle esigenze dei servizi offerti dall'Ente e alle esigenze di sicurezza, anche in relazione alle evoluzioni organizzative e tecnologiche.

4.5.1 Accesso ai documenti informatici e gestioni delle abilitazioni

L'accesso al Sistema di Gestione Documentale avviene tramite autenticazione (verifica delle credenziali applicative, username e password) e profili di autorizzazione gestiti ed assegnati agli utenti.
L'autorizzazione consiste in un insieme di funzionalità operative rese disponibili all'utente, tra cui le funzioni principali sono:

- consultazione/visibilità: possibilità per un utente di visualizzare i dati/documenti registrati nel sistema;
- inserimento/Creazione: possibilità per un utente di inserire i dati relativi alla registrazione di protocollo e/o alla gestione del documento;
- modifica: possibilità per un utente di modificare i dati gestionali, con esclusione di quelli obbligatori della registrazione di protocollo;
- annullamento: possibilità di annullare (con motivazione) una richiesta una registrazione di protocollo autorizzata del responsabile preposto.

Sulla base delle funzioni svolte all'interno dell'Ente, il Responsabile della Gestione Documentale governa e assegna le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate dal sistema. Il Sistema di Gestione Documentale consente il controllo differenziato dell'accesso alle risorse di sistema per ciascun utente o gruppi di utenti, permettendo altresì di tracciare tutte le operazioni svolte individuandone, in base alle circostanze, l'autore.

I profili di accesso al sistema sono tipicamente suddivisi secondo le seguenti categorie:

- Responsabile della gestione documentale (e delegati), hanno la visibilità completa di tutti gli oggetti documentali del sistema;
- Utenti che hanno la visibilità per competenza o per conoscenza dei dati, documenti e dei fascicoli secondo la struttura organizzativa e le esigenze espresse dall'Ente;
- Utenti amministratori del Sistema.

Il sistema consente di tracciare tutte le operazioni svolte.

Accesso e diritto alla riservatezza

Il Sistema di Gestione Documentale è organizzato nel rispetto delle norme vigenti in materia di diritto di accesso (artt. 22 e ss. L. 241/1990 sul procedimento amministrativo e D. Lgs 33/2013 sulla Trasparenza) e protezione dei dati personali (D. Lgs. n. 196/2003 e s.m.i e Regolamento UE 2016/679).
Tipicamente, il personale può legittimamente accedere soltanto alle informazioni, ai documenti e ai fascicoli presenti nel sistema, la cui consultazione sia relativa a procedimenti e attività di propria competenza, ovvero secondo la posizione che riveste all'interno della struttura organizzativa dell'Ente.
La riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita dal Sistema di Gestione Documentale attraverso l'uso di profili e password. Una autorizzazione di accesso (profilo) limita le operazioni dell'utente nel sistema alle operazioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.
Di seguito alcune configurazioni a carattere generale:

- I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio;
- Di norma, tutti gli utenti che devono protocollare sono abilitati alla consultazione, inserimento e modifica, ma è possibile abilitare un utente anche alla sola consultazione
- Ciascun utente del Sistema può accedere solamente ai documenti che sono stati assegnati al sua area o agli uffici ai settori ad essa subordinati;
- Un utente può avere la visibilità completa sul registro di protocollo solo a seguito di abilitazione;
- Il personale utente dell'unità protocollo generale e altri (appositamente autorizzati dal Responsabile della Gestione Documentale) sono abilitati alla visualizzazione completa sul registro protocollo;
- Associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione;
- Nel caso in cui sia effettuata la registrazione di un documento riservato, la visibilità completa sul documento stesso è possibile solo alla persona destinataria del documento;
- Solo il personale appositamente autorizzato dal Responsabile della Gestione Documentale è abilitato all'annullamento.

La riservatezza è inoltre assicurata dall'uso delle funzionalità di cifratura del canale di comunicazione messe a disposizione dal protocollo TLS/SSL.
La sessione di lavoro attivata al momento della login dell'utente è automaticamente interrotta nel caso in cui la sua inattività superi il timeout impostato (tipicamente 30 minuti o configurabile).

Accesso di utenti esterni all'Ente

Normalmente, ogni qualvolta è necessario consultare uno o più documenti custoditi dall'Ente, dovrà essere compilata apposita richiesta di accesso agli atti. L'Ente si organizza per consentire la consultazione soltanto di dati o notizie che riguardino il soggetto interessato ed adottando gli opportuni accorgimenti volti ad evitare la diffusione di informazioni di carattere personale, nel rispetto di quanto disposto dalla legge 241/90 e del D. Lgs. 196/03 e s.m.i..
Al momento non è consentito l'accesso al Sistema di Gestione Documentale da parte di altre PA esterne.

4.5.2 Assegnazione, riesame e revoca delle credenziali di accesso

Riguardo al Servizio di Gestione Documentale sono assicurate le seguenti misure:

- L'accesso alle informazioni e funzioni di sistemi applicativi deve essere limitato alle effettive necessità;
- Rimozione o adattamento dei diritti di accesso: i diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni devono essere rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate ad ogni variazione;
- A fronte della cessazione verranno disattivati (storicizzati) gli identificativi di accesso del personale non più in servizio e dei consulenti non più operativi;
- Nessun identificativo di accesso dovrà essere cancellato ma dovranno essere eliminate le abilitazioni;
- Gli identificativi utente assegnati una volta non potranno più essere assegnati successivamente a persone diverse;
- Gestione dei diritti di accesso privilegiato: l'assegnazione e l'utilizzo delle utenze e dei privilegi amministrativi deve essere ristretto e controllato;
- Nel caso sia necessario accedere "in emergenza" a specifici dati/sistemi da parte di personale non ancora abilitato si deve richiedere un'abilitazione temporanea;
- A fronte della definizione di nuove credenziali di accesso / modifica delle esistenti, viene inviata una notifica all'interessato.

4.5.3 Servizi garantiti dai fornitori Co.el.da e Kibernetes

La progettazione e l'attuazione del sistema organizzativo della Gestione Documentale è di responsabilità dell'Ente e delle figure preposte.
Le richieste di servizio/assistenza sono comunicate ai Fornitori, tramite canali concordati con prefissati e garantiti orari di reperibilità, che provvede a gestire le richieste mediante la struttura organizzativa e tecnica predisposta.
Relativamente alla gestione delle credenziali, le policy e la tecnologia utilizzata dai Fornitori sono idonee a garantire sicurezza al sistema sulla base dei seguenti principi:

- account univoci per ogni utente;
- policy di lunghezza e complessità minima della password;
- definizione periodo di scadenza della password;
- policy di lockout dopo N tentativi errati;

- sono registrati gli accessi da parte degli utenti e le attività;
- memorizzate le attività di aggiornamento dei dati di protocollo con evidenza dell'utente che le ha effettuate;
- registrazione degli accessi degli amministratori di sistema mediante credenziali individuali con riferimenti temporali e descrizione eventi;
- le registrazioni conservate per un periodo non inferiore a quanto stabilito dalle disposizioni vigenti.

4.5.4 Raccomandazioni sull'utilizzo responsabile delle password

Di seguito sono riassunte i principali provvedimenti da adottare nella scelta delle password personali e nella loro gestione:

- L'utilizzo e la gestione delle credenziali deve garantire di evitare utilizzi impropri delle password e delle credenziali di autenticazione;
- Le regole relative alla costruzione ed utilizzo delle password si applicano a tutto il personale e terze parti che ne fanno uso per accedere alle risorse dell'Ente;
- L'utilizzo delle password ed in genere delle credenziali utente deve essere controllato con un processo di gestione formale, anche automatizzato, fin ove possibile;
- Le credenziali sono personali e non cedibili, devono essere assegnate in base alla necessità di accedere ai dati o ai sistemi aziendali e devono essere gestite contemporaneamente alle abilitazioni, sulla base del principio del "minimo privilegio";
- Ogni utente è responsabile della corretta gestione della propria password, dei dispositivi di riconoscimento, delle informazioni per l'accesso ai sistemi e ai dati;
- Le credenziali e i dispositivi di riconoscimento devono essere conservati adeguatamente e non essere mai lasciati incustoditi;
- La responsabilità delle azioni compiute nella fruizione del Servizio di Gestione Documentale è dell'utente fruitore del servizio;
- La responsabilità delle operazioni compiute tramite un'utenza è sempre del legittimo titolare, anche se compiute in sua assenza.

4.6 Politica di sicurezza durante il ciclo di vita delle applicazioni

L'obiettivo è quello di assicurare che gli aspetti di sicurezza siano inclusi nelle fasi di realizzazione del software di Gestione Documentale e Protocollo, anche considerando la sua modalità di erogazione. I Fornitori pongono attenzione allo sviluppo applicativo gestito internamente; sono seguite le migliori pratiche, framework e standard di applicazione delle contromisure di sicurezza conosciuti, per ogni livello dell'applicazione.
A titolo esemplificativo e non esaustivo, durante la progettazione e lo sviluppo del Sistema di Gestione Documentale sono considerati gli aspetti di sicurezza che riguardano in particolare:

- le specifiche funzionali e tecniche, per una prima valutazione degli impatti sulle componenti hardware e software e la valutazione dei requisiti di sicurezza;

- le raccomandazioni internazionali di sviluppo sicuro;
- Code Review, analisi delle vulnerabilità e penetration test;
- l'organizzazione delle attività e delle responsabilità;
- la separazione degli ambienti di sviluppo e di test;
- la gestione della documentazione;
- il controllo di accettazione dei rilasci negli ambienti di esercizio;
- la conservazione sicura del codice sviluppato.

Le caratteristiche di sviluppo sicuro, sono descritte e mantenuti aggiornati dai Fornitori Co.el.da e Kibernetes nel Sistema di Governo della sicurezza delle informazioni.

4.7 Politica di protezione da malware

L'obiettivo è quello di garantire un adeguato livello di sicurezza della piattaforma tecnologica a supporto del Servizio di Gestione Documentale (sia lato client che lato server), considerando opportunamente tali aspetti nelle tematiche relative alla gestione di malware/virus.
La politica di protezione delle Postazioni di Lavoro, dei Server e Apparati di rete dalla contaminazione di malware/virus, si applica all'erogazione e fruizione del Servizio di Gestione Documentale e raccomanda di considerare le seguenti direttive:

- le informazioni di proprietà dell'Ente o da essa gestite e le infrastrutture IT preposte alla loro elaborazione devono essere protette contro il malware/virus;
- 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 e controlli di individuazione, di prevenzione e di ripristino relativamente a malware;
- formazione e sensibilizzazione degli utenti per prevenire le minacce e le vulnerabilità derivanti da malware.

Contromisure per la protezione da malware

La tecnologia utilizzata per la protezione da malware/virus è installata su tutte gli apparati con sistema operativo Windows, siano essi server dedicati ad erogare servizi, che postazioni di lavoro dalle quali si accede ai servizi; l'antivirus è installato sia sui sistemi fisici (server, postazione di lavoro), che virtuali utilizzati dall'Ente.
Nei sistemi su cui è installato, l'antivirus con estensione anti-malware è sempre attivo e la scansione opera in tempo reale su ogni movimentazione di file, proteggendo così l'apparato da malware/virus. Le componenti sopra descritte sono periodicamente aggiornate per assicurare adeguate e tempestive misure di protezione.

Contromisure per la protezione dal spamming

Tipicamente, il sistema di gestione la posta elettronica utilizza meccanismi per la protezione dallo spamming; le finalità della strumentazione sono:

- controllare le informazioni di provenienza dei messaggi;
- a seconda della correttezza di tali informazioni, eliminare, inserire in quarantena o consegnare i messaggi al destinatario;
- eliminare dai messaggi ricevuti eventuali programmi eseguibili in essi contenuti;
- inviare ai destinatari l'elenco dei messaggi inseriti in quarantena.

Il personale dell'Ente, qualora ritenga che un messaggio ricevuto sia indesiderato, lo può inviare al sistema che aumenta così la base di conoscenza per l'individuazione dello spamming.
Le componenti sopra descritte sono periodicamente aggiornate per assicurare adeguate e tempestive misure di protezione.

Raccomandazioni e buone pratiche contro malware

Il regolamento dell'Ente, richiede di osservare i seguenti comportamenti e buone pratiche:

- l'utente s'impegna a tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'Ente mediante malware/virus o mediante ogni altro software malevoli (sono tipici esempi; non aprire mail o relativi allegati sospetti, non navigare su siti non riconosciuti come affidabili, altro);
- l'utente s'impegna a controllare la presenza e il regolare funzionamento del software antivirus dell'Ente controllando eventuali notifiche di mancato aggiornamento (tipicamente con cadenza frequente, anche giornaliera), presenza di virus, altro. In questi casi si raccomanda all'utente di:
    - sospendere ogni operazione in corso, possibilmente senza spegnere la postazione;
    - segnalare tempestivamente l'accaduto alla struttura responsabile preposta dall'Ente.

4.8 Sicurezza delle postazioni di lavoro e comportamento degli utenti

Devono essere rispettate le regole sul corretto utilizzo degli strumenti di lavoro assegnati agli utenti per svolgere le attività lavorative. L'uso delle Postazione di Lavoro (in generale per tutte le dotazioni informatiche), del software installato e certificato, aggiunto alla gestione dei permessi sulle singole utenze, consente un controllo effettivo sull'uso improprio degli strumenti di lavoro e sul divieto di installare software non aziendale.

Di seguito sono descritte alcune direttive e raccomandazioni attuate:

Aggiornamenti del software

- L'Ente mediante la struttura preposta, mantiene adeguato il livello di aggiornamento del software installato sulle Postazioni di Lavoro;
- L'utente deve evitare di compromettere gli strumenti/meccanismi di aggiornamento automatico o centralizzato previsti dall'Ente.

Limitazione della connettività a supporti esterni

L'utilizzo improprio di dispositivi rimovibili può aumentare il rischio di fuga di dati riservati. Non bisogna:

- consentire a personale non autorizzato il collegamento di dispostivi rimovibili alla propria postazione;
- connettere alla propria postazione eventuali dispositivi rimovibili non sicuri e lasciarli incustoditi;
- lasciare incustodito il dispositivo all'esterno degli ambienti dell'Ente.

Modifica delle impostazioni di sistema

Il personale ha la responsabilità di non modificare le configurazioni standard (sia software che hardware) impostate al momento dell'installazione iniziale nelle postazioni di lavoro, e di qualsiasi dotazione informatica assegnata, senza specifica autorizzazione della struttura preposta.

Configurazione delle Postazioni di lavoro

Il Sistema di Gestione Documentale è fruibile come applicazione e\o servizio web, con interfacce semplici ed intuitive; le Postazioni di Lavoro ed i browser devono essere adeguatamente configurati da personale autorizzato, secondo le specifiche tecniche riportate nel Manuale di configurazione [MCF CLIENT].

Postazioni di Lavoro virtuali

All'occorrenza l'Ente può organizzare le attività lavorative utilizzando sistemi di virtualizzazione opportunamente configurati in sicurezza, adeguati alle esigenze organizzative a protezione dei dati trattati. L'obiettivo è quello di aderire ad un approccio sicuro di una moderna organizzazione del lavoro, che sfrutta sempre di più i dispositivi mobili e concezioni di lavoro flessibili o decentrate.

4.8.1 Raccomandazioni per un uso accettabile degli asset informatici dell'Ente

Le Postazioni di Lavoro ed altri dispositivi affidati al personale dipendente sono strumenti di lavoro. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche assegnate.
Ogni utilizzo non inerente all'attività lavorativa può contribuire a provocare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
Eventi di furto, di danneggiamento, di smarrimento delle dotazioni assegnate o altre situazioni avverse, devono essere tempestivamente segnalati alla struttura preposta dall'Ente.

Per tutto il personale dell'Ente, si riassume un elenco di raccomandazioni e buone pratiche che devono essere considerate durante lo svolgimento delle attività lavorative assegnate:

- essere a conoscenza del proprio ruolo e delle responsabilità e contribuire al corretto e sicuro utilizzo delle risorse assegnate;
- non è consentito all'utente non autorizzato di modificare le caratteristiche hardware e software impostate sul dispositivo in dotazione, neppure l'installazione di software aggiuntivo se non previa autorizzazione esplicita da parte del Responsabile preposto dall'Ente;
- proteggere i dispositivi assegnati, in caso di assenza, anche temporanea, dalla postazione di lavoro (scrivania/area non presidiata). Ad esempio, impostare un salvaschermo automatico protetto da password che nasconda lo schermo entro alcuni minuti in caso di inutilizzo;
- le informazioni trattate devono essere strettamente necessarie all'attività lavorativa. Nessuna delle informazioni archiviate sul dispositivo in dotazione è tipicamente soggetta a procedure di salvataggio o backup. Pertanto l'utente, in quanto responsabile dei dati contenuti nello stesso,

è tenuto ad archiviare i dati e documenti utilizzando il Sistema di gestione Documentale di cui si effettua il backup periodico e risiede su infrastruttura sicura amministrata dai Fornitori;
- evitare di lasciare informazioni ritenute strategiche e/o di categoria particolare (su supporto cartaceo e/o elettronico) dove possono essere lette, copiate e sottratte da personale non autorizzato e procedere allo smaltimento sicuro (es. distruzione/cancellazione sicura) dei supporti cartacei/elettronici contenenti tali informazioni quando essi non siano più necessari;
- astenersi dall'utilizzo di dispositivi mobili e supporti rimovibili non autorizzati;
- la Postazione di Lavoro deve essere spenta a termine della giornata lavorativa prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Per assenze di breve durata l'utente deve comunque chiudere la sessione di lavoro. Nel caso in cui il responsabile della struttura preposta dall'Ente lo ritenga necessario, può configurare le postazioni in modo tale da andare in lock dopo un predeterminato tempo di inattività (sospensione automatica);
- nel caso di necessità di scambio dati non riservati tra personale intento dell'Ente, appoggiarsi a cartelle temporanee di rete condivise;
- Informazioni riservate, sensibili o classificate, una volta stampate, devono essere rimosse immediatamente dalle stampanti.

Qualunque violazione a queste raccomandazioni deve essere individuata e gestita secondo quanto definito dal regolamento dell'Ente.

4.9 Politica di gestione e dismissione sicura degli asset informatici

L'obiettivo di questa politica è quello di garantire un adeguato livello di sicurezza nel ciclo di vita degli asset e si applica a tutte le risorse dell'Ente e dei Fornitori interessati all'amministrazione del Servizio di Gestione Documentale.

Sono requisiti essenziali, per quanto possibile applicati:

Gestione apparati e supporti informatici

Gli apparati e i supporti informatici devono essere protetti da accessi non autorizzati, utilizzi impropri, manomissioni, danneggiamento o furti:
- durante il loro utilizzo all'interno e all'esterno delle sedi dell'Ente;
- durante il trasporto;
- durante i periodi di inattività.

Specificatamente per dispositivi mobili in dotazione al personale individualmente o secondo una regola di gruppo di appartenenza:
- il personale è autorizzato a portare con sé al di fuori delle sedi dell'Ente gli apparati mobili assegnati;
- la memorizzazione di dati personali non aziendali da parte del personale su apparati mobili non è ammessa a meno di esplicita autorizzazione da parte dell'Ente (a titolo di esempio, smartphone in comodato d'uso).

dismissione apparati e supporti informatici

In caso di restituzione o dismissione di un dispositivo o di un supporto di memoria rimovibile si deve provvedere alla cancellazione in modo sicuro delle informazioni sugli stessi contenute (sono incluse anche istanze virtuali e servizi correlati), incluse le eventuali aree-disco temporanee del dispositivo utilizzate per la memorizzazione delle informazioni durante la sessione di lavoro. Il procedimento di rimozione deve avvenire in modo che le informazioni non siano più recuperabili.
Nell'ambito del rispetto della politica sulla sicurezza delle informazioni, ci possono essere casi in cui sia necessario lo smaltimento sicuro dei supporti.

gestione supporti cartacei

In generale le informazioni presenti sui supporti cartacei (documenti, annotazioni) non dovrebbero mai essere lasciate dal personale in luoghi al di fuori del proprio controllo.
Nello specifico le informazioni rilevanti o riservate presenti sui supporti cartacei non devono mai essere lasciate dal personale al di fuori del proprio controllo.
Sulle scrivanie degli uffici, sui tavoli delle sale riunioni, o in altri luoghi, al termine del lavoro o al termine delle riunioni non deve essere lasciata documentazione riservata.
Sui dispositivi di stampa, fotocopia, acquisizione ottica delle immagini e nelle loro vicinanze non deve essere lasciata documentazione riservata.
A maggior ragione la documentazione riservata deve essere gestita con particolare cura all'esterno delle sedi dell'Ente.

dismissione supporti cartacei

Le informazioni rilevanti o riservate presenti sui supporti cartacei che non si intende più utilizzare, devono essere distrutte o rese non consultabili.
Nel caso di cessato utilizzo di documenti cartacei riservati, essi devono essere triturati/distrutti con gli appositi strumenti.

Scelta del metodo di smaltimento

Rispetto al tipo di supporto e al contenuto (ad esempio, documenti sensibili o particolari prodotti dagli uffici non destinati alla conservazione a norma) viene deciso quale metodo di smaltimento/distruzione sicuro adottare: in loco o con utilizzo di terze parti.
Per lo smaltimento/distruzione sicuro è raccomandabile utilizzare un servizio fornito da un terzo certificato (che applica le norme specifiche del settore, ad esempio UNI-EN 15713).
Il fornitore del servizio dovrà rilasciare un certificato di smaltimento conforme alla normativa vigente. Eventualmente se necessario, alcune delle apparecchiature (o componenti di esso) possono essere riciclati in conformità con la legislazione vigente.

5. SICUREZZA NELLE COMUNICAZIONI

L'uso del network (sistemi di rete fisiche e virtuali) ha un ruolo essenziale nelle attività dell'Ente per lo scambio di informazioni e l'utilizzo di servizi necessari.
Le reti non solo collegano fra loro tutti i componenti dei processi dell'Ente, ma collegano l'Ente con i suoi fornitori, utenti e in generale con il mondo esterno.

Pertanto, il sistema rete deve essere protetto per garantire che la riservatezza, l'integrità e la disponibilità delle informazioni vitali sia garantita in ogni momento.

L'accesso ai servizi Internet (navigazione web, posta elettronica, altri servizi di collaborazione e condivisione risorse), tramite risorse informatiche e di rete dell'Ente, deve avvenire in modalità sicura (a titolo di esempio, utilizzando apparati e protocolli di sicurezza come: firewall, HTTPS, SMTPS, altro), per garantire la protezione degli asset e del patrimonio informativo trattato. Gli utenti dovranno essere identificabili individualmente prima di poter avere accesso ai servizi Internet. È vietato il compimento di atti di criminalità informatica, come accedere abusivamente a sistemi informatici altrui, diffondere programmi la cui presenza danneggia la rete e/o le risorse ad essa collegate, intercettare abusivamente comunicazioni telematiche altrui, pubblicare su siti web password o altri codici d'accesso etc.
L'inosservanza di queste regole potrebbe avere un effetto significativo sul funzionamento efficiente dell'Ente e può provocare perdite di immagine e interruzione di servizi necessari.

5.1 Sicurezza nella trasmissione e interscambio dei documenti

La trasmissione e l'interscambio di documenti e fascicoli informatici all'interno dell'Ente avviene tramite:

- sistema di gestione documentale
- posta ordinaria
- posta elettronica tradizionale
- altre modalità indicate nel Manuale di Gestione
- cartelle condivise

considerando l'adeguatezza dello strumento di comunicazione a garantire idonei livelli di sicurezza, anche in funzione del rispetto della normativa in materia di protezione dei dati personali; obiettivo principale è evitare la diffusione non autorizzata di documenti e dati.

La trasmissione di documenti informatici e fascicoli informatici al di fuori dell'Ente avviene principalmente tramite:

- il Sistema di Gestione Documentale, se configurato per collegarsi ad una casella PEC istituzionale, consente di ricevere documenti informatici provenienti da altri Enti e Operatori privati.
- la PEC dell'Ente, verificata la necessità della firma digitale e la conversione in un formato standard, solitamente un PDF
- altri meccanismi dell'interoperabilità e della cooperazione applicativa autorizzati, utilizzando, ove necessario, le informazioni contenute nella segnatura di protocollo, strutturate in un file conforme alle specifiche XML, compatibile con un file XML Schema e/o DTD, secondo lo schema previsto da AgID.

I messaggi di posta elettronica certificata prodotti dall'Ente sono compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045 e 2049 e successive modificazioni. Il server di posta certificata del fornitore esterno di cui si avvale l'Ente consente il:

- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute.

Mediante l'utilizzo della tecnologia di firma digitale, durante lo scambio tramite PEC di messaggi protocollati, viene garantita al ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la sua riservatezza.

6. CONSERVAZIONE A NORMA DEI DOCUMENTI

I documenti registrati sul Sistema di Gestione Documentale, sono conformi ai requisiti e contengono i metadati previsti ai fini della conservazione a norma, secondo quanto indicato nelle Regole tecniche di riferimento. Il trasferimento nel sistema di conservazione avverrà mediante la produzione di Pacchetti di Versamento, basati su uno schema XML conforme a quanto previsto nel Manuale di Conservazione del Soggetto Conservatore.
In particolare, il Sistema di Gestione Documentale, al termine della giornata lavorativa effettuerà la generazione automatica del registro di protocollo, secondo una struttura predeterminata, trasferito in forma statica entro la giornata lavorativa successiva nel Sistema di Conservazione, come indicato nelle regole tecniche di riferimento.

Per le modalità operative di trasmissione del contenuto del Pacchetto di Versamento (PdV) al sistema di conservazione si rimanda al Manuale di Conservazione dei Fornitori, in qualità di Soggetto Conservatore accreditato AgID, pubblicato sul portale
https://www.agid.gov.it/it/piattaforme/conservazione/conservatori-accreditati che illustra nel dettaglio: l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione a norma.

7. SINTESI DELLE MISURE DI SICUREZZA PER TRATTAMENTO DATI PERSONALI

Con l'introduzione del Regolamento UE n. 679/2016 (GDPR) il Legislatore europeo ha inteso affermare la sicurezza dei dati come condizione di legittimità di ogni trattamento messo in atto. È stata infatti inserita tra i principi generali di cui all'art 5 par. 1 lett. f), per cui i dati personali devono essere trattati in maniera da garantirne "*un'adeguata sicurezza…compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).*

L'Ente, in qualità di Titolare del trattamento dei dati personali è responsabile della sicurezza delle proprie risorse e dei sistemi applicativi implementati per l'utilizzo del Servizio di Gestione Documentale e protocollo d'intesa con le società Co.el.da e Kibernetes che, in qualità di Responsabile al Trattamento dei dati personali, mettono a disposizione le infrastrutture IT e le risorse necessarie per supportare l'Ente nella protezione di dati trattati, adottando i provvedimenti necessari per preservare la sicurezza e la

riservatezza dei dati, per impedire che vengano violati, danneggiati o che siano resi disponibili a soggetti terzi non autorizzati.
In base alla condivisione delle responsabilità, si applicano procedure formalizzate sotto riportate, senza che questa lista costituisca un elenco esaustivo:

- procedere ad una puntuale mappatura e classificazione dei dati trattati;
- analizzare il rischio e verifica la necessità di eventuale valutazione d'impatto di trattamenti;
- nominare ed eseguire formazione continua agli operatori incaricati ai trattamenti, anche in base allo svolgimento delle mansioni e dei compiti assegnati;
- nominare il personale autorizzato al ruolo di Amministratore di Sistema;
- nominare la figura di DPO;
- stabilire una procedura di Data Breach e di comunicazioni alle Autorità preposte;
- mantenere aggiornata una lista di controllo degli accessi;
- amministrare un adeguato sistema di autenticazione;
- registrare e riesaminare eventi di pericolo;
- utilizzare adeguate tecnologie e meccanismi per proteggere i dati in transito ed archiviati;
- controllare i Fornitori nominati Responsabili Esterni al Trattamento.

L'Ente supervisiona e controlla che i Fornitori coinvolti nell'erogazione del Servizio di Protocollo e Gestione Documentale rispettino le misure di sicurezza in materia di riservatezza dei dati personali in aderenza al Regolamento UE ed alla normativa italiana.
Nello svolgimento delle attività di registrazione di protocollo, il sistema di sicurezza adottato dall'Ente in collaborazione con il Fornitore, garantisce la protezione di tali informazioni sulla base dell'architettura del sistema informativo, sui controlli di accesso e sui livelli di autorizzazione previsti.
Per le operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici, il personale incaricato, non può prendere conoscenza della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate ad essere rese pubbliche.
Il personale addetto al protocollo adotta tutti gli accorgimenti necessari per la tutela dei dati soggetti a categoria particolare e/o relativi a condanne penali e reati, verificando che non risultino nel campo "oggetto" del registro di protocollo.

Gli utenti sono profilati per ruoli, permettendo la visualizzazione di documenti solo per le necessità legate all'appartenenza ad un ufficio o alla responsabilità di un procedimento amministrativo determinato, senza consentire di disporre del registro di protocollo in maniera indistinta attraverso una semplice ricerca testuale. Il servizio è configurato in modo da segmentare la visibilità dei documenti e dei fascicoli (particolari) ai soli dipendenti incaricati del trattamento dei dati.

8. MONITORAGGIO E CONTROLLI

Il Sistema di Protocollo e Gestione Documentale utilizzato è sottoposto a procedure di monitoraggio e di controllo, secondo quanto previsto dalle Regole Tecniche e Linee Guida AgID, che ne garantiscono la disponibilità e la corretta funzionalità agli utenti autorizzati assicurando livelli di sicurezza adeguati.

I Fornitori coinvolti nell'erogazione del Servizio assicurano che tutte le componenti fisiche e logiche utilizzate siano soggette a controlli automatici e manuali, per rilevare anomalie ed eventi che possono compromettere il corretto funzionamento del servizio, eventuali guasti, malfunzionamenti, prestazioni degradate, saturazione delle risorse, rilevazione intrusioni fisiche e logiche, violazioni della riservatezza, dell'integrità e della disponibilità delle risorse IT.
Le segnalazioni sono sottoposte a verifiche del personale autorizzato, incaricato dai Fornitori, in qualità di Fornitore del Servizio di Gestione Documentale e >Protocollo. Le segnalazioni di anomalie verranno gestite come indicato nella sezione "2.*8 Gestione segnalazioni anomalie e richieste di supporto*" e dagli accordi di servizio aggiornati.

8.1 Conformità e Certificazioni dei Fornitori

I Fornitori Co.el.da e Kibernetes, per garantire il mantenimento della conformità e valutare le prestazioni del sistema, esegue periodicamente secondo un piano di audit predefinito, verifiche tra cui:

- audit esterni, effettuati da organismi di certificazioni accreditati;
- audit interni, effettuati da personale interno/esterno, finalizzati a valutare e migliorare i processi di gestione dei rischi, di controllo, e di governance;
- audit tecnici, effettuati da personale interno/esterno che comprendono test di intrusione, scansioni di vulnerabilità, revisioni del codice;
- audit di attività affidate a terzi specialisti nel campo della sicurezza informatica;
- audit di affidabilità dei data center.

Quando si identifica una situazione non conforme, viene eseguita un'azione correttiva e migliorato il processo di gestione. Tutte le attività vengono tracciate, revisionate e riesaminate periodicamente.

8.2 Livelli di servizio

L'Ente include, nel monitoraggio continuo del servizio erogato dal Fornitore, alcuni indicatori a garanzia di un adeguato livello minimo di qualità. A titolo esemplificativo e non esaustivo, si riportano le metriche maggiormente rappresentative che possono essere considerate.

Orario di servizio	08:00 – 21:00 Lunedì– Venerdì 08:00 – 14:00 Sabato
Disponibilità del servizio	Superiore al 99%
Tempo massimo di presa in carico di una segnalazione	Come indicato negli accordi di servizio
Tempo massimo di risoluzione di una segnalazione	
RTO	72 ore
RPO	24 ore

8.3 Ripristino del Servizio

Il Responsabile della Gestione Documentale cura che le funzionalità del sistema, in caso di guasto o anomalia, siano ripristinate nel più breve tempo possibile e, comunque, entro ventiquattro ore dal blocco delle attività (art. 61, comma 3 del TUDA DPR 445/2000).
Il Fornitore si impegna a garantire la continuità operativa delle infrastrutture (apparecchiature, applicazione e processi operativi) secondo quando indicato nella sezione "*2.3 Continuità Operativa del Servizio*".

8.3.1 Monitoraggio e Controllo delle segnalazioni

I Fornitori rendono disponibile un servizio di assistenza al quale il personale dell'Ente può accedere attraverso l'apertura di una segnalazione (ticket) per chiedere la risoluzione di eventuali anomalie emerse durante la fruizione del servizio. Le segnalazioni di anomalie verranno gestite come indicato dagli accordi di servizio aggiornati.
Resta inteso che, in caso di malfunzionamento del Servizio, i Fornitori sono tenuti a comunicare il problema riscontrato al Responsabile della Gestione Documentale; la comunicazione deve essere effettuata (anche tramite email o altro canale concordato negli accordi di servizio) entro due ore all'interno dell'orario di servizio dal lunedì al venerdì.

8.4 Monitoraggio e Controllo dei servizi e delle infrastrutture

Il Servizio di Gestione Documentale e di Protocollo sono ospitati rispettivamente su infrastruttura di Kibernetes e di Co.el.da e sono continuamente monitorati sulle prestazioni e sulle performance con i seguenti obiettivi:

- prevenire ed individuare eventi, problemi e incidenti di sicurezza;
- assicurare la continuità del servizio nel miglior modo possibile;
- monitorare le funzioni critiche con sistemi di early warning alla struttura preposta;
- avvisare i responsabili per attuare le azioni necessarie;
- prendere precauzioni per proteggere l'integrità delle risorse coinvolte nel servizio.

Il controllo degli obiettivi viene amministrato dal fornitore tramite processi, strumenti e meccanismi tecnici-operativi di seguito riassunti.

Procedure operative
Co.el.da e Kibernetes implementano, applicano e tengono costantemente aggiornati i documenti di processo che contengono le istruzioni necessarie per:

- assicurare il monitoraggio ed il controllo del corretto funzionamento dell'infrastruttura IT del Sistema di Gestione Documentale;

- descrivere le attività necessarie affinché ai sistemi ed alle procedure applicative siano rese disponibili le risorse necessarie al corretto funzionamento;
- garantire il supporto centralizzato gestito dai team della sicurezza H24/365.

Strumenti

Co.el.da e Kibernetes utilizzano diversi strumenti hardware e software al fine di monitorare la disponibilità e le prestazioni dell'ambiente di produzione dei servizi del Cliente e l'operatività dell'infrastruttura e dei componenti di rete, tra cui:

- sonde di rilevazione,
- registrazione degli eventi;
- management console;
- segnalazioni generate automaticamente.

Lo staff operativo de due Fornitori esamina ogni allarme automatico e avviso associato a deviazioni dell'ambiente dalle soglie di monitoraggio definite e segue procedure operative standard definite al fine di investigare e risolvere i problemi sottesi

8.5 Generazione di file di log degli eventi

Co.el.da e Kibernetes attuano una politica di gestione eventi per i propri Sistemi e Applicazioni, in conformità alle normative esistenti, generando file di log per ogni Sistema/Applicazione utilizzata per l'esercizio del Servizio di Gestione Documentale.
I file di log includono gli accessi ai dati ed alle configurazioni degli ambienti di produzione; sono contrassegnati con data e ora (sincronizzazione delle risorse hw), adeguatamente protetti da manomissione e accessi non autorizzati; sono verificate le configurazioni dei sistemi e analizzato chi è come può accedere ai file di log, con quali permessi e se può modificarli.

Tipicamente, sono tracciate, registrando le informazioni minime richieste per ricostruire le modalità di accesso, malfunzionamenti, performance e permettere il monitoraggio sul sistema, dati tipo:

- Identificazione utente;
- Fonte dell'evento;
- Tipo di evento;
- Data e ora;
- Indicazioni di riferimento, quali dati/campi, altro.

A seconda della tipologia dei log, delle fonti dei log e della loro importanza, sono definite appropriate modalità di registrazione, accesso, archiviazione e cancellazione.
Le principali tipologie/fonti di log:

- log di sistema e degli apparati, registra gli eventi significativi delle componenti infrastrutturali;
- log di sicurezza, registra tutte le operazioni che sono considerate critiche per l'integrità del sistema e dei dati;

- log applicativi, registra gli eventi specifici dell'applicazione, evidenziando il tipo di errore, i problemi e le modifiche effettuate;
- log di accesso e autenticazione, corrisponde al login per l'acceso di un'utenza al sistema, contiene riferimenti tipo: codice identificativo utilizzato, data e ora di login, informazioni sull'eventuale fallimento e data e ora di logout.

L'analisi/revisione dei dati di log (eventi), suddivisa per tipologia, è attuata periodicamente con un sistema SIEM che analizza i dati evidenziando attacchi, minacce, violazioni delle policy e molte altre attività sospette. Lo scopo è sempre quello di generare alert di sicurezza per la prevenzione e rilevamento minacce alla sicurezza delle informazioni, asset e dati personali.
I file di log sono conservati per il tempo minimo necessario a rispondere alla finalità per la quale sono stati raccolti e comunque nel rispetto di quanto previsto dalle leggi e alle normative esisti (Garante Privacy, GDPR, regolamenti AgID, altre fonti).

Su richiesta dell'Ente Titolare, i Fornitori dei Servizi, rende disponibile i file di log di riferimento in un formato adeguato alla consultazione.

8.6 Monitoraggio degli incidenti di sicurezza

I Fornitori garantiscono il monitoraggio, la gestione e la verifica costanti e integrati degli incidenti relativi alla sicurezza, comprese le segnalazioni degli utenti su argomenti di sicurezza secondo quanto indicato nella sezione "*2.6 Gestione incidenti di sicurezza e violazione dei dati personali*".

È stabilita e attuata una procedura per la registrazione, classificazione e quando necessario, segnalazione di tali incidenti ad un Gruppo di Sicurezza. In caso di gravi incidenti, relativi alla sicurezza dei dati personali, si attiva il processo di notifica/comunicazione alle autorità competenti (tra cui il Garante per la protezione dei dati personali e l'Autorità Giudiziaria).
Gli audit log che possono compromettere la sicurezza delle risorse informative sono tracciati, registrati e conservati (secondo la normativa vigente) ai fini della ricostruzione dell'evento e a supporto di future analisi forensi per gli accertamenti di comportamenti illeciti.
Il Fornitore si avvale di una procedura di comunicazione per:

- tenere al corrente gli utenti degli aggiornamenti e delle procedure di sicurezza in cui sono coinvolti;
- notificare in modo tempestivo alle autorità competenti (vale a dire alle autorità di vigilanza e alle autorità preposte alla protezione dei dati), laddove esistano, in caso di gravi incidenti relativi alla sicurezza dei dati personali trattati.

8.7 Monitoraggio e Controllo degli Amministratori di Sistema

La figura professionale di Amministratore di Sistema (AdS), ha un considerevole impatto di responsabilità sui dati e riveste sul piano operativo un ruolo sostanziale ai fini di un efficace prevenzione dei reati organizzativi.

Alla figura di Amministratore di Sistema è consentito l'accesso ai dati personali contenuti nei sistemi di archiviazione esclusivamente e solo per il tempo necessario per garantire un adeguato funzionamento. Normalmente, restano esclusi dalla definizione di AdS tutti quei soggetti che solo occasionalmente intervengono per manutenzioni o guasti del sistema e delle applicazioni.

La designazione degli AdS, che, a seconda dei casi, è in carico ai Fornitori di tecnologia ed all'Ente, è nominativo e gli estremi identificativi con l'elenco delle funzioni ad essi attribuite, sono riportati in un documento aggiornato e disponibile alla consultazione delle Autorità in caso di accertamenti. Considerando gli incarichi attribuiti e gli ambiti di operatività consentiti secondo il profilo di autorizzazione assegnato, di seguito si riepilogano le principali attività e compiti assegnati:

- operare secondo le prescrizioni di sicurezza e le procedure interne previste;
- amministrare e monitorare l'infrastruttura IT di competenza attraverso l'analisi dei log, identificando e prevenendo potenziali problemi;
- ottenere le migliori prestazioni possibili con le risorse IT a disposizione;
- introdurre ed integrare nuove tecnologie negli ambienti esistenti;
- installare e configurare nuovo hardware/software sia lato client sia lato server;
- applicare le patch e gli aggiornamenti necessari al software di base ed applicativo;
- installare e amministrare sistemi di antimalware;
- organizzare e adempiere allo smaltimento degli strumenti elettronici;
- organizzare e amministrare sistemi di accessi logici per gestire e tenere aggiornati gli account utente ed i relativi profili di autorizzazione;
- disattivare gli account non utilizzati oppure in caso di perdita di qualifica dell'incaricato, secondo le politiche predisposte;
- custodire le copie delle credenziali degli incaricati;
- modificare le configurazioni in base alle esigenze dell'organizzazione;
- fornire risposte alle questioni tecniche sollevate dall'utenza, porre rimedio ai problemi/guasti;
- pianificare e verificare la corretta esecuzione dei backup e delle repliche;
- documentare le operazioni effettuate, le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni ai problemi;
- collaborare con il Titolare, il Responsabile e il DPO al fine di attuare le prescrizioni del Garante e comunicare problemi ed esigenze al Titolare o al Responsabile del trattamento dati;
- confrontarsi con il Responsabile della Protezione dei Dati.

9. RIESAME DELLE POLITICHE DI SICUREZZA

È compito dei servizi competenti in materia di sistemi informativi dell'Ente e dei Fornitori di tecnologie procedere all'adeguamento, alla comunicazione, al riesame e alla verifica delle politiche di sicurezza sopra descritte, ciascuno per quanto di propria pertinenza.

I riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti attinenti alla sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza

complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste da AgID, o a seguito dei risultati delle attività di audit.

Si rimanda alla consultazione delle procedure per la gestione della sicurezza IT adottate:

- dall'Ente, in ottemperanza alla Circolare AGID 2/2017 avente ad oggetto "Misure minime di sicurezza ICT per le P.A.";
- dal Fornitore della piattaforma applicativa di Gestione Documentale.

Firmato digitalmente dal
Dirigente Area Pianificazione Sviluppo

Giovanni Piccolo
03.11.2023 13:25:47
GMT+01:00