CAMERA DI COMMERCIO
INDUSTRIA ARTIGIANATO E AGRICOLTURA
DI TORINO

Piano della sicurezza del sistema di gestione informatica dei documenti

Allegato 5 del Manuale di gestione documentale
approvato con Delibera di Giunta del 26 novembre 2024

Sommario

1. INTRODUZIONE 4
1.1 Scopo e campo di applicazione del documento 4
1.2 Riferimenti normativi 4
1.3 Riferimenti documentali 4
1.4 Termini e definizioni 5
2. ORGANIZZAZIONE SICUREZZA DEL SISTEMA 6
2.1 Ambiti di responsabilità 6
2.2 Coordinamento misure di sicurezza coordinate 6
3. POLITICHE PER LA SICUREZZA INFORMATICA DEI DOCUMENTI 7
3.1 Politica di gestione della sicurezza dei sistemi 7
3.1.1 Inventario degli asset IT 7
3.1.2 Installazione dei sistemi 7
3.1.3 Piano dei fabbisogni IT 7
3.1.4 Configurazione dei sistemi 8
3.1.5 Backup 8
3.1.6 Amministratori di Sistema 8
3.2 Politica per le abilitazioni dell'utenza e per il controllo degli accessi logici 8
3.2.1 Assegnazione, riesame e revoca delle credenziali degli utenti 9
3.2.3 Utilizzo delle password 9
3.2.4 Responsabilità degli utenti 9
3.2.5 Servizi informatici forniti da InfoCamere 10
3.2.6 Esecuzione degli accessi al Sistema 10
3.3 Politica di gestione delle postazioni di lavoro 10
3.3.1 Aggiornamenti del software 10
3.3.2 Limitazione della connettività a supporti esterni 10
3.3.3 Modifica delle impostazioni 11
3.3.4 Configurazione delle postazioni di lavoro 11
3.3.5 Postazioni di lavoro virtuali 11

3.4 Politica di gestione, dismissione e smaltimento degli apparati mobili e dei supporti 11
3.4.1 Gestione apparati e supporti informatici 11
3.4.2 Dismissione apparati e supporti informatici 11
3.4.3 Gestione supporti cartacei 11
3.4.5 Dismissione supporti cartacei 12
3.5 Politica di protezione dal malware 12
3.5.1 Contromisure per la protezione dal malware 12
3.5.2 Contromisure per la protezione dallo spamming 12
3.6 Misure organizzative: scrivania e schermo puliti 13
4. CONTINUITÀ OPERATIVA 13
4.1 Continuità Operativa del Sistema 13
4.2 Continuità Operativa del Servizio 13
5. MONITORAGGIO SERVIZIO 14
5.1 Ripristino del Servizio 14
5.2 Livelli di servizio 14
5.3 Comunicazione con il fornitore InfoCamere 14
6. MONITORAGGIO DELL'INFRASTRUTTURA IT 14
6.1 Procedure operative 14
6.2 Strumenti 14
6.3 Gestione dei log 15
7 ANALISI DEI RISCHI E VALUTAZIONE DI IMPATTO 15
7.1 Contesto e aspetti generali dell'analisi dei rischi 15
7.3 Rischio residuo e formazione 17
8 MISURE DI SICUREZZA: PROCESSO CONTINUO 17

1. INTRODUZIONE

1.1 Scopo e campo di applicazione del documento

Il Piano per la sicurezza informatica del sistema di gestione e conservazione impiegato dall'Ente (nel seguito anche "PIANO") garantisce che:

- i documenti e le informazioni trattati dalla AOO siano resi disponibili, integri e riservati;
- i dati personali comuni e particolari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Il documento costituisce un allegato al Manuale di Gestione Documentale [MANUALE] e al Manuale di Conservazione [MANUALE CONS] dell'Ente, riprendendo e approfondisce i contenuti del paragrafo "Misure di sicurezza" dei suddetti Manuali.

Tenuto conto che il sistema di gestione documentale e il sistema di conservazione dell'Ente è fornito come servizio (SAAS) dal fornitore inhouse InfoCamere, come descritto nel successivo punto 2, il Piano riporta i criteri di sicurezza del sistema tuttavia si focalizza sulle misure di sicurezza di competenza dell'Ente mentre rimanda alla documentazione di sicurezza del fornitore InfoCamere cui è affidata la conservazione dei Documenti Informatici dell'Ente, secondo quanto previsto dalla normativa applicabile alla PA [SCN_IC].

1.2 Riferimenti normativi

Codifica	Descrizione
TESTO UNICO	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
CAD	D.Lgs. 82/2005 - Codice dell'amministrazione digitale
GDPR	Regolamento UE 2016/679 tutela trattamento dati personali e dei diritti delle persone
CODICE PRIVACY	Decreto Legislativo 196/03 e ss.mm.ii.
LINEE GUIDA	AgID - Linee guida sulla formazione, gestione e conservazione dei documenti informatici (determinazione AgID n. 407/2020)

1.3 Riferimenti documentali

Codifica	Descrizione
MANUALE	Manuale di Gestione documentale della Camera di commercio di Torino
MANUALE CONS	Manuale del Sistema di conservazione della Camera di commercio di Torino

POLICY SICUREZZA ICT	Documento interno inerente le Politiche e misure di sicurezza per il trattamento delle informazioni della Camera di commercio di Torino
MISURE MINIME DI SICUREZZA	Documento interno inerente l'attuazione della direttiva AgID sulle misure minime di sicurezza ICT per le pubbliche amministrazioni
TESTO UNICO	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
SCN_IC	Sistema di Conservazione a Norma D.P.C.M. 3/12/2013 di InfoCamere. Rispondente ai "Requisiti di Qualità e Sicurezza" di AGID, presso cui InfoCamere è accreditata quale gestore. Il sistema è Descritto nel Manuale del Sistema di Conservazione di InfoCamere, redatto ai sensi dell'art. 8 del DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis, 23 -ter, comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (di seguito Regole Tecniche). Tale Manuale è pubblicato sul sito dell'AGID.
SGD_IC	Servizio di Gestione Documentale di InfoCamere, erogato alle CCIAA aderenti, in modalità SAAS (software as a service) e in conformità a quanto richiesto dal D.PC.M. 3 dicembre 2013 sul protocollo e dal D.P.C.M. 13 novembre 2014 sui documenti informatici.
ACCREDIA	Ente Italiano di Accreditamento – unico organismo nazionale autorizzato dallo Stato a svolgere attività di accreditamento, ossia l'unico ente riconosciuto in Italia ad attestare che gli organismi di certificazione e ispezione, i laboratori di prova, anche per la sicurezza alimentare, e quelli di taratura abbiano le competenze per valutare la conformità dei prodotti, dei processi e dei sistemi agli standard di riferimento.

1.4 Termini e definizioni

Codifica	Descrizione
AOO	Area Organizzativa Omogenea ovvero l'Ente camerale
Servizio	Servizio di gestione documentale (Gedoc) e servizio per la conservazione dei documenti informatici.
GEDOC	Sistema per la gestione dei flussi documentali (SGD_IC), sviluppato e gestito da InfoCamere e utilizzato via internet/intranet dalle Camere di commercio, come servizio, in modalità SAAS – software as a service.
SCN_IC	Il Servizio InfoCamere per la conservazione dei documenti informatici della Camera di commercio.

Orario di servizio	Intervallo temporale entro il quale è garantita al cliente l'erogazione del "servizio" sulla base di quanto previsto da regolamento con le Camere o da contratti in essere con il Cliente. E' uno degli elementi che concorrono al calcolo dell'indicatore sulla disponibilità del servizio. Al di fuori di tale orario, il sistema è comunque disponibile ai clienti senza garanzia del livello di servizio.
RTO	Tempo massimo di disallineamento dei dati che il servizio di Disaster Recovery garantisce in caso di disastro.
RPO	Tempo in cui la soluzione di Disaster Recovery garantisce il ripristino della disponibilità dei servizi in caso di disastro.
DPIA	Data protection Impact Assessment
CNIL	Commission nationale de l'informatique et des libertés

2. ORGANIZZAZIONE SICUREZZA DEL SISTEMA

2.1 Ambiti di responsabilità

L'ambiente del ciclo di vita dei documenti informatici della Camera di commercio di Torino comprende sia l'ambito camerale, per gli aspetti di produzione/gestione, sia quello del fornitore InfoCamere, responsabile delle attività di conservazione.

La sicurezza complessiva del sistema di gestione e conservazione, pertanto, è garantita dall'insieme delle misure di sicurezza adottate dall'Ente produttore e dal Soggetto conservatore, per i propri ambiti di responsabilità, come sintetizzato dallo schema di fig.1.

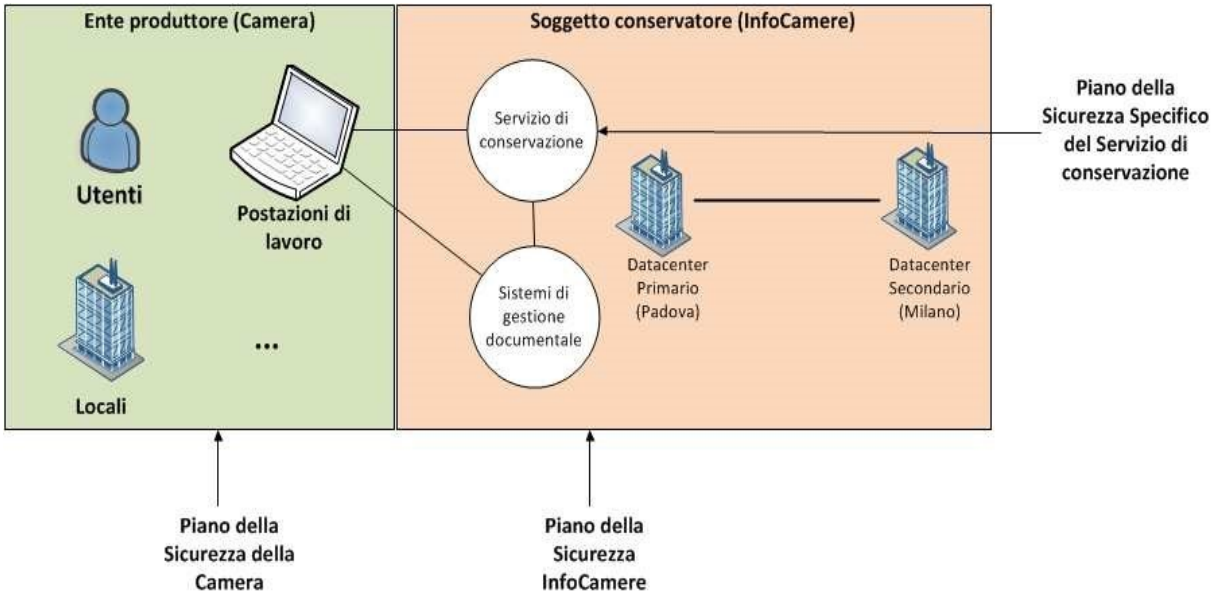


Fig. 1 – Ambiti di responsabilità

2.2 Coordinamento misure di sicurezza coordinate

Il presente documento descrive la policy di sicurezza del sistema di gestione e conservazione, che necessariamente focalizza maggiori dettagli sulla componente

tecnologica e organizzativa dell'Ente mentre rimanda alla documentazione del fornitore InfoCamere per quanto di sua competenza.

3. POLITICHE PER LA SICUREZZA INFORMATICA DEI DOCUMENTI

3.1 Politica di gestione della sicurezza dei sistemi

Tenuto conto dei diversi ambiti di responsabilità (vedi punto 2.1), le politiche e le misure di sicurezza descritte nel presente paragrafo riguardano essenzialmente l'infrastruttura IT gestita dall'Ente, anche se alcuni aspetti dei servizi di gestione informatica del soggetto produttore sono condivisi con il fornitore, mentre per quanto di diretta competenza di InfoCamere si rimanda alle policy del fornitore.

Per i dettagli delle misure di sicurezza informatica si rimanda al documento "Politiche e misure di sicurezza delle informazioni" dell'Ente.

3.1.1 Inventario degli asset IT

Gli asset associati ad informazioni e a strutture di elaborazione delle informazioni sono identificati; un inventario di questi asset deve essere pubblicato e mantenuto aggiornato.

Gli asset vengono censiti, catalogati e valutati in relazione alla loro importanza per il business; sono quindi assegnati ad un responsabile.

La valutazione viene fatta in base al valore, alle normative cui sono assoggettati, ai requisiti di riservatezza, integrità e disponibilità, alla criticità per l'organizzazione.

3.1.2 Installazione dei sistemi

L'integrità dei sistemi di produzione è un requisito di sicurezza essenziale; pertanto, vengono attuate procedure per controllare l'installazione del software sui sistemi di produzione (postazioni di lavoro).

I sistemi ritenuti critici, come dispositivi di rete, sistemi e pc contenenti informazioni critiche per la sicurezza informatica, devono essere protetti dall'accesso logico e fisico non autorizzato.

Sono inoltre stabilite e attuate regole (limitazioni) per il governo dell'installazione del software da parte degli utenti.

- Cambiamento. Le modifiche alle componenti di software applicativo, hardware e software di sistema sono gestite applicando, a seconda dei casi, dei processi di governo del cambiamento relativi alla pianificazione, progettazione, sviluppo, test e rilascio delle nuove funzionalità o di quelle modificate, includendo gli opportuni passi di verifica ed autorizzazione.
- Documentazione. I cambiamenti apportati all'infrastruttura IT vengono periodicamente opportunamente aggiornati e documentati.

3.1.3 Piano dei fabbisogni IT

Per poter garantire che l'infrastruttura tecnologica dell'Ente sia in grado di soddisfare i livelli di servizio richiesti, tutte le componenti hardware e software vengono tenute sotto controllo; vengono inoltre svolte previsioni sui futuri requisiti di capacità per assicurare le prestazioni di sistema richieste.

Il Processo è strutturato nelle seguenti fasi:

- analizzare i piani aziendali a breve e lungo termine
- osservare l'attuale performance di ciascuna componente coinvolta, identificando ogni collo di bottiglia e verificando il carico di lavoro attuale e la sua evoluzione prevista per il futuro
- valutare la crescita del carico di lavoro nel tempo
- avviare l'eventuale attività di approvvigionamento delle risorse in esame.

3.1.4 Configurazione dei sistemi

Nel tempo deve essere mantenuto un modello dell'infrastruttura IT attraverso l'identificazione, il controllo, la manutenzione ed il "versionamento" delle informazioni di configurazione; tali informazioni vanno gestite in un apposito archivio.

3.1.5 Backup

Infocamere si occupa di effettuare copie di backup delle informazioni, del software e delle immagini dei sistemi; le copie vengono sottoposte a test periodici di restore.

Il Processo che regola l'esecuzione del backup garantisce che la modalità di salvataggio sia selezionata in base ai parametri: tipologia del dato (dato di produzione / non produzione, dato strutturato / non strutturato), frequenza, ubicazione copie, periodo di *retention*, supporto fisico, ambiente tecnologico.

Le copie di *backup* dei dati di produzione sono replicate nel datacenter secondario (Disaster Recovery).

3.1.6 Amministratori di Sistema

Devono essere minimizzati i rischi di:

- violazione alla compliance relativa agli Amministratori di Sistema
- danneggiamento di dati e sistemi informatici derivanti da accessi non autorizzati o non adeguatamente controllati ai sistemi ed alle applicazioni da parte dei medesimi Amministratori.

La nomina degli Amministratori di Sistema viene effettuata, da parte dei Responsabili delle competenti strutture aziendali, previa una attenta valutazione delle caratteristiche soggettive, ovvero: è necessaria una valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza. Inoltre, la designazione quale Amministratore di Sistema deve essere in ogni caso individuale e deve recare l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, sono riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti, anche da parte del Garante della Privacy.

L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

3.2 Politica per le abilitazioni dell'utenza e per il controllo degli accessi logici

La politica per il controllo degli accessi logici definita nel documento sulle Misure minime di sicurezza e nelle lettere di incarico per il trattamento dati (Codice Privacy) si applica anche al caso specifico ai Servizi di gestione documentale e di conservazione; pertanto anche in tale ambito si deve limitare l'accesso alle informazioni ed ai servizi di elaborazione delle informazioni ai cosiddetti "need to access" ovvero alle effettive e legittime necessità operative, è considerato obiettivo fondamentale della Sicurezza delle Informazioni nell'Ente.

Tutto il personale dell'Ente e le terze parti interessate sono informati sulla esistenza di una Politica specifica per la gestione ed il controllo degli accessi logici alle risorse e sono vincolati, in dipendenza delle loro responsabilità o competenze, a rispettarne le prescrizioni.

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

3.2.1 Assegnazione, riesame e revoca delle credenziali degli utenti

Riguardo ai Servizi di Gestione e Conservazione documentale:

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

L'attuazione del processo organizzativo è di responsabilità delle figure designate dall'Ente; le relative richieste sono effettuate a InfoCamere che provvedono, tramite gli opportuni strumenti tecnici, a soddisfarle e a fornire il relativo riscontro ai richiedenti.

3.2.3 Utilizzo delle password

Riguardo ai Servizi di Gestione e Conservazione documentale:

- L'utilizzo e la gestione delle credenziali devono garantire di evitare utilizzi impropri delle password e delle credenziali di autenticazione.
- Le regole relative alla costruzione ed utilizzo delle password si applicano a tutto il personale e terze parti che ne fanno uso per accedere agli asset dell'Ente.
- L'utilizzo delle password ed in genere delle credenziali utente viene controllato con un processo di gestione automatizzato, fin dove possibile, al fine di assicurare una corretta gestione delle password (scadenza password, criteri di complessità, aging delle password, etc...)
- Le credenziali sono personali e non cedibili, devono essere assegnate in base alla necessità di accedere ai dati o ai sistemi aziendali e devono essere gestite contemporaneamente alle abilitazioni, sulla base del principio del "minimo privilegio".
- Le password devono essere 'robuste', ovvero costruite in modo da non essere facilmente 'indovinabili' (password guessing) e custodite con cura, nonché variate periodicamente.
- Analoghe regole valgono per i cosiddetti PIN dei dispositivi con a bordo certificati digitali (smart card, token usb wirelwss, etc.).

3.2.4 Responsabilità degli utenti

Le credenziali sono personali e non cedibili. Ogni utente è responsabile della corretta gestione della propria password, dei dispositivi di riconoscimento, delle informazioni per l'accesso ai sistemi e ai dati.

Le credenziali e i dispositivi di riconoscimento devono essere conservati adeguatamente e non essere mai lasciati incustoditi.

La responsabilità delle azioni compiute nella fruizione dei Servizi di gestione documentale e di conservazione è dell'utente fruitore del servizio.

La responsabilità delle operazioni compiute tramite un'utenza è sempre del legittimo titolare, anche se compiute in sua assenza.

3.2.5 Servizi informatici forniti da InfoCamere

I processi organizzativi e la strumentazione tecnica utilizzata da InfoCamere per la gestione delle richieste dell'Ente relative alle credenziali di accesso al Sistema sono coerenti con la politica ed i processi dell'Ente.

La strumentazione tecnica utilizzata da InfoCamere per la gestione delle password di accesso ai servizi forniti è coerente con la politica dell'Ente in quanto:

- I sistemi di gestione delle password sono interattivi e assicurano password di qualità.
- I sistemi di autenticazione impongono il rispetto della password policy.

3.2.6 Esecuzione degli accessi al Sistema

I Sistemi di Gestione e Conservazione documentale, realizzati su infrastruttura IT di InfoCamere e da questa gestiti, sono dotati di:

- Procedure di log-on sicure. L'accesso a sistemi e applicazioni è controllato da procedure di log-on sicure.
- Controllo degli accessi alle applicazioni ed alle informazioni. L'accesso alle informazioni ed alle funzionalità dei sistemi applicativi da parte degli utenti e del personale di supporto è progettato e realizzato in base al principio di necessità.
- Password di accesso. La strumentazione tecnica utilizzata da InfoCamere per la gestione delle password di accesso ai servizi forniti è coerente con la politica.

3.3 Politica di gestione delle postazioni di lavoro

La politica definita nel documento sulle Misure minime di sicurezza e nelle lettere di incarico per il trattamento dati (Codice Privacy) si applica anche al caso specifico dei Servizi di gestione e conservazione documentale; pertanto, devono essere rispettate le regole descritte nei seguenti punti.

3.3.1 Aggiornamenti del software

- L'Ente mantiene adeguato il livello di aggiornamento del software installato sulle postazioni di lavoro.
- Il personale non deve inibire gli eventuali strumenti di aggiornamento automatico o centralizzato previsti dall'Ente.

3.3.2 Limitazione della connettività a supporti esterni

L'utilizzo improprio di dispositivi rimovibili può aumentare il rischio di fuga di dati riservati aziendali; pertanto, il personale:

- non deve consentire ad altro personale il collegamento di dispostivi rimovibili alla propria postazione;
- non deve connettere alla propria postazione dispositivi rimovibili e lasciarli incustoditi - non deve lasciare incustodito il dispositivo all'esterno del perimetro aziendale.

3.3.3 Modifica delle impostazioni

Il personale ha la responsabilità di non modificare le configurazioni standard (sia software che hardware) impostate al momento dell'installazione iniziale nelle postazioni di lavoro, dispositivi mobili o supporti rimovibili affidati in dotazione individuale, senza specifica autorizzazione delle funzioni di sicurezza.

3.3.4 Configurazione delle postazioni di lavoro

Il sistema di gestione documentale, lato utente, è reso disponibile in modalità di navigazione web tramite browser di ultima generazione; le postazioni di lavoro ed i browser sono pertanto configurati secondo le specifiche tecniche fornite e aggiornate da InfoCamere.

3.3.5 Postazioni di lavoro virtuali

Quale elemento primario per la razionalizzazione delle risorse strumentali, progressiva riduzione delle spese di esercizio ed incremento delle caratteristiche di sicurezza, viene previsto l'utilizzo delle tecnologie di virtualizzazione del desktop, sia in modo permanente (lavoro remoto) che occasionale (smart working).

3.4 Politica di gestione, dismissione e smaltimento degli apparati mobili e dei supporti

La politica definita nel documento sulle Misure minime di sicurezza e nelle lettere di incarico per il trattamento dati (Codice Privacy) si applica anche al caso specifico dei Servizi di gestione e conservazione documentale; pertanto, devono essere rispettate le regole dei punti seguenti.

3.4.1 Gestione apparati e supporti informatici

Gli apparati e i supporti informatici sono protetti da accessi non autorizzati, utilizzi impropri, manomissioni, danneggiamento o furti:

- durante il loro utilizzo all'interno e all'esterno delle sedi dell'Ente;
- durante il trasporto;
- durante i periodi di inattività.

Riguardo alle postazioni di lavoro mobili, in genere, sono assegnate personalmente al dipendente; in alcuni casi possono essere assegnate ad un responsabile di struttura ed utilizzate dal personale ad essa afferente.

Tale personale è autorizzato a portare con sé al di fuori delle sedi dell'Ente gli apparati mobili assegnati e avendo ricevuto esplicite avvertenze sui comportamenti tesi a prevenire furti e/o danneggiamenti.

La memorizzazione di dati personali non aziendali da parte del personale su apparati mobili non è ammessa a meno di esplicita autorizzazione da parte dell'Ente.

3.4.2 Dismissione apparati e supporti informatici

Tutti gli apparati e i supporti informatici vengono controllati per assicurare che ogni dato critico sia rimosso e distrutto in modo sicuro prima della dismissione o del riutilizzo.

3.4.3 Gestione supporti cartacei

In generale le informazioni eventualmente presenti sui supporti cartacei (documenti, appunti) non dovrebbero mai essere lasciate dal personale in luoghi al di fuori del proprio controllo.

Nello specifico le informazioni rilevanti o riservate presenti sui supporti cartacei non devono mai essere lasciate dal personale al di fuori del proprio controllo.

Sulle scrivanie degli uffici, sui tavoli delle sale riunioni, o in altri luoghi, al termine del lavoro o al termine delle riunioni non deve essere lasciata documentazione riservata.

Sui dispositivi di stampa, fotocopia, acquisizione ottica delle immagini e nelle loro vicinanze non deve essere lasciata documentazione riservata. Sono previste, e messe a disposizione del personale, modalità di stampa protetta per le stampanti multifunzione condivise.

A maggior ragione la documentazione riservata deve essere gestita con particolare cura all'esterno delle sedi dell'Ente.

3.4.5 Dismissione supporti cartacei

Le informazioni rilevanti o riservate presenti sui supporti cartacei che non si intende più utilizzare, devono essere distrutte o rese non consultabili.

Nel caso di cessato utilizzo di documenti cartacei riservati, essi devono essere distrutti con gli appositi apparecchi messi a disposizione del dipendente.

3.5 Politica di protezione dal malware

La politica definita nel documento sulle Misure minime di sicurezza e nelle lettere di incarico per il trattamento dati (Codice Privacy) si applica anche al caso specifico dei Servizi di gestione e conservazione documentale; pertanto, devono essere rispettate le seguenti regole:

- Le informazioni di proprietà dell'Ente o da essa gestite e le infrastrutture IT preposte alla loro elaborazione sono protette contro il malware.
- Sono previsti ed attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware.
- Attraverso specifica formazione e\o informazione viene assicurata la diffusione di consapevolezza degli utenti per prevenire le minacce e le vulnerabilità derivanti dal malware.

3.5.1 Contromisure per la protezione dal malware

La strumentazione software per la protezione dal malware (c.d. antivirus) è installata su tutte gli apparati dell'Ente con sistema operativo Microsoft e Linux, siano essi server dedicati ad erogare servizi oppure postazioni di lavoro dalle quali l'utente accede ai servizi.

L'antivirus è installato sia sui sistemi fisici (server, personal computer) che virtuali utilizzati dall'Ente.

Nei sistemi "endpoint" su cui è installato, l'antivirus è sempre attivo e la scansione opera in tempo reale su ogni movimentazione di file, oltre ad un'analisi del comportamento, proteggendo così l'apparato dal malware.

Le componenti sopra descritte sono periodicamente aggiornate per assicurare adeguate misure di protezione.

3.5.2 Contromisure per la protezione dallo spamming

I sistemi che gestiscono la posta elettronica utilizzano una strumentazione software per la protezione dallo spamming; le finalità della strumentazione sono:

- controllare le informazioni di provenienza dei messaggi
- a seconda della correttezza di tali informazioni, eliminare, inserire in quarantena o consegnare i messaggi al destinatario
- eliminare dai messaggi ricevuti eventuali software, codice o collegamenti malevoli in essi contenuti
- mettere a disposizione dei destinatari l'elenco dei messaggi inseriti in quarantena.

Il personale dell'Ente, qualora ritenga che un messaggio ricevuto sia indesiderato, lo può inviare al sistema che aumenta così la base di conoscenza per l'individuazione dello spamming.

Le componenti sopra descritte sono periodicamente aggiornate per assicurare adeguate misure di protezione.

3.6 Misure organizzative: scrivania e schermo puliti

La politica definita nel documento sulle Misure minime di sicurezza e nelle lettere di incarico per il trattamento dati (Codice Privacy) si applica anche al caso specifico del Servizio di Gestione Documentale.

Pertanto, devono essere adottate e rispettate le politiche di "scrivania pulita" per i documenti ed i supporti di memorizzazione rimovibili e di "schermo pulito" per i servizi di elaborazione delle informazioni.

Le regole di “scrivania pulita” sono essenziali per proteggere le informazioni su supporto cartaceo e su supporti rimovibili di memorizzazione:

- *scrivania pulita* Al termine del lavoro o durante lunghe pause, sulle scrivanie non deve essere lasciata alcuna documentazione riservata cartacea o su supporti rimovibili.
- *schermo pulito* Non lasciare accessibile la postazione di lavoro durante la propria assenza: bloccarla, prevedendo lo sblocco con password e attivare comunque un “screensaver” automatico protetto da password che pulisca la videata entro alcuni minuti (almeno 5) in caso di inutilizzo.

Sullo schermo della postazione, anche durante lo svolgimento della propria attività, non devono essere facilmente visibili o accessibili informazioni riservate ma inutili per la corrente sessione di lavoro (ad esempio: lasciare aperto inutilmente un documento contenente informazioni sensibili, che possono essere inopportunamente lette da terzi durante o alla ripresa della sessione).

Tali regole sono essenziali per proteggere tutti gli apparati di elaborazione delle informazioni sia in utilizzo individuale (postazioni di lavoro) sia condiviso (console di sistemi di controllo, server, cartelle di rete, etc.).

Le regole devono essere rispettate dal personale dell’Ente, dai fornitori e dalle terze parti.

4. CONTINUITÀ OPERATIVA

4.1 Continuità Operativa del Sistema

Poiché il Sistema di Gestione e Conservazione Documentale è ospitato sull’infrastruttura IT di InfoCamere, il Sistema di Gestione Documentale è inserito nell’ambito del Sistema di Gestione della Continuità Operativa e di Disaster Recovery di InfoCamere; tale soluzione è dotata di una infrastruttura tecnologica dedicata e delle necessarie caratteristiche di ridondanza geografica.

La soluzione di Disaster Recovery di InfoCamere garantisce un tempo massimo di disallineamento dei dati (RPO) di 24 ore ed il ripristino della disponibilità (RTO) dei servizi che InfoCamere eroga in outsourcing all’Ente entro 72 ore dal disastro.

4.2 Continuità Operativa del Servizio

In caso di disastro ambientale, essendo le sedi camerali a breve distanza fra esse, e quindi soggetti a rischi analoghi, l'Ente valuterà l'opportunità di eventuali spostamenti del personale in altre sedi (non camerali), tenendo comunque in considerazione che le dotazioni di dispositivi mobili e l'architettura di rete possono offrire soluzioni alternative efficaci, quali lavoro remoto e smart working.

In caso di fermi prolungati di altra natura (quali danneggiamento o prolungata assenza di alimentazione elettrica), l'Ente valuterà l'opportunità di uno spostamento di personale tra le sedi camerali disponibili, sfruttando la flessibilità e ridondanza degli impianti di trasmissione dati e delle postazioni.

Se un evento disastroso (naturale o doloso) impattasse solo sulla sede di Palazzo Affari, sede del nodo provinciale della rete geografica InfoCamere, l'Ente potrà valutare di

assicurare, anche se in misura contenuta e limitata alle attività prioritarie, la continuità del servizio di protocollazione attraverso soluzioni mobili e di virtualizzazione.

5. MONITORAGGIO SERVIZIO

5.1 Ripristino del Servizio

Il Responsabile del Servizi di Gestione documentale, ovvero il soggetto che mantiene i sistemi di gestione e conservazione, cura che le funzionalità dei Sistemi, in caso di guasto o anomalia, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile [art. 61, comma 3 del TESTO UNICO].

5.2 Livelli di servizio

In coerenza con il paragrafo precedente, InfoCamere garantisce che i Servizi siano erogati con i seguenti livelli di servizio:

Orario di servizio:	08:00 – 21:00 lunedì – venerdì 08:00 – 14:00 sabato
Disponibilità del servizio:	migliore del 99%
RTO:	72 ore
RPO:	24 ore

5.3 Comunicazione con il fornitore InfoCamere

InfoCamere rende disponibile uno specifico servizio di assistenza al quale il personale dell'Ente può accedere attraverso l'apertura di una segnalazione (ticket) per chiedere la risoluzione di eventuali anomalie emerse durante la fruizione del servizio.

In caso d'anomalia o malfunzionamento del Servizio, InfoCamere è tenuta a comunicare il problema riscontrato al Responsabile del Servizio; la comunicazione deve essere effettuata (anche tramite email) entro due ore all'interno dell'orario di servizio dal lunedì al venerdì.

6. MONITORAGGIO DELL'INFRASTRUTTURA IT

I Sistemi di gestione e conservazione documentale sono ospitati su infrastruttura IT di InfoCamere, la quale li mantiene sotto controllo tramite i processi e gli strumenti descritti nei punti seguenti.

6.1 Procedure operative

La procedura di Operation & Event Management di InfoCamere:

- assicura il monitoraggio ed il controllo del corretto funzionamento dell'infrastruttura IT del Sistema di Gestione Documentale
- descrive le attività necessarie affinché ai sistemi ed alle procedure applicative siano rese disponibili le risorse necessarie al corretto funzionamento - è focalizzata al supporto 24 ore x 365 giorni all'anno.

6.2 Strumenti

La strumentazione per il monitoraggio infrastrutturale del servizio erogato da InfoCamere è essenzialmente costituita dalle componenti:

- sonde di rilevazione

- registrazione degli eventi
- console
- segnalazioni generate automaticamente.

6.3 Gestione dei log

InfoCamere mantiene sotto controllo gli eventi anomali legati a:

- malfunzionamenti
- performance

registrandoli ai fini di:

- riesame
- audit.

I log sono classificati nelle tipologie:

- log infrastrutturali: riguardano le componenti software (acquisite da fornitori) e i sistemi hardware che compongono l'infrastruttura IT
- log applicativi: riguardano le applicazioni software (sviluppate da InfoCamere) con rilevanza dal punto di vista di monitoraggio delle funzionalità.

A seconda della tipologia dei log e della loro importanza, sono definite appropriate modalità di registrazione, accesso, archiviazione e cancellazione.

7 ANALISI DEI RISCHI E VALUTAZIONE DI IMPATTO

A seguito di una significativa evoluzione organizzativa - attività lavorative da remoto e in mobilità (lavoro agile e smart working) - e dai mutati scenari di cybersecurity nazionali e internazionali, in attuazione dei principi generali della gestione della sicurezza, nel secondo semestre del 2024 è stata condotta internamente una nuova analisi dei rischi e valutazione di impatto con riferimento al sistema di gestione informatica dei documenti.

La valutazione d'impatto è stata condotta seguendo la metodologia implementata dall'applicazione opensource messa a disposizione dal CNIL (Commission nationale de l'informatique et des libertés) per le DPIA (Data protection Impact Assessment).

Tale applicazione è utilizzata dall'ente anche per le valutazioni di impatto sui sistemi ritenuti maggiormente critici per l'ente e/o quelle per cui la DPIA è richiesta da specifica normativa di riferimento.

7.1 Contesto e aspetti generali dell'analisi dei rischi

Sono stati analizzati il contesto generale e gli aspetti fondamentali del trattamento dei dati per il sistema di gestione e conservazione dei documenti dell'ente, oltre che analizzati i dati e i processi organizzativi e gestionali coinvolti.

La valutazione d'impatto e l'analisi dei rischi è stata focalizzata su:

- accesso illegittimo ai dati/documenti/informazioni
- modifiche indesiderate
- perdita dei dati mettendoli

e mettendoli in relazione con tutte le misure di sicurezza (fisiche, organizzative e tecniche) attuate per la mitigazione del rischio.

È stato preso in considerazione l'intero asset di risorse ICT coinvolto nei processi di gestione documentale e le relative misure a tutela dei diritti degli interessati che vanno garantiti come previsto dal regolamento europeo sulla protezione dei dati e normativa territoriale vigente (GDPR).

In particolare, con riferimento al modello organizzativo della sicurezza del sistema di gestione documentale (punto 2.1), l'analisi di rischio sulle risorse di competenza dell'Ente è stata effettuata tenuto conto che:

- l'infrastruttura di rete locale dell'Ente è realizzata nell'ambito della più ampia infrastruttura tecnologica InfoCamere (IC Rete) che ne gestisce gli aspetti tecnologici di base: collegamenti in rete geografica, firewall, antivirus, servizio internet, manutenzione data center;
- i sistemi per la gestione dei flussi documentali (SGD_IC) e di conservazione (SCD_IC) sono sviluppati e gestiti interamente da InfoCamere e utilizzati dall'Ente via internet/intranet, come servizio, in modalità SAAS – software as a service;
- il processo di protocollazione dei flussi documentali in entrata (Servizio di protocollazione) è centralizzato su una specifica unità organizzativa;
- il livello di rischio relativo all'ambito di competenza InfoCamere è stato assunto come minimo/trascurabile, in virtù delle specifiche capacità organizzative e operative della società di informatica del sistema camerale.

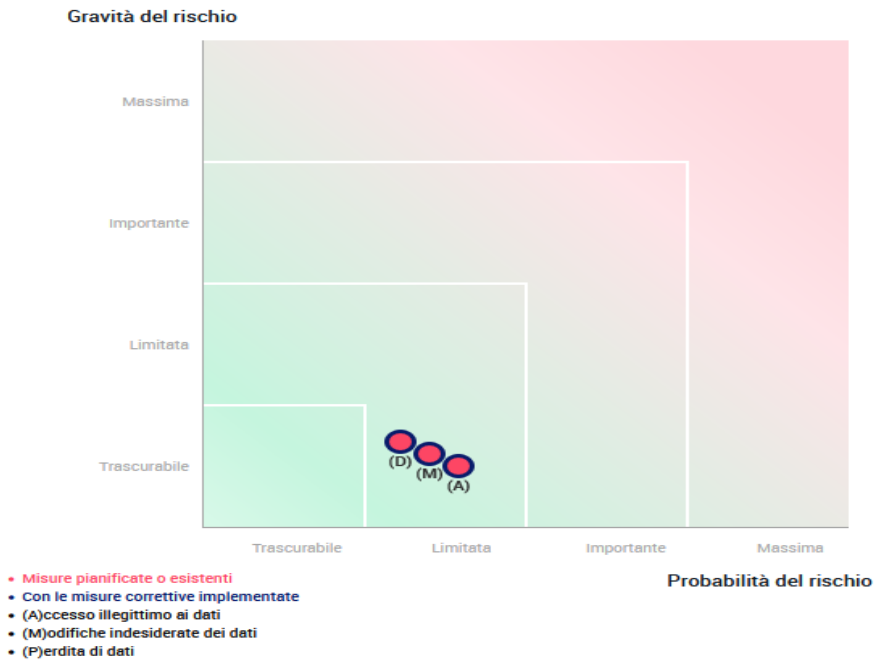
Le minacce e le vulnerabilità che insistono sugli asset dell'Ente sono state individuate in base a:

- standard di settore, best practice di sicurezza e livello tecnologico delle infrastrutture IT dell'Ente;
- esperienza del personale e scelte organizzative interne;
- indicazioni provenienti da incidenti accaduti e audit interni;
- suggerimenti e condivisioni da parte di esperti del settore.

Per ogni minaccia o vulnerabilità che insiste su ciascun asset sono state individuate le contromisure applicabili, e per ognuna è stato anche valutato il grado di attuazione (valore percentuale che esprime quanto la contromisura è stata attuata; ad esempio: 100% per misura completamente attuata, 0% per misura assolutamente non attuata, 50% parzialmente attuata).

7.2 Mappatura dei rischi e valutazione di impatto

Incrociando quindi, rischi, probabilità e misure di sicurezza adottate è stata condotta una mappatura del rischio secondo la procedura CNIL la quale ha evidenziato un livello di rischio\probabilità trascurabile\limitato.



7.3 Rischio residuo e formazione

Il rischio residuo è sostanzialmente circoscritto alla componente umana, ovvero nel livello di conoscenza e competenza del personale coinvolto nei processi di gestione documentale, e per il quale la misura di sicurezza preventiva idonea e adeguata risiede nelle azioni di formazione.

Con riferimento al Piano di formazione del personale, relativamente ai servizi della Gestione Documentale, l'Ente garantisce che:

- le iniziative di formazione/aggiornamento siano finalizzate al mantenimento e sviluppo del patrimonio delle conoscenze dell'Ente in un'ottica di formazione continua in grado di recepire le esigenze formative e le evoluzioni normative, istituzionali e tecnologiche;
- la formazione di ogni persona avvenga sulla base di una pianificazione che tenga conto del percorso formativo seguito, della figura professionale di appartenenza e quindi delle attività che la persona svolge o dovrà svolgere oltreché delle competenze e potenzialità espresse.

La formazione viene pianificata ed attuata, di concerto con il Responsabile della Gestione Documentale con il supporto del Responsabile della Sicurezza informatica, secondo le attività:

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

8 MISURE DI SICUREZZA: PROCESSO CONTINUO

Con l'evolvere della tecnologia e delle minacce in ambito di cybersecurity occorre tenere aggiornate continuamente le misure di sicurezza adottate. Pertanto, possiamo definire l'implementazione delle misure di sicurezza un processo continuo, che prevede periodicamente la verifica di nuove vulnerabilità, nuove minacce e nuove tecnologie messe a disposizione per mitigare i rischi e le probabilità di accadimento.

La Camera di commercio di Torino, in collaborazione con il partner tecnologico InfoCamere, pone particolare attenzione alle tematiche di sicurezza ICT, attuando misure di sicurezza periodicamente aggiornate in relazione ai potenziali rischi individuati.