Piano della Sicurezza del sistema di gestione informatica dei documenti

Versione	2	Data Versione:	13-11-2026
Descrizione modifiche	Redazione ex novo del documento		
Motivazioni	Adeguamento alle linee guida Agid 2022		
Approvazione	Deliberazione della Giunta camerale n. 113 del 20/11/2026		
Note	Il presente documento è un allegato al Manuale di Gestione documentale		

Sommario

INTRODUZIONE 3
FINALITÀ E AMBITO DI APPLICAZIONE 3
AGGIORNAMENTI DEL DOCUMENTO 4
QUADRO NORMATIVO E STANDARD DI RIFERIMENTO 5
ACRONIMI E DEFINIZIONI 7
INDIVIDUAZIONE DEI DATI PERSONALI 9
CLASSIFICAZIONE DATI E SERVIZI PUBBLICI 11
ORGANIZZAZIONE DELLA SICUREZZA INFORMATICA DEL SISTEMA 11
SICUREZZA ORGANIZZATIVA 13
SICUREZZA FISICA E SICUREZZA LOGICA 19
SICUREZZA DELLE COMUNICAZIONI 27
MONITORAGGIO E CONTROLLO 28
RIFERIMENTI DI SICUREZZA NELL'AMBIENTE DI CONSERVAZIONE DEI DOCUMENTI INFORMATICI 31
SINTESI DEGLI INTERVENTI RELATIVI ALLA PROTEZIONE DEI DATI PERSONALI 32
RIESAME DELLE POLITICHE E PROCEDURE DI SICUREZZA 33

INTRODUZIONE

Il presente documento costituisce un allegato necessario al Manuale di Gestione Documentale, in ottemperanza di quanto previsto dal Codice dell'Amministrazione Digitale (d.Lgs. 82/2005) e finalizzato a definire e sviluppare gli argomenti relativamente agli aspetti che riguardano la gestione informatica dei documenti).

Il documento riporta l'organizzazione delle misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio e l'accesso dei documenti gestiti inclusi nell'utilizzo del servizio applicativo per il protocollo informatico e per la gestione dei flussi documentali, erogati da Piattaforme Applicative di proprietà di InfoCamere, ospitata su Infrastruttura IT presso Datacenter di proprietà di InfoCamere, localizzati a Padova e Milano.

Come descritto nelle sezioni seguenti, l'amministrazione e la manutenzione della Piattaforma Applicativa e della relativa Infrastruttura IT su cui è ospitata, è disciplinata dal sistema di governo della sicurezza delle informazioni del fornitore InfoCamere, mentre la componente locale della sicurezza, (che riguarda, a titolo di esempio la gestione di risorse utilizzate per la fruizione del servizio di gestione informatica dei documenti, del tipo: Postazioni di Lavoro, comportamento degli utenti, rete locale, eec.), sono principalmente disciplinate dal presente Piano e da ulteriori disposizioni interne, in ottemperanza alla normativa vigente ed alle buone pratiche riconosciute.

Per quanto concerne le misure di sicurezza di InfoCamere non espressamente riportate nelle pagine a seguire si rinvia al documento di sintesi delle Politica di Sicurezza pubblicato sul portale di InfoCamere https://www.infocamere.it/certificazioni-e-accreditamenti che costituisce il quadro generale di riferimento delle misure di sicurezza delle informazioni, implementate per assicurare una corretta gestione della sicurezza del servizio digitale erogato.

FINALITÀ E AMBITO DI APPLICAZIONE

Il presente documento descrive il Piano per la Sicurezza del Sistema di Gestione Informatica dei documenti, ai sensi della vigente normativa (il Codice dell'Amministrazione Digitale e regole tecniche di riferimento, in conformità agli standard ed alle normative europee), applicando modelli e linee guida del settore. Fornisce una descrizione delle misure di sicurezza adottate e pianificate per la prevenzione delle minacce e il contrasto agli attacchi, tenendo conto del livello di esposizione al rischio del tipo: furto, perdita, accessi non autorizzati, trattamento non consentito e di qualsiasi altra compromissione di dati, informazioni e di risorse informatiche utilizzate durante la fornitura del servizio di gestione informatica dei documenti.

Considerando che, il patrimonio informativo gestito, regolato e amministrato secondo i principi dell'organizzazione amministrativa in aree, servizi, e uffici, le soluzioni di sicurezza messe in atto, hanno l'obiettivo di:

- mitigare eventi di pericolo che possano compromettere la riservatezza, l'integrità, la disponibilità del patrimonio informativo e la resilienza dei sistemi e dei servizi utilizzato durante il trattamento;
- assicurare la protezione degli interessi dei soggetti pubblici e privati interessati.

Ulteriori vantaggi rappresentano il miglioramento della consapevolezza su aspetti di sicurezza delle informazioni e protezione dei dati e fornire una guida di consultazione accessibile al personale incaricato sulla

organizzazione e gestione della sicurezza del patrimonio informativo trattato, che riprende e integra le misure di sicurezza contenute nei documenti di politiche e piani della sicurezza delle informazioni previsti dai Fornitori di risorse tecnologiche che a vario titolo sono coinvolti nel sistema di gestione informatica dei documenti.

Il Piano per la Sicurezza è orientato sulle seguenti tematiche:

- la competenza e l'affidabilità del fornitore InfoCamere, dell'infrastruttura fisica e logica e le politiche di sicurezza adottate per l'erogazione del servizio digitale di gestione informatica dei documenti;
- la sintesi delle misure di sicurezza adottate internamente;
- il risultato dell'analisi dei rischi a cui sono esposti dati e informazioni trattate, nelle sedi dove sono ospitati i sistemi di elaborazione e archiviazione (fisici e logici) e nei locali dove si usufruisce del servizio digitale;
- le modalità di accesso e l'adeguata disponibilità del servizio di protocollo, di gestione documentale ed archivistico (anche definito "Sistema Gestione Informatica dei documenti");
- i piani di formazione del personale riguardo la sicurezza delle informazioni;
- le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza applicate;
- le modalità di gestione degli incidenti di sicurezza e le attività di ripristino.

AGGIORNAMENTI DEL DOCUMENTO

Il Responsabile del Servizio di Gestione Documentale è responsabile di provvedere, anche considerando il supporto di gruppi specialistici preposti, all'aggiornamento puntuale del medesimo documento ogni qualvolta vengano:

- riviste le strategie organizzative interne;
- introdotte modifiche applicative, funzionali e procedurali con impatti sulla gestione del servizio;
- riviste le politiche di sicurezza dei fornitori coinvolti;
- adeguamenti a standard le normative di riferimento;
- altre motivazioni indicate nella sezione "Riesame delle politiche e procedure di sicurezza".

LIVELLO DI CLASSIFICAZIONE DEL DOCUMENTO

	Livello	**Ambito di diffusione consentito**
	Pubblico	Il documento può essere diffuso all'esterno.
X	Uso interno	Il documento può essere diffuso solo all'interno. È consentito darne comunicazione a terzi solo a seguito della sottoscrizione di una clausola di non diffusione.

		Si raccomanda di non pubblicare il presente documento su siti pubblici.
	Riservato	Il documento non può essere diffuso erga omnes all'interno dell'Amministrazione. La sua visibilità è limitata ad un gruppo ristretto di soggetti autorizzati. L'indicazione "Riservato" dev'essere riportata anche nel Piè-di-pagina del documento

QUADRO NORMATIVO E STANDARD DI RIFERIMENTO

Alla data della presente revisione, di seguito sono riportati le fonti principali di riferimento normativo, regolamenti, standard e linee guida utilizzate per predisporre i contenuti del Piano.

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
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 – *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 2016/679 (GDPR)	General Data Protection Regulation, 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.
Provvedimento del Garante n.32 del 13 febbraio 2020	Parere sullo schema di "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"
Provvedimento del Garante del 27 novembre 2008 e s.m.i.	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema
Provvedimento del Garante n. 393 del 2 luglio 2015	Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche
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
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

** Sono standard di gestione, adottati e mantenuti aggiornati dal fornitore InfoCamere*

ACRONIMI E DEFINIZIONI

Per favorire l'interpretazione di alcune definizioni utilizzate, sono di seguito elencati alcuni acronimi e definizioni generalmente utilizzati.

Termine	Descrizione
Asset informatici	In generale rappresentano qualunque cosa di valore che necessita di essere protetto o salvaguardato. In questo contesto sono tutte le risorse ICT (componenti hw, sw, rete, applicazioni e servizi) tra cui: dispositivi informatici e supporti (fisici e logici), altri apparati, servizi e applicazioni, etc. che trattano il patrimonio informativo digitale
AdS	Amministratore di Sistema. Figura dedicata alla gestione ed alla manutenzione di impianti di elaborazione, compresi sistemi di gestione delle basi di dati, i sistemi software complessi e gli apparati di sicurezza. Resta inteso che, con l'espressione "Amministratore di Sistema" possono individuarsi una pluralità di figure con ruoli e responsabilità ben definite
Audit	Processo di valutazione e verifica (interna o di terze parti)
Backup	Per backup dati si intende la creazione di una copia di sicurezza di dati e informazioni (strutturati e non). Tipicamente i backup servono a ripristinare dati e processi che sono in uso, nel caso si verifichi un'interruzione imprevista e i dati non siano più disponibili o integri
BC	Business Continuity. Tipicamente un processo per affrontare le emergenze e garantire un livello adeguato di servizi
DR	Disaster Recovery. Tipicamente l'insieme di misure tecnologiche ed organizzative (organizzate in un processo) atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi in seguito ad un evento considerato disastroso
DPO	Data Protection Officer

Cybersecurity	Il regolamento (UE) 2019/881 definisce la cybersecurity come l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi interconnessi, gli utenti e altre persone interessate dalle minacce informatiche.
Documento informatico	Il Codice dell'Amministrazione Digitale (CAD - DLgs 82/2005) definisce il documento informatico come "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" in contrapposizione al documento analogico ("rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti"). Il Regolamento eIDAS n. 910/2014 definisce il documento elettronico come "qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva".
Flusso documentale	In generale è il percorso che un documento deve seguire nel suo ciclo di vita. Il governo del flusso consente di controllare tutte le fasi del ciclo, dalla sua creazione/acquisizione fino alla sua archiviazione finale, controllando tutto ciò che sta "nel mezzo": validazione, approvazioni, visti, firme, e includendo la possibilità di visualizzare lo stato degli avanzamenti, degli accessi, altre attività configurabili.
GEDOC	Applicazione di Gestione Documentale, di proprietà di InfoCamere fornita come servizio digitale
GDPR	General Data Protection Regulation
Incidente di sicurezza informatica	Qualsiasi evento o insieme di eventi che sottintendono una compromissione della riservatezza, integrità o disponibilità di dati, sistemi informativi o servizi digitali, che può derivare da attacchi intenzionali (malware, phishing) o errori umani e minacciare la sicurezza dell'Amministrazione

Ingegneria sociale	È la manipolazione delle persone per ottenere informazioni o accessi che compromettano la sicurezza di un individuo o di un'organizzazione. Può essere basata su persone (es. contattare al tel. la vittima per chiedere credenziali, vedere di nascosto password che la vittima digita sulla tastiera, etc.) o basata su computer (es. invio mail false con link a siti fasulli per ottenere credenziali o infettare computer, collocare hw o sw per catturare la tastiera, lo schermo o altre informazioni della vittima, invio di file allegati malevoli via mail per prendere il controllo della macchina della vittima e rubare informazioni o usarla come punto intermedio per attaccare terzi.
Malware	Software dannoso utilizzato per compromettere sistemi informatici
Registro dei rischi	Un documento aggiornato che contiene una descrizione degli eventi di rischio (eventi di minaccia singoli o concatenati), l'impatto (conseguenze) se il rischio si verificasse, la probabilità che si verifichi, le strategie di mitigazione (indicazioni in termini di risorse, processi e tecnologie da mettere in campo per gestire il rischio), i responsabili della gestione del rischio e una classifica per identificare il livello del rischio.
Patching	Attività di aggiornamento consiste nel risolvere: vulnerabilità di sicurezza scoperte nel tempo, problemi che possono insorgere nel normale funzionamento, aggiunte di funzionalità e miglioramenti
Sistema di Gestione Informatica dei documenti	Anche riportato come "Sistema di Gestione Documentale". Rappresenta una categoria di piattaforme applicative utilizzate per organizzare e facilitare la creazione collaborativa di documenti elettronici e di altri contenuti digitali, di proprietà di InfoCamere. Per le pubbliche amministrazioni, costituisce il sistema per la formazione, gestione e conservazione del patrimonio informativo digitale pubblico
Phishing	Tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati riservati o codici di accesso, fingendosi una controparte affidabile in una comunicazione digitale

INDIVIDUAZIONE DEI DATI PERSONALI

La sicurezza informatica si occupa della salvaguardia dei sistemi informatici proteggendo i requisiti di riservatezza, integrità e disponibilità delle informazioni trattate, tematiche a cui è correlato il requisito della privacy, ossia il diritto alla riservatezza delle informazioni personali di cui si è titolari o piuttosto responsabili.

Ai sensi dell'articolo 4 del GDPR, sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica ("interessato") e che possono fornire informazioni sulle sue

caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, culturale e sociale. Come riferimento, sono di seguito indicati le tipologie di dati personali comunemente classificati, tenendo conto che, con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

Dato Personale (art. 4 del GDPR)	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 (art. 4 del GDPR)	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 (art. 9 del GDPR)	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 (art. 9 del GDPR)	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 (art. 9 del GDPR)	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 (art. 10 del GDPR)	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

CLASSIFICAZIONE DATI E SERVIZI PUBBLICI

La classificazione, definita dall'Agenzia per la Cybersicurezza Nazionale e dal Dipartimento per la trasformazione digitale, consente di determinare il livello di criticità dei dati e dei servizi pubblici scegliendo tra strategico, critico e ordinario, sulla base del danno che una loro compromissione, in termini di confidenzialità, integrità e disponibilità, provocherebbe al sistema Paese. Tale classificazione è un requisito fondamentale per tutte le Pubbliche Amministrazioni e rappresenta una delle tre direttrici della Strategia Cloud Italia, insieme alla qualificazione dei servizi cloud e al Polo Strategico Nazionale, a garanzia di efficienza e affidabilità dei servizi e delle infrastrutture.

Seguendo le indicazioni definite dall'Agenzia per la Cybersicurezza Nazionale e utilizzando la piattaforma dedicata, il Responsabile della gestione documentale ha seguito il processo di classificazione dati e servizi, tenendo conto degli elenchi di servizi pre-classificati tra cui "Gestione Documentale" e "Protocollo".

Questa classificazione astrae da specifiche normative e requisiti di sicurezza descrivendo esclusivamente l'impatto per il sistema Paese di una eventuale compromissione di certi dati e servizi.

ORGANIZZAZIONE DELLA SICUREZZA INFORMATICA DEL SISTEMA

L'articolo 51 del CAD, rubricato "*Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni*", prescrive ad AgID, al comma 1, il compito di adottare Linee Guida, ai sensi dell'art. 71 del CAD, al fine di individuare le soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità, la riservatezza dei dati e, da ultimo, anche la continuità operativa dei sistemi e delle infrastrutture.

Lo stesso articolo 51, al comma 2, stabilisce che i documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.

Tutto ciò premesso, obiettivo di sicurezza del patrimonio dei dati digitali dell'Amministrazione è mitigare il rischio di compromettere in modo significativo le caratteristiche di riservatezza, integrità e disponibilità e che include a titolo di esempio: la distruzione accidentale o non autorizzata, la perdita accidentale, l'accesso, la modificazione o la diffusione non autorizzata, nonché di qualsiasi altra forma illecita di trattamento di dati e informazioni.

La sicurezza è implementata mettendo in atto una serie adeguata di misure (di prevenzione, di protezione, di controllo e risposta, di recupero) che comprendono attività tecniche ed organizzative di cui: politiche, procedure, istruzioni e raccomandazioni, definizione di ruoli e responsabilità, strumenti e meccanismi tecnologici di tipo fisico e logico. Tali misure rispondono ai requisiti di sicurezza che possono essere rilevati dall'analisi dei rischi e dai requisiti legislativi e regolamentari di riferimento. Nelle prossime sezioni del documento, con il contribuito di InfoCamere, si descrivono gli elementi per la gestione della sicurezza nei vari ambiti, i soggetti coinvolti, le responsabilità ed ogni altra informazione utile alla gestione e verifica dell'architettura complessiva.

AMBIENTE DELLA GESTIONE INFORMATICA DEI DOCUMENTI

Il sistema è costituito dall'insieme di processi, tecnologie interconnesse presenti presso le infrastrutture on premise o presso sistemi e componenti esternalizzati e dislocati sotto il controllo e la gestione dei Fornitori di tecnologie coinvolti, nonché da tutti i dispositivi e i software presenti presso le varie sedi operative dell'Amministrazione, e utenti che, a diversi livelli, sono coinvolti nell'erogazione e nella fruizione del servizio digitale di gestione del ciclo di vita dei documenti informatici nella fase corrente.

Le soluzioni applicative impiegate per distribuire ed utilizzare il sistema di gestione informatica dei documenti (secondo quando indicato nel Codice dell'Amministrazione Digitale), sono di proprietà di InfoCamere, progettate e realizzate internamente secondo gli standard qualità e di sicurezza, in aderenza alle normative di riferimento tra cui ad esempio, la ISO 9001 e la ISO/IEC 27001 (consulta la pagina (https://www.infocamere.it/certificazioni-e-accreditamenti) e con l'obiettivo di proteggere il documento informatico (atti e fatti giuridicamente rilevanti) nei suoi elementi costitutivi, contribuendo a salvaguardare quelli che sono i requisiti irrinunciabili (di provenienza, contenuto stabile, data certa, identità dell'autore, integrità del documento nella fase corrente), e garantire la funzione probatoria e legale di un documento informatico in ogni fase del suo ciclo di vita.

Le soluzioni sono tipicamente piattaforma applicative, tra cui il Gestore documentale - GEDOC usufruibili da interfaccia web, che consentono l'automazione dell'intero ciclo di vita del documento informatico 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'Amministrazione vengono firmati digitalmente (verificata la necessità di conversione in un formato standard, solitamente un PDF, riconosciuto come standard internazionale, ovvero qualsiasi formato stabilito nel Manuale di Gestione Documentale) 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 del titolare (salvo che questi ne dia prova contraria).

Nel complesso il sistema è progettato per fornire il servizio digitale volto a consentire una gestione efficace e razionale della struttura organizzativa. L'accesso alle funzionalità è stabilito dal ruolo applicativo o dall'insieme di ruoli associati all'utente, i quali si articolano in un insieme di permessi funzionali, in funzione delle specifiche attività che dovranno essere eseguite dall'utente. Per soddisfare eventuali esigenze operative è possibile configurare la creazione di nuovi ruoli, in funzione delle attività che dovranno essere svolte.

Le regole e raccomandazioni sul corretto utilizzo e configurazione di GEDOC, per svolgere in modo adeguato e sicuro le attività di competenza, sono riportate all'interno del Manuale di Gestione Documentale.

VALUTAZIONE DEI RISCHI DI SICUREZZA DIGITALE INERENTI AL SISTEMA

L'Amministrazione è rispettosa di leggi, norme e regolamenti di riferimento ed è in grado di dimostrare, che gli obiettivi di sicurezza digitale definiti siano adeguatamente presidiati. A titolo indicativo sono identificate le seguenti classi di misure d'intervento pianificate ed attuate, approvate e riesaminate periodicamente (per

verificarne l'adeguatezza e l'efficacia) in modo regolare dalle strutture interne preposte, congiuntamente con i fornitori coinvolti.

- Struttura Organizzativa, Politiche di Sicurezza e di Gestione del Rischio documentate;
- Compliance normativa;
- Modalità di Acquisizione, Amministrazione e Configurazione sicura degli Asset;
- Gestione degli Incidenti di sicurezza e di Violazione dei Dati Personali (Data breach);
- Protezione da Malware con sistemi periodicamente aggiornati;
- Meccanismi di backup/ripristino per garantire un'adeguata continuità operativa;
- Protezione dei dati in termini di riservatezza, integrità e disponibilità;
- Monitoraggio e Controllo delle attività;
- Formazione e consapevolezza del personale;
- Sicurezza delle postazioni di lavoro, anche con modalità di lavoro flessibile o decentrato;
- Controllo degli accessi fisici e logici;
- Modifiche apportate alle risorse IT;
- Sviluppo software sicuro;
- Gestione degli aggiornamenti e dell'obsolescenza tecnologica;
- Sicurezza della rete e delle comunicazioni;
- Cancellazione/eliminazione dei dati (in conformità agli obblighi di legge).

L'Allegato 9B del Manuale di Gestione documentale riporta i principali eventi di rischio di minacce che potrebbero manifestarsi, singolarmente oppure in forme avanzate, relativi al processo di formazione e gestione documentale, su cui basare azioni d'intervento in termini di attività tecniche ed organizzative da adottare. Sono identificati gli eventi che, nel verificarsi, possono produrre effetti dannosi rilevanti (in particolare situazioni di incidenti di sicurezza delle informazioni e violazione dei dati personali) e le eventuali principali azioni adottate e/o pianificate per mitigare/contenere eventuali conseguenze negative che coinvolgono diversi aspetti: dalla perdita della capacità operativa al furto di dati, ai costi di contenimento danni, alle implicazioni legali.

SICUREZZA ORGANIZZATIVA

In questa sezione sono descritte le misure pianificate ed attuate al fine di trattare i rischi di sicurezza derivanti da criticità gestionali e operative tra cui: insufficiente formazione e addestramento del personale, mancata o poco chiara attribuzione di responsabilità, mancanza o inefficacia di procedure specifiche, carenza nella comunicazione e nella gestione del rischio, inefficace gestione delle relazioni, altri interventi necessari e raccomandati delle buone pratiche riconosciute nel settore.

DEFINIZIONE DEI RUOLI E DELLE RESPONSABILITA'

Secondo quanto previsto dal quadro normativo di riferimento, il presente Piano di Sicurezza per la gestione informatica dei documenti (considerando le attività di formazione, gestione, trasmissione, interscambio, accesso) è predisposto dal Responsabile della Gestione Documentale d'intesa con il Responsabile della Transizione Digitale sentito il Responsabile della Protezione dei Dati che, qualora richiesto, fornisce consulenza sul trattamento e controllo dei dati personali. In aggiunta, qualora necessario, si richiede il supporto e la collaborazione dei Fornitori di tecnologie, di servizi di sicurezza e di protezione dati, seguendo un approccio di condivisione e suddivisione delle responsabilità, specificando chi fa cosa all'interno del sistema informativo.

InfoCamere, in qualità di Fornitore di infrastruttura IT e piattaforme applicative della soluzione di gestione informatica dei documenti, in ottemperanza alle richieste del Codice dell'Amministrazione Digitale, si impegna a garantire un'adeguata sicurezza delle infrastrutture fisiche e logiche, organizzando sistemi di gestione della sicurezza delle informazioni e della continuità operativa, in aderenza alla legislazione vigente ed agli standard internazionali di riferimento a cui aderisce.

GESTIONE DEGLI UTENTI

Rappresenta una misura non di natura esclusivamente informatica, ma in primo luogo di tipo organizzativo. Una corretta gestione degli accessi permette di limitare l'accesso a determinati dati (tra cui ovviamente anche dati personali) unicamente agli utenti che ne hanno necessità per lo svolgimento delle proprie mansioni lavorative.

Il Responsabile della Gestione Documentale predispone e mantiene aggiornato l'organigramma delle persone autorizzate all'accesso al Sistema informatico di gestione documentale, con le relative abilitazioni disposte mediante un atto oggetto di comunicazione formale.

Il Fornitore di tecnologia InfoCamere, in qualità di Responsabile Esterno al Trattamento, predispone e mantiene aggiornato al proprio interno un elenco di soggetti autorizzati alle operazioni di trattamento sotto la sua autorità: Incaricati al trattamento, Amministratori di Sistema, altre tipologie di utenze che possono essere individuate (ad esempio, altri soggetti esterni autorizzati che effettuano il trattamento dei dati) e tutti inquadrati in base alle attività assegnate.

FORMAZIONE E ADDESTRAMENTO DEL PERSONALE

L'Amministrazione predispone idonea attività formativa per il personale coinvolto nelle fasi del ciclo di vita del documento informatico, nell'ottica di aumentare il livello di consapevolezza del rischio informatico a tutti i livelli, con particolare attenzione alle seguenti tematiche:

- utilizzo adeguato e consapevole dei sistemi informatici (applicativi di gestione documentale, posta elettronica ed altri strumenti informatici), con il supporto dei fornitori di tecnologie;
- sicurezza, privacy e principali rischi inerenti in particolare la violazione dei dati e delle identità digitali;
- organizzazione sicura del lavoro a distanza e modalità di fruizione dei servizi in base ai devices utilizzati;
- organizzazione dei documenti informatici;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative alla gestione documentale;
- comunicazione di incidenti di sicurezza e violazione dati.

La pianificazione di attività formative viene formulata dalla struttura interna preposta, d'intesa con il Responsabile della Gestione Documentale, tenendo conto dei seguenti aspetti:

- analisi dei bisogni formativi;
- programmazione dei percorsi formativi;
- diffusione delle informazioni sui corsi e del relativo materiale illustrativo;
- scelta degli strumenti per la realizzazione degli interventi info-formativi.

CONTINUITA' OPERATIVA DEL SERVIZIO

Come stabilito dall'art. 51 comma 2-quarter del CAD, con l'obiettivo di garantire la continuità operativa del servizio e l'eventuale ripristino tempestivo in caso di incidenti di sicurezza di una certa gravità, sono adottate tutte le iniziative organizzative e tecnologiche volte a ridurre, a un livello ritenuto accettabile, le conseguenze che impattano sull'adeguata disponibilità e resilienza dei servizi digitali inerenti la gestione informatica dei documenti, anche tenendo conto dell'art. 32 del Regolamento UE 2016/679 (GDPR).

In particolare, il Fornitore InfoCamere ha stabilito e mantiene adeguata una struttura gestionale per assicurare la capacità di ripristinare tempestivamente la disponibilità dei servizi e l'accesso dei dati impattati da un incidente, includendo il sistema di gestione informatica dei documenti:

- nell'ambito del Sistema di Gestione della Continuità Operativa di InfoCamere (SGSO), mantenuto adeguato allo standard ISO 22301 di riferimento e sottoposto a periodiche attività di audit;
- nell'ambito della soluzione tecnologica di Disaster Recovery di InfoCamere.

Sono stabilite e mantenute aggiornate le procedure di backup, di ridondanza e di ripristino (a seguito di un incidente di sicurezza) in caso di malfunzionamenti, errori, manomissioni e guasti in generale sui sistemi server e sulle apparecchiature utilizzate per l'erogazione del servizio, e sono pianificati interventi di manutenzione e di monitoraggio, affidate a personale autorizzato ed in linea con le migliori pratiche riconosciute.

Per ulteriori indicazioni, si rimanda alla consultazione della documentazione specifica del Fornitore InfoCamere.

REGISTRO DI EMERGENZA DEL PROTOCOLLO

In casi di indisponibilità, a livello centralizzato del sistema di gestione informatica dei documenti (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 indicato 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 successivamente nel sistema informatico, seguendo le istruzioni del Responsabile del Sistema di Gestione Documentale.

GESTIONE INCIDENTI DI SICUREZZA E VIOLAZIONE DATI PERSONALI

Per "incidente di sicurezza delle informazioni" si intende qualsiasi evento o insieme di eventi che compromette la riservatezza, l'integrità o la disponibilità (c.d. triade RID) di dati, sistemi informativi o servizi digitali, che può derivare da attacchi intenzionali/errori umani e minacciare la sicurezza dell'Amministrazione o, vista la sempre crescente interconnessione, una molteplicità di Amministrazioni pubbliche. Da tale evento possono derivare un insieme di effetti dannosi tra cui la violazione delle politiche di sicurezza informatica e il danno agli asset (beni, sistemi, servizi, dati e informazioni, etc.) per i quali si rende necessaria l'applicazione di misure di contrasto e/o mitigazione da parte delle strutture preposte. Sono esempi di eventi offensivi:

- accesso non autorizzato a servizi e sistemi che supportano il processo di gestione elettronica dei documenti;
- diffusione non autorizzata di informazioni riservate provenienti dagli asset IT;
- impersonificazione di utenti legittimi, tramite la compromissione delle credenziali di autenticazione;
- perdita o modifica non autorizzata delle configurazioni del sistema di gestione informatica;
- interruzione del servizio e di sistemi critici;
- furto di dati, informazioni e di dispositivi

Una sotto-categoria degli incidenti di sicurezza è quella relativa alla compromissione di dati personali, il c.d. "data breach" (violazione dati personali), il quale indica la distruzione, perdita, modifica, divulgazione o accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati. Sono esempi significativi di tale fenomeno:

- l'accesso o l'acquisizione dei dati personali da parte di terze parti non autorizzate;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- la perdita o la distruzione di dati personali a causa di incidenti o eventi avversi;
- la divulgazione non autorizzata dei dati personali.

Al fine di rendere consapevoli tutti gli utenti del comportamento da adottare e dell'elenco dei soggetti da contattare in caso di incidente di sicurezza o del verificarsi di un evento insolito che interessa il sistema di gestione dei documenti informatici, sono attivi piani di formazione e sensibilizzazione.

Normalmente, a seguito del verificarsi di un incidente, la gestione interna segue le seguenti macro fasi, con il supporto di un team di esperti:

- Rilevazione, identificazione e classificazione degli incidenti;
- Gestione degli incidenti e condivisione dei risultati dell'attività svolta (cause individuate, effetti, remediation da mettere in campo);
- Chiusura degli incidenti e registrazione all'interno di un apposito registro.

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 interessate coinvolte tra cui:

- i Titolari e Responsabili del trattamento;
- gli utenti degli aggiornamenti e delle procedure di sicurezza in cui sono coinvolti;
- le autorità competenti (di vigilanza e di protezione dei dati personali), laddove esistano, in caso di gravi incidenti che coinvolgono dati personali.

Nei casi in cui l'incidente consista in una violazione di dati personali e si ritiene significativamente probabile che la violazione dei dati personali presentino effettivamente un rischio per i diritti e le libertà delle persone fisiche, viene segnalato tempestivamente alla struttura preposta che provvede, ove necessario e 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 dai Provvedimenti del Garante privacy, sulla notifica delle violazioni dei dati personali).

TEMPISTICHE E MODALITA' DI GESTIONE DEL FORNITORE DELLE VIOLAZIONI DATI PERSONALI

InfoCamere, in caso di violazione di sicurezza dei dati personali tale da compromettere i diritti e le libertà degli individui, i cui dati sono autorizzati a trattare in qualità di Responsabile del trattamento, agisce secondo quanto prescritto dalla normativa in materia di protezione dei dati personali:

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

Per ulteriori indicazioni, fare riferimento alla specifica documentazione dell'Amministrazione (il rapporto di fornitura sotto il profilo del trattamento dati personali), del Fornitore, alle disposizioni normative in vigore (tra cui il Regolamento UE 2016/679, Provvedimenti del Garante privacy).

SEGNALAZIONI ANOMALIE, RICHIESTE DI ASSISTENZA E DI SUPPORTO

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/o segnalazione incidenti, utilizzando i canali concordati con il Fornitore.

Il processo di intervento adottato a fronte di anomalie riscontrate a seguito del monitoraggio delle funzionalità del Servizio o su segnalazioni di utenti autorizzati, viene condotto secondo quanto indicato nel presente documento e in accordo con eventuali altre indicazioni formalizzate e adottate per le comunicazioni con i Fornitori di tecnologie coinvolti.

L'assistenza ed il supporto tecnico alla piattaforma applicativa che eroga il servizio è gestito da un sistema di gestione centralizzata delle richieste degli utenti adottato e amministrato da InfoCamere che consente una gestione completa delle anomalie, tracciando il mittente, l'incaricato alla risoluzione, le azioni intraprese e lo stato del problema fino alla completa risoluzione.

TEMPISTICHE PER LA PRESA IN CARICO E RISOLUZIONE ANOMALIE

Le tempistiche d'intervento (considerando le fasi di: presa in carico, analisi iniziale, eventuali soluzioni di ripristino) che riguardano la gestione delle segnalazioni di malfunzionamento e le richieste di assistenza e supporto, dipendono dalle priorità assegnate dal Fornitore InfoCamere, dalla criticità rilevata e tenendo conto del livello di servizio erogato e stabilito da InfoCamere, considerando le eventuali disposizioni normative in vigore.

Generalmente, le richieste di assistenza saranno prese in carico dal gruppo preposto (p.e. Contact Center e assistenza tecnica da remoto) durante l'orario lavorativo di erogazione del servizio di gestione informatica dei documenti, secondo quanto comunicato da InfoCamere.

GESTIONE DEI FORNITORI

L'adeguata regolamentazione del rapporto di fornitura aiuta a prevenire problematiche, ma anche a gestire eventuali contenziosi nell'attribuzione delle responsabilità.

L'Amministrazione seleziona e collabora, formalizzando un rapporto di fornitura, con fornitori adeguati nelle attività di gestione informatica dei documenti, i quali s'impegnano a garantire la sicurezza delle proprie infrastrutture ICT e risorse utilizzate per l'erogazione del servizio (tra cui, Data Center, Sistemi, Applicazioni, Servizi, Personale autorizzato), in particolare implementando una politica di sicurezza informatica adeguata, che risponda alle normative di riferimento, agli standard di settore e alle buone pratiche riconosciute dalla comunità di riferimento.

Sotto il profilo del trattamento dati personali, 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, di conseguenza, se previsti sub-fornitori) 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.

Le clausole di utilizzo del servizio di gestione informatica dei documenti sono redatte in conformità ai requisiti ed ai principi previsti in materia di sicurezza dei dati e dei sistemi dal Regolamento (sono esempi gli articoli 32 e 34), con riferimento alle principali vulnerabilità evidenziate nei provvedimenti del Garante e tenendo conto anche dell'attività di notifica delle violazioni dei dati personali di cui all'art. 33 del Regolamento stesso.

INVENTARIO DELLE RISORSE INFORMATICHE

Il censimento e la classificazione delle risorse ICT utilizzate per la gestione informatica dei documenti (asset informatici, tra cui componenti hardware e software, sistemi, servizi e applicazioni), sono informazioni desunte dalla documentazione inerente le attività svolte dall'Amministrazione e dal Fornitore (ogni organizzazione è in possesso delle informazioni sulla propria infrastruttura IT e le mantiene aggiornate).

I criteri di valutazione della criticità delle risorse (in termini di livello di esposizione alle minacce informatiche), tengono conto del livello di rischio di perdita della riservatezza, integrità e disponibilità delle informazioni trattate, dell'aderenza alle normative di riferimento e di altri parametri eventualmente stabiliti.

La gestione delle risorse avviene mediante l'utilizzo di procedure e strumenti che permettono sia un monitoraggio delle stesse per l'erogazione e la fruizione del servizio digitale all'interno dell'Amministrazione, sia l'attività di distribuzione controllata di componenti hardware e software. Sulla base dell'operatività delle attività svolte, si possono suddividere le responsabilità per l'identificazione e gestione degli asset informatici come segue:

- Le Postazioni di Lavoro, software di supporto ed altri dispositivi collegati, sono censiti e amministrati dalla struttura interna preposta;
- InfoCamere identifica e cataloga tutte le risorse informatiche (applicativi, server dedicati, apparati di rete, ed altri dispositivi e software a supporto) necessari ad erogare il servizio digitale, utilizzando un sistema per la gestione amministrativa dell'intero ciclo di vita delle risorse, configurazioni, collegamenti e interdipendenze tra di esse per consentire una corretta configurazione e un adeguato processo di gestione dei cambiamenti.

PROCESSI DI MANUTENZIONE E AGGIORNAMENTO DELLE RISORSE INFORMATICHE

L'Amministrazione controlla che le risorse informatiche di propria competenza siano adeguatamente supportate e che siano effettuati tutti gli aggiornamenti relativi alla sicurezza del sistema in base a processi documentati. I rischi derivanti da risorse informatiche non aggiornate o non più supportate sono valutati e mitigati seguendo le indicazioni dei fornitori di tecnologie e della comunità di riferimento, in un'ottica di condivisione delle informazioni.

A livello di Infrastruttura server ed altri apparati, utilizzati per ospitare ed eseguire le applicazioni che erogano il servizio digitale, le configurazioni di sicurezza e la gestione degli aggiornamenti seguono le indicazioni descritte dalle specifiche procedure previste nel sistema di governo della sicurezza di Infocamere. Tipicamente è previsto un processo che prevede la preparazione di un piano di lavoro basato sulla criticità di funzioni e servizi erogati dalle risorse informatiche nell'ambito server.

A livello di Postazione di Lavoro (i sistemi client da cui il servizio viene fruito), la gestione del ciclo di vita delle risorse informatiche è implementata attraverso strumenti e meccanismi, amministrati dalla struttura di competenza, seguendo le buone pratiche in materia e le politiche specifiche in vigore.

SICUREZZA FISICA E SICUREZZA LOGICA

In questa sezione, sono illustrate le attività messe in atto per trattare i rischi operativi e di sicurezza derivanti da problematiche di tipo tecnologico che incidono tanto la sicurezza fisica quanto la sicurezza logica.

Sono adottate misure, attive e passive, per la sicurezza fisica:

- dei datacenter, localizzati in Italia, che ospitano le infrastrutture ICT utilizzate per realizzare ed erogare il servizio digitale ed archiviare i dati trattati;
- degli ambienti di lavoro dove si fruisce del servizio digitale e si elaborano i documenti.

Sono adottate misure, attive e passive, per la sicurezza logica di:

- identificazione, autenticazione e autorizzazione delle utenze che accedono al sistema;
- installazione e aggiornamento di soluzioni di prevenzione e protezione;
- tracciamento delle attività e monitoraggio, con le registrazioni di operazioni rilevanti che l'utente esegue durante l'utilizzo del servizio.

Le due dimensioni che riguardano gli aspetti di sicurezza tecnica, agiscono in sinergia per implementare un sistema adeguato ed efficace che garantisca la sicurezza del patrimonio informativo digitale.

Nel complesso, la sicurezza fisica rappresenta il primo livello di tale approccio, mentre la sicurezza logica ne rappresenta il successivo.

LOCALIZZAZIONE E SICUREZZA FISICA DELLE INFRASTRUTTURE

L'architettura del Sistema di gestione informatica dei documenti è costituita da risorse informatiche (in generale: beni, componenti e apparati, servizi, applicazioni) ospitate e realizzate su infrastruttura fisica collocata in armadi rack, presso il Data Center primario localizzato a Padova (IT), ed il Data Center secondario localizzato a Milano (IT), utilizzato come sito di Disaster Recovery. Sono attuate misure di sicurezza fisica per proteggere i locali, data center e aree sensibili dall'accesso non autorizzato, da rischi ambientali, da impedimento di svolgimento dei servizi ed altri danneggiamenti.

Nel complesso, sono affidati all'Amministrazione e controllo di InfoCamere le misure di sicurezza fisica e di affidabilità necessarie per proteggere:

- dall'accesso non autorizzato (a titolo di esempio, la vigilanza della sede; l'adozione di sistemi di allarme, sistemi anti intrusione alle finestre, sistemi di riconoscimento del personale, ecc.) e da rischi ambientali i locali, data center e aree sensibili (a titolo di esempio, la predisposizione di locali idonei adibiti ad archivio oppure il ricorso ad armadi chiusi ed ignifughi, ecc.);
- il complesso di server dedicati, dei dispositivi di rete ed altri apparati attivi, cablaggio, alimentazione (energia elettrica protetta, stabile e senza interruzioni), condizionamento (controllo costante della temperatura), impianto antincendio, connettività e collegamenti alla rete sicuri ed affidabili nonché la disponibilità di banda sufficiente.

InfoCamere dispone di un sistema di sicurezza ICT basato su un'analisi del rischio in aderenza alla normativa sulla sicurezza delle informazioni (standard ISO/IEC 27001) ed alle principali pratiche riconosciute a livello internazionale per l'affidabilità e le prestazioni di data center (tra l'altro, il data center di Padova è conforme allo standard ANSI/TIA-942-2017 LEVEL Rating 3).

Le caratteristiche architetturali e tecnologiche dell'infrastruttura ICT e le misure di sicurezza adottate, sia per reagire al concretizzarsi di una minaccia, sia per evidenziare tempestivamente il manifestarsi, sono documentate e mantenute aggiornate da InfoCamere.

Nel complesso, sono affidati all'Amministrazione le misure di sicurezza fisica e di affidabilità necessarie a garantire dei livelli appropriati delle aree dove il servizio viene fruito, ossia la protezione degli ambienti che ospitano il personale autorizzato che opera sul sistema di gestione informatica dei documenti. Si riportano alcune misure minime implementate:

- assicurare la chiusura delle porte di accesso ai locali riservati;
- rafforzamento dei controlli fisici di accesso;
- disponibilità, ove necessario, di un deposito sicuro (per esempio un armadio chiuso a chiave) per archiviare documenti riservati o copie di sicurezza;
- dotazione, ove necessario, di distruggi documenti;
- protezione delle risorse informatiche con adeguati impianti di alimentazione e condizionamento

MANUTENZIONE DELLE INFRASTRUTTURE

Nel complesso, le apparecchiature di supporto e gli impianti sono oggetto di manutenzione programmata e continuativa per garantire la corretta funzionalità ed efficienza. In particolare, è stata definita una procedura operativa per la gestione degli interventi in emergenza e il controllo delle manutenzioni ordinarie / straordinarie finalizzata al ripristino delle apparecchiature di supporto in caso di malfunzionamenti ed all'aggiornamento delle infrastrutture obsolete.

CONFIGURAZIONE SICURA DELLE RISORSE INFORMATICHE

Lo stato della sicurezza e le configurazioni delle postazioni di lavoro, utilizzate per usufruire del servizio di gestione informatica dei documenti, sono gestite secondo le procedure di sicurezza definite, monitorate e attuate dalla struttura preposta.

I sistemi di tipo server e apparati di rete coinvolti nella fornitura del servizio, sono sottoposti ad un processo di configurazione di sicurezza e monitoraggio continuo, seguendo le procedure documentate da InfoCamere, in accordo alle migliori raccomandazioni del settore nel rispetto alla politica di sicurezza delle informazioni adottata. Sono considerati essenziali i seguenti elementi:

- eliminazione dei servizi e dei componenti non necessari;
- costante e tempestivo aggiornamento del sistema operativo e applicazioni, seguendo le indicazioni e i bollettini di sicurezza che rilasciano i fornitori;
- attivazione di meccanismi di raccolta degli eventi;
- scansione regolare delle vulnerabilità note e simulazione di attacchi a componenti critici del sistema;
- policy delle password;
- restrizione degli accessi per collegamenti alla rete ed alle risorse critiche.

IMPOSTAZIONI DI SICUREZZA DELLE POSTAZIONI DI LAVORO E INDICAZIONI SUL COMPORTAMENTO DEGLI UTENTI

Le regole e raccomandazioni sul corretto utilizzo e configurazione degli strumenti di lavoro assegnati agli utenti per svolgere in sicurezza le attività di competenza, sono riportate all'interno di raccomandazioni che sono state comunicate internamente e vengono mantenute aggiornate dall'Ufficio Provveditorato e sistemi informatici. L'uso delle postazioni di lavoro, del software installato e la gestione dei permessi delle utenze, consentono un controllo effettivo sull'uso improprio degli strumenti di lavoro e sul divieto di installare software pericolosi e non affidabili. A scopo generale si riportano di seguito gli orientamenti comunemente riconosciuti e raccomandati:

1. **Aggiornamento delle componenti software necessarie**
2. **Limitazione di utilizzo di dispositivi removibili e connettività**

L'utilizzo improprio di dispositivi removibili non controllabili (ad esempio chiavette USB) può aumentare il rischio di fuga di dati sensibili e riservati, nonché la possibilità di introdurre contenuti malevoli. Compatibilmente alle attività assegnate, non è consentito al personale:

- connettere alla propria postazione di lavoro dispositivi removibili non sicuri e lasciarli incustoditi;
- lasciare accesi ed incustoditi dispositivi che contengono documenti all'esterno degli ambienti lavorativi dell'Amministrazione;
- connettere alla rete (via cavo e senza fili) dispositivi non autorizzati.

3. **Modalità di configurazione delle postazioni di lavoro utilizzate per la gestione dei documenti**

Il Sistema è fruibile come servizio web, con interfacce semplici ed intuitive; le Postazioni di Lavoro ed i sistemi browser approvati devono essere adeguatamente configurati da personale autorizzato, secondo le specifiche tecniche individuate da Infocamere.

4. **Modalità di utilizzo della postazione di lavoro virtualizzata**

Qualora necessario e tenendo conto dei limiti tecnici di applicazione, le attività lavorative possono essere svolte utilizzando le soluzioni di virtualizzazione messe a disposizione dall'Amministrazione.

INDICAZIONI PER UN USO ACCETTABILE DELLE RISORSE INFORMATICHE

Nell'ambito del Sistema di gestione dei documenti informatici, le Postazioni di Lavoro ed altri dispositivi affidati al personale dipendente e collaboratori sono strumenti di lavoro che devono necessariamente essere utilizzati nel modo corretto, seguendo le indicazioni delle politiche e dei Responsabili di riferimento. Ogni impiego delle risorse non conforme alle indicazioni fornite ed alle attività lavorative assegnate può contribuire a provocare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza ed alla protezione dei dati trattati. Tutti gli eventi non intenzionali quali il furto, di danneggiamento, di smarrimento delle dotazioni assegnate o altre situazioni avverse, devono essere tempestivamente segnalati all'Ufficio provveditorato e sistemi informatici.

Per ulteriori indicazioni, fare riferimento alla documentazione in materia opportunamente pubblicata e mantenuta aggiornata

GESTIONE, DISMISSIONE E RIUTILIZZO DELLE RISORSE INFORMATICHE

Con l'obiettivo di garantire un adeguato livello di sicurezza delle risorse informatiche (dispositivi e supporti di elaborazione e memorizzazione, sia fisici che virtuali) che ospitano ed elaborano i documenti informatici, sono stabilite ed applicate procedure ai vari livelli, in base alla responsabilità condivisa tra l'Amministrazione, responsabile degli ambienti client, ed il Fornitore, responsabile degli ambienti server), per monitorare e gestire il ciclo di vita delle risorse informatiche amministrate e garantire che le stesse continuino a soddisfare e a sostenere i requisiti funzionali, di qualità e di sicurezza. Sono stabiliti controlli per verificare se le risorse informatiche sono supportate, in termini di capacità ed obsolescenza, dai loro fornitori e se tutte le patch e gli aggiornamenti pertinenti sono applicati in base a processi definiti.

In particolare la dismissione delle risorse informatiche deve essere gestita in modo sicuro ed organizzato:

- rispettando una procedura definita di disattivazione;
- verificando la presenza di eventuali vincoli (normativi, contrattuali e tecnologici);
- garantendo, se necessario, tutte le adeguate comunicazioni verso le terze parti;
- garantendo, se necessario, la restituzione di tutti i dati al titolare, e fatti salvi diversi accordi e limiti di legge;
- garantendo un corretto e sicuro smaltimento / riutilizzo delle risorse da dismettere, prevedendo, ove necessario, la cancellazione dei dati trattati e la rimozione del software installato (i metodi di cancellazione adottati devono essere coerenti, in termini di livelli di sicurezza garantiti, con i livelli di criticità delle informazioni gestite);
- aggiornando l'inventario delle risorse.

GESTIONE DEGLI ACCESSI

L'obiettivo di questo ambito è garantire l'accesso autorizzato alle informazioni in modo da salvaguardare la riservatezza e prevenire trattamenti non autorizzati, danni e interferenze da parte di utenti che non possiedono i diritti di accesso appropriati.

Sono messe in atto delle procedure formali riguardanti tutte le fasi del ciclo di vita di accesso degli utenti, dalla registrazione iniziale di nuovi utenti per la finale de-registrazione di utenti che non richiedono l'accesso ai sistemi di informazione e servizi. Particolare attenzione viene disposta al controllo dell'assegnazione dei diritti di accesso privilegiato, che consentono agli utenti un accesso permanente ai dati critici/sensibili, l'accesso alle impostazioni di configurazione delle risorse, l'esecuzione di attività rischiose.

L'Amministrazione ha istituito controlli per limitare in modo efficace l'accesso al sistema di gestione informatica dei documenti solo al personale necessario per la prestazione delle attività richieste (seguendo il principio del c.d. need to know), tenendo conto dei seguenti principi:

- metodi di autenticazione commisurati alla criticità dei sistemi informatici;
- minimo privilegio e separazione dei compiti volti ad impedire accessi ingiustificati e aggiramento dei controlli;
- limitazione dei diritti di accesso privilegiato e registrazione dei log degli account in possesso di ampie autorizzazioni per individuare, qualora necessario, le attività svolte e svolgere le relative indagini;
- procedure di approvazione dei diritti di accesso predefiniti (concessione, revoca, modifiche, abilitazione temporanea, rimozione);
- strumenti e istruzioni operative per il controllo degli accessi sono mantenuti adeguati alle esigenze dei servizi offerti ed alle esigenze di sicurezza, tenendo conto delle evoluzioni organizzative e tecnologiche e normative.

Nello specifico, il Sistema di gestione informatica dei documenti è predisposto per il rispetto delle normative vigenti in materia di diritto di accesso, trasparenza e protezione dei dati personali. Il personale può legittimamente accedere (a seconda dei permessi attribuiti) soltanto ai dati e informazioni (in forma di documenti, fascicoli, altro) trattati ed ospitati nel sistema, la cui consultazione sia relativa a procedimenti e attività di propria competenza. La riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita dal Sistema attraverso regole di visibilità gerarchica e attraverso l'uso di profili e credenziali applicative. Le regole di visibilità gerarchica circoscrivono i documenti e i fascicoli cui l'utente può avere accesso a quelli di competenza della UO cui è assegnato e a quelli delle UO gerarchicamente subordinate. 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 vengono riportate alcune regole di configurazione predisposte:

- I documenti non vengono visualizzati dagli utenti privi di diritti di accesso;
- Tipicamente, 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 alla sua unità o agli uffici ad esso subordinati;
- Un utente può avere la visibilità completa sul registro di protocollo, ad eccezione dei protocolli riservati, solo a seguito di specifica abilitazione denominata "Visibilità totale";
- Un utente può avere la visibilità completa sul registro di protocollo, comprensiva dei protocolli riservati, solo a seguito di specifica abilitazione, denominata "SuperUser", richiesta formalmente ad Infocamere;

- Il personale utente dell'unità protocollo generale e altri (se 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 (o la sua ricerca) è possibile solo alla persona destinataria del documento o a chi ha eseguito la registrazione al protocollo generale;
- Solo il Responsabile della Gestione Documentale, o il suo delegato, è abilitato all'uso della funzione di annullamento di una registrazione di protocollo;
- La sessione di lavoro aperta tramite login utente è automaticamente interrotta in casi di inattività superiore al timeout impostato (tipicamente di 30 minuti o comunque configurabile)
- La riservatezza e l'integrità dei dati trasmessi è assicurata dall'uso di funzionalità di cifratura, affidabili e non deprecate, del canale di comunicazione, come indicato nella sezione "Sicurezza delle Comunicazioni".

Per gli utenti che operano in qualità di Amministratori di Sistema (AdS), di cui vale ancora la definizione presente nel provvedimento del Garante del 2008, 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.

Il personale e le terze parti interessate devono essere informati sull'esistenza di una politica specifica per la gestione ed il controllo degli accessi fisici e logici e devono essere vincolati, in funzione delle loro responsabilità o competenze, a rispettare le disposizioni regolamentate.

MODALITA' DI AUTENTICAZIONE

Le identità associate alle persone fisiche e le modalità di accesso al Servizio sono gestite, periodicamente verificate e revocate.

Con riferimento alla gestione delle credenziali applicative, le specifiche politiche che regolamentano le attività dedicate e le tecnologie utilizzate da InfoCamere, risultano idonee a garantire un'adeguata sicurezza al sistema, tenendo conto dei seguenti principi base adottati:

- un singolo account per ogni utente;
- definizione della lunghezza e complessità minima delle password (anche in funzione del sistema a cui si richiede l'accesso e del ruolo ricoperto dall'utente);
- definizione periodo di scadenza della password;
- definizione di un blocco dopo un determinato numero di N tentativi errati;
- registrazione degli accessi;
- policy di conservazione delle registrazioni di accesso per un periodo non inferiore a quanto stabilito dalle disposizioni vigenti.

REGOLE E CRITERI DI ABILITAZIONE

I diritti di accesso e le autorizzazioni sono gestite osservando le indicazioni stabilite dall'organizzazione e consistono 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, il Responsabile della Gestione Documentale amministra e definisce come assegnare le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate dal sistema. I profili di accesso al Servizio ed alle componenti hardware e software utilizzate, sono tipicamente suddivisi nelle seguenti principali categorie:

- Il Responsabile della gestione documentale (e suoi delegati), hanno la visibilità completa di tutti gli oggetti documentali del sistema, ad eccezioni di quelli riservati;
- Gli Utenti che hanno la visibilità per competenza o per conoscenza dei dati, dei documenti e dei fascicoli secondo la struttura organizzativa e le esigenze espresse;
- Gli Amministratori del Sistema, anche considerando la tipologia di attività da svolgere sui componenti hardware, software e di rete utilizzati per erogare il servizio.

Il Sistema consente di tracciare le operazioni svolte, all'occorrenza utilizzabili per svolgere attività di indagini e verifiche.

ACCESSO DI UTENTI ESTERNI

Di regola, ogni qualvolta è necessario consultare uno o più documenti informatici custoditi, dovrà essere compilata apposita richiesta di accesso agli atti, di competenza della struttura preposta e, ove possibile, attuando quanto disposto dall'articolo 64-bis del CAD, rendono fruibili i propri servizi in rete anche in modalità digitale, in conformità alle Linee guida dell'AgID, tramite il punto di accesso telematico.

INDICAZIONI PRINCIPALI SULLE CREDENZIALI DI ACCESSO

Di seguito sono riassunte le principali indicazioni e precauzioni da adottare nella scelta delle password personali (in generale i segreti di autenticazione) e nella loro gestione minima, rimandando alla consultazione del documento interno predisposto ed aggiornato dall' Provveditorato e sistemi informatici.
L'utilizzo e la gestione delle credenziali devono garantire di evitare utilizzi impropri delle password e delle credenziali di autenticazione;

- Le credenziali sono personali e non cedibili, devono essere assegnate in base alla necessità di accedere ai dati o ai sistemi informativi che li trattano e devono essere gestite contemporaneamente alle abilitazioni, sulla base del principio del "minimo privilegio";
- Le password devono essere adeguatamente 'robuste', ovvero lunghe almeno 8 caratteri e costruite in modo da non essere facilmente 'indovinabili' (usare carattere numeri, alfanumerici, speciali) e custodite con cura, nonché variate periodicamente o all'occorrenza;
- 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 operazioni compiute tramite l'utenza è sempre del legittimo titolare, anche se compiute in sua assenza (salvo prova contraria ammissibile).

APPROCCIO ALLA PROTEZIONE CONTRO MALWARE

L'Amministrazione è consapevole che l'utilizzo di sistemi che proteggono da software pericoloso (malware, worm, trojan, virus informatici, etc.) e piani di sensibilizzazione e formazione efficaci possono garantire la sicurezza riducendo l'esposizione agli attacchi anche di tipo avanzato che possono causare danni al sistema informatico, ai processi ed alla reputazione. Pertanto, sono implementate e mantenute aggiornate politiche contro malware ed utilizzati strumenti adeguati.

- La tecnologia utilizzata per la protezione da malware è installata su tutti i dispositivi individuati, siano essi server dedicati ad erogare servizi o postazioni di lavoro dalle quali si accede ai servizi. Nei sistemi su cui è installato, lo strumento di protezione è sempre attivo e la scansione opera in tempo reale su ogni movimentazione di file ed altri oggetti digitali.
- Le componenti che lo richiedono sono periodicamente aggiornate seguendo le indicazioni dei fornitori e, per quanto possibile, in modo centralizzato.
- Viene effettuata un'attenta gestione delle patch volta ad eliminare le vulnerabilità nei sistemi informatici in uso.
- Sono definiti ed attuati processi di backup volti ad isolare i dati dai sistemi di produzione principali e consentire un ripristino veloce e sicuro in caso di un'infezione da malware;
- Viene effettuata una sensibilizzazione del personale sulla modalità di diffusione dei malware nell'ambito dell'ambiente digitale (sono esempi: file infetti, e-mail di phishing, navigazione su siti web non affidabili, etc.), considerando che qualunque sia il tipo di "infezione", le conseguenze possono essere molto diverse (da lievi a estremamente gravi).

Le disposizioni interne messe in atto richiedono di osservare comportamenti e buone pratiche riconosciute, che valgono per tutti gli utenti che utilizzano sistemi per la gestione dei documenti informatici, tra cui:

- Impegno da parte degli utenti a tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante software dannosi;
- Impegno da parte degli utenti di controllare la presenza e il regolare funzionamento del software di protezione installato e se presenti segnali sospetti circa possibili infezioni da malware. In questi casi si raccomanda all'utente di:
    - ➔ sospendere ogni operazione in corso;
    - ➔ segnalare tempestivamente l'accaduto all'Ufficio Provveditorato e sistemi informatici per la corretta gestione e risoluzione.

MISURE PRINCIPALI PER CONTRASTARE ATTACCHI DI SPAMMING E PHISHING

Tipicamente, il sistema di gestione della posta elettronica utilizza meccanismi per la protezione dallo spamming (mailing pubblicitario) con le seguenti principali finalità:

- controllare le informazioni relative alla provenienza dei messaggi eventualmente elaborati ed archiviati nel sistema di gestione;
- 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.

È raccomandato al personale, qualora ritenga che un messaggio ricevuto sia indesiderato, di inviarlo al sistema in modo da aumentare la base di conoscenza per l'individuazione dello spamming.

Le email di phishing sono più rischiose perché riguardano una tipologia di frode che utilizza particolari tecniche di ingegneria sociale (manipolazione delle persone) con lo scopo di entrare in possesso delle credenziali e dei permessi degli utenti così da accedere a documentazione riservata dell'utente e/o dell'Amministrazione.

La migliore difesa contro attacchi di phishing è rendere consapevoli ed informare gli utenti, mediante politiche adeguate e attività formative (es. esercitazioni) a prestare attenzione ogni volta che si riceve un messaggio di richiesta di informazioni personali o riservate, di mail false con link a siti replica di siti legittimi, di file allegati malevoli etc.). Se si riceve questo tipo di messaggio, non fornire le informazioni richieste senza verificare che il destinatario sia legittimo.

Quando si identifica una e-mail come potenziale messaggio di phishing o messaggio sospetto, è necessario spostarla nel cestino e segnalarla alla struttura di competenza.

INDICAZIONI SULLO SVILUPPO SICURO DELLE APPLICAZIONI SOFTWARE

InfoCamere con l'obiettivo di garantire l'adeguata consapevolezza e attuazione degli elementi di sicurezza e di privacy durante le fasi di ciclo di sviluppo delle applicazioni software che interessano la gestione informatica dei documenti, predispone le strutture organizzative, il personale specialistico e le tecnologie adottando buone pratiche, framework e standard di sviluppo sicuro riconosciuti livello internazionale.

Di seguito si riepilogano gli aspetti chiave che vengono considerati durante la progettazione e lo sviluppo di applicazioni e componenti del Sistema di gestione informatica dei documenti:

- specifiche funzionali e tecniche, per una prima valutazione degli impatti sulle componenti hardware e software e la valutazione dei requisiti di sicurezza;
- raccomandazioni internazionali di sviluppo sicuro;
- analisi statiche ed attività di testing del software, a vari livelli;
- organizzazione delle attività e delle responsabilità;
- separazione degli ambienti di sviluppo e di test;
- conservazione sicura del codice sviluppato;
- gestione organizzata della documentazione ed artefatti;
- controllo di accettazione dei rilasci negli ambienti di esercizio;
- esecuzioni periodiche di scansioni vulnerabilità e penetration test.

SICUREZZA DELLE COMUNICAZIONI

Nel contesto delle comunicazioni digitali, viene tenuto in considerazione il fatto che le reti (via cavo e senza fili) interconnettono le risorse informatiche (sistemi, servizi, applicazioni, dati, utenti) utilizzate durante i flussi documentali e processi sia la medesima con il mondo esterno (imprese, cittadini, fornitori, altri enti). L'interconnessione dei sistemi informativi comporta sempre più spesso la mancanza di confini fisici e limiti geografici dello spazio cyber, la cui protezione è necessaria per garantire che le caratteristiche di riservatezza, integrità e disponibilità del patrimonio informativo siano adeguate in ogni momento, anche durante comunicazioni e interazioni, tenendo conto, ai sensi del Codice dell'Amministrazione Digitale, delle raccomandazioni e linee guida di AgID e della continua evoluzione tecnologica.

SICUREZZA NELLA TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI

La trasmissione e l'interscambio di informazioni, documenti e aggregazioni (es. fascicoli informatici) all'interno dell'Amministrazione avviene tramite i seguenti strumenti, che opportunamente presidiati garantiscono di evitare la diffusione non autorizzata ed incontrollata di dati nel rispetto delle normative vigenti:

- sistema di gestione documentale adottato;
- posta ordinaria analogica;
- posta elettronica ordinaria (PEO);
- posta elettronica certificata (PEC);
- sistemi di condivisione sicura (cartelle condivise, utilizzo di canali cifrati, etc.);
- supporti di archiviazione considerati affidabili (es. applicando meccanismi di restrizione accesso e/o tecniche di crittografia riconosciute al volume ed ai dati trasportati) ed autorizzati dalla struttura preposta.

La trasmissione e l'interscambio di informazioni, documenti e aggregazioni (es. fascicoli informatici), ai sensi del Codice dell'Amministrazione Digitale, all'esterno avviene invece tramite:

- funzionalità integrate nel Sistema di gestione informatica dei documenti, se configurato per collegarsi ad una casella PEC istituzionale, consente di ricevere documenti informatici provenienti da altri Enti e Operatori privati;
- la PEC, verificata la necessità della firma digitale e la conversione in un formato standard, solitamente formato PDF affidabile;
- 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 le raccomandazioni e gli schemi previsti da AgID;
- Pubblicazioni con soluzioni web accessibili e sicure;
- trasmissione cartacea dei documenti limitatamente ai casi in cui il destinatario non è obbligato ad essere titolare di casella PEC o nei casi di PEC del destinatario non funzionante.

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 (messaggio e documenti visibili sono agli utenti autorizzati a gestire la casella di posta elettronica).

MONITORAGGIO E CONTROLLO

Per una gestione efficiente del Sistema si pone attenzione al monitoraggio dell'infrastruttura in esercizio, all'applicazione di controlli intelligenti ed impostazione di sistemi di gestione centralizzati che concorrono tutti ad aumentare la disponibilità e la corretta funzionalità agli utenti autorizzati, assicurando livelli di qualità e di sicurezza adeguati, secondo quanto previsto dalle Regole, Linee Guida AgID e tenendo conto delle disposizioni interne.

I Fornitori coinvolti durante l'erogazione del servizio si impegnano al meglio a salvaguardare, mediante un processo di protezione continuo esteso alla manutenzione e al funzionamento dell'infrastruttura sottostante, tutte le componenti fisiche e logiche impiegate, ricorrendo a controlli, 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 informatiche impiegate.

A questo proposito, le segnalazioni sono sottoposte a verifiche del personale autorizzato, incaricato da InfoCamere, in qualità di Fornitore tecnologico del sistema di gestione informatica dei documenti. Le anomalie verranno gestite come indicato nella sezione "Segnalazione anomalie, richieste di assistenza e di supporto" e dagli accordi di servizio aggiornati.

Considerando che molteplici sono i temi rilevanti da considerare in un sistema di monitoraggio adeguato allo scenario di minacce in forte evoluzione che occorre contrastare, tra questi, si riportano di seguito gli aspetti che sono particolarmente importanti da presidiare.

Valutazione dei fornitori

È formalizzato un rapporto di fornitura che regolamenta gli obblighi del fornitore, anche relativamente alla possibilità di svolgere vigilanza e verifiche che l'affidabilità e la solidità sia mantenuta nel tempo.

In particolare, il Fornitore InfoCamere, per garantire il mantenimento della conformità e valutare le prestazioni del sistema, esegue regolarmente:

- audit effettuati da organismi di certificazioni accreditati volti a garantire l'aderenza agli standard internazionali di cui mantiene la certificazione (i certificati a aderenza ai Sistemi di Gestione sono disponibili sulla pagina "*certificazioni*" del portale istituzionale di InfoCamere);
- audit effettuati da personale interno finalizzati a valutare e migliorare l'efficacia e l'efficienza dei processi operativi e di governance;
- verifiche tecniche svolte da personale interno/esterno e basate sulle best practice di settore che comprendono test di intrusione, scansioni di vulnerabilità e penetration test;
- audit specifici di certificazione dei data center.

Quando si identifica una circostanza non conforme, viene eseguito un intervento correttivo e migliorato il processo di gestione. Tutte le attività vengono tracciate, revisionate e riesaminate periodicamente.

Livelli di servizio

Il Fornitore InfoCamere è in grado di garantire degli standard adeguati relativamente ai parametri di qualità, come modalità e tempi di erogazione del servizio. Tali indicatori sono misurabili in qualsiasi momento e riscontrabili nelle statistiche relative ai livelli di efficienza elaborate periodicamente.

Ripristino del servizio

Il Responsabile della Gestione Documentale pone attenzione che le funzionalità del sistema di protocollazione, in caso di guasto o anomalia, siano ripristinate ai sensi dell'art 61 del TUDA DPR 445/2000 e successive modifiche e integrazioni.

Il Fornitore si impegna a garantire la continuità operativa delle infrastrutture (apparecchiature, applicazioni e processi operativi) secondo quando indicato nella sezione "Continuità operativa del servizio".

Segnalazione utenti

InfoCamere rende disponibile un servizio di assistenza al quale il personale autorizzato può accedere attraverso l'apertura di una segnalazione (ticket) per chiedere assistenza e 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, InfoCamere è tenuta 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 l'intervallo concordato all'interno dell'orario di servizio dal lunedì al venerdì.

Infrastrutture che elaborano ed ospitano dati e informazioni

Il Servizio di gestione informatica dei documenti è ospitato su infrastruttura di InfoCamere ed è periodicamente monitorato 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 personale della gestione sistemistica di Infocamere 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 sottostanti.

Registrazione degli eventi di sicurezza

InfoCamere attua 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 digitale.

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 hardware), 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. Ad esempio:

- 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, tenendo conto di garantire la protezione di eventuali dati personali trattati.

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 in vigore (Garante Privacy, GDPR, regolamenti AgID, altre fonti).

Amministratori di Sistema

La figura professionale di Amministratore di Sistema (AdS), ha un considerevole impatto di responsabilità sui dati trattati e riveste sul piano operativo un ruolo sostanziale ai fini di un'efficace prevenzione dei reati informatici. Di conseguenza, il suo operato deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica, volta a controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza, previste da regolamenti interni e dalle norme vigenti.

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. La designazione degli AdS è nominativa 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 richieste ed accertamenti.

Incidenti di sicurezza

Il Fornitore InfoCamere s'impegna al meglio a garantire il monitoraggio, la gestione e la verifica in modo regolare degli incidenti relativi alla sicurezza, comprese le segnalazioni degli utenti su argomenti di sicurezza secondo quanto indicato nella sezione "Gestione incidenti di sicurezza e violazione dei dati personali".

È stabilita e attuata una procedura per la registrazione, classificazione e gestione degli incidenti di sicurezza, qualora necessario anche con il supporto di team specialistici esterni, e in caso di gravi incidenti relativi alla sicurezza dei dati personali, è prevista l'attivazione di un processo di notifica volta a:

- informare gli utenti dell'accaduto e dei possibili impatti sui propri dati, provvedendo a fornire gli opportuni aggiornamenti;
- notificare in modo tempestivo alle autorità competenti (vale a dire alle Autorità di vigilanza e alle Autorità preposte alla protezione dei dati) tramite i canali dedicati l'incidente occorso e gli impatti rilevati sui dati gestiti.

Gli audit log che riguardano l'eventuale compromissione della 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.

In caso di data breach, anche solo sospetto o potenziale, gli utenti sono tenuti a informare tempestivamente con comunicazione scritta l'Ufficio Provveditorato e sistemi informatici e/o il DPO e/o il Responsabile della Gestione Documentale (RGD).

RIFERIMENTI DI SICUREZZA NELL'AMBIENTE DI CONSERVAZIONE DEI DOCUMENTI INFORMATICI

I documenti registrati sul Sistema di gestione informatica dei documenti, sono conformi ai requisiti e contengono i metadati previsti ai fini della conservazione a norma. 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, 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 al sistema di conservazione si rimanda al Manuale di Conservazione di InfoCamere, in qualità di Soggetto Conservatore per la fornitura del servizio di conservazione dei documenti informatici e attualmente pubblicato sul portale AgID di riferimento (https://www.agid.gov.it/).

Sono illustrati 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 dei documenti elettronici.

SINTESI DEGLI INTERVENTI RELATIVI ALLA PROTEZIONE DEI DATI PERSONALI

Con riferimento all'art. 5 del Regolamento UE n. 679/2016 nel quale si afferma che i dati personali devono essere trattati in maniera da garantire "*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»)*", di seguito si riassumono gli impegni e le disposizioni organizzative che l'Amministrazione ed i Fornitori mettono in atto durante la gestione dei documenti informatici.

L'c, in qualità di Titolare del trattamento dei dati personali è responsabile della sicurezza delle proprie risorse e dei sistemi implementati per l'utilizzo del servizio di gestione informatica dei documenti congiuntamente con il Fornitore InfoCamere che, in qualità di Responsabile al Trattamento dei dati personali, mette a disposizione le infrastrutture ICT e risorse necessarie a supportare la protezione di dati personali trattati, adottando i provvedimenti necessari per preservare la loro sicurezza, per impedire che vengano violati, danneggiati o che siano resi disponibili a soggetti terzi non autorizzati.

In particolare, sono applicate e formalizzate le seguenti misure:

- adottare un documento che definisca il modello organizzativo per la gestione degli adempimenti "sistemici" in materia di protezione dei dati e degli interessati;
- procedere ad una puntuale mappatura e classificazione dei trattamenti di dati personali;
- analizzare il rischio e verificare 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;
- nominare i Fornitori quali Responsabili del Trattamento ai sensi dell'art.28 GDPR e controllare l'operato degli stessi.

L'Amministrazione 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 ed in generale durante gestione del ciclo di vita documentale, il sistema di sicurezza adottato 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 di gestione informatica dei documenti è configurato in modo da segmentare la visibilità dei documenti e dei fascicoli (particolari) ai soli dipendenti autorizzati, incaricati del trattamento dei dati.

RIESAME DELLE POLITICHE E PROCEDURE DI SICUREZZA

Le politiche e le procedure di sicurezza sono, a diversi livelli, la definizione delle direttive, delle regole e delle azioni necessarie che il personale e gli utenti devono rispettare. Ciò garantisce la protezione adeguata delle caratteristiche di integrità, disponibilità, riservatezza e di compliance delle infrastrutture informatiche e delle informazioni in esse contenute, in risposta ai diversi rischi a cui è esposto il sistema informativo.

I riesami delle politiche e procedure di sicurezza delle informazioni sono periodici o conseguenti al verificarsi di incidenti relativi alla sicurezza, alla continua evoluzione tecnologica e normativa, o a cambiamenti organizzativi interni. Per i dettagli, si rimanda alla consultazione delle procedure per la gestione della sicurezza delle informazioni e protezione dati personali adottate e rese disponibili alla consultazione dei dipendenti.