Camera di Commercio
Roma

# PIANO DELLA SICUREZZA PER IL SISTEMA DI GESTIONE INFORMATICA E LA CONSERVAZIONE DIGITALE DELLA CAMERA DI COMMERCIO DI ROMA

Redatto ai sensi dell'art. 4, co. 1, lett. c) e dell'art. 7 del DPCM 03.12.2013 e dell'art. 12 del DPCM 13.11.2014

**EMISSIONE DEL DOCUMENTO**

| Azione | Data | Nominativo | Funzione |
|---|---|---|---|
| *Redazione* | 15.05.2025 | Massimo Traversa | Vicario del Responsabile della gestione documentale, della conservazione e della sicurezza informatica della CCIAA di Roma |
| *Verifica* | 15.05.2025 | Andrea Belli | Responsabile della gestione documentale, della conservazione e della sicurezza informatica della CCIAA di Roma |
| *Approvazione* | 03.06.2025 | Andrea Belli | Responsabile della gestione documentale, della conservazione e della sicurezza informatica della CCIAA di Roma |

**REGISTRO DELLE VERSIONI**

| N°Ver/Rev/Bozza | Data emissione | Autore | Modifiche |
|---|---|---|---|
| 1.1 | 15.05.2025 | Andrea Belli | Prima redazione |

SOMMARIO

# 1 PREMESSE

## 1.1 Generalità

Il presente Piano della Sicurezza del Sistema di Gestione Informatica e della Conservazione Digitale descrive e riporta le misure di sicurezza adottate dalla Camera di Commercio di Roma per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali di cui al Regolamento UE 2016/679 (GDPR), ai sensi dell'art. 4, co. 1, lett. c), dell'art. 7 del DPCM 03 dicembre 2013 e dell'art. 12 del DPCM 13 novembre 2014.

Come di seguito meglio descritto, gli elementi, gli strumenti tecnologici, le modalità organizzative ed i processi che costituiscono l'intero Sistema di gestione dei documenti informatici della Camera di Commercio di Roma sono governati secondo un principio di responsabilità condivisa con il fornitore dei servizi tecnologici ed informatici InfoCamere; in particolare:

- l'amministrazione e la manutenzione della Piattaforma applicativa e della relativa Infrastruttura IT su cui è ospitata, è regolamentata dal sistema di governo della sicurezza delle informazioni del fornitore InfoCamere;
- la componente locale di sicurezza (tecnica ed organizzativa) relativa agli ambienti, alle postazioni di lavoro ed alle loro configurazioni nonché agli altri dispositivi e supporti in uso al personale, in ottemperanza alla normativa vigente e con l'eventuale contributo di fornitori terzi, è prerogativa della Camera di Commercio di Roma.

Le modalità di accesso ai diversi software applicativi che gestiscono il protocollo informatico ed i flussi documentali sono definite da specifiche procedure interne alla Camera.

Il presente documento, come previsto dall'art. 12 del DPCM 13 novembre 2014, costituisce un imprescindibile allegato al Manuale della Conservazione Digitale della Camera di Commercio di Roma.

## 1.2 Obiettivi

Scopo del presente documento è descrivere la strategia che la Camera di Commercio di Roma adotta per poter soddisfare i seguenti requisiti di sicurezza:

- confidenzialità: l'accesso e la divulgazione delle informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, deve poter essere effettuato solo da soggetti autorizzati; deve essere ridotta al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, la probabilità che un'informazione riservata sia resa pubblica;

- integrità: la modifica o la distruzione di informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, devono poter essere effettuate solo da soggetti all'uopo formalmente autorizzati; devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, le probabilità che le informazioni siano in qualche modo modificate. Devono essere altresì garantiti sia l'origine del dato (non ripudiabilità) che la sua conformità all'originale (autenticità);
- disponibilità: l'accesso all'informazione ed ai sistemi deve essere sempre affidabile e tempestivo;
- tracciabilità: tutte le azioni che un soggetto compie nell'ambito del sistema sono memorizzate in modo tale da poter essere, in tempi successivi, ricondotte in maniera inequivocabile al soggetto stesso.

L'adozione di idonee e preventive misure di sicurezza garantisce da un lato che i documenti e le informazioni trattati dalla AOO siano resi disponibili, integri e riservati e, dall'altro, che il trattamento dei dati personali indicati nel GDPR venga effettuato in modo da ridurre al minimo 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 Piano per la sicurezza informatica si basa essenzialmente sull'analisi dei rischi a cui è esposto il sistema informatico, i relativi dati ed i documenti in esso contenuti e sulle direttive strategiche stabilite dal vertice della Camera di Commercio di Roma. Il presente Piano è soggetto a revisione, in funzione dell'estensione del sistema, dell'evoluzione tecnologica, della variazione degli obiettivi dell'organizzazione e del manifestarsi di nuovi o mutati rischi per la sicurezza; in caso di eventi straordinari il Piano è soggetto ad una revisione estemporanea.

### 1.3 Livello di riservatezza

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

### 1.4 Riferimenti normativi e standard di riferimento

- D.P.R. 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- D. Lgs. 7 marzo 2005, n. 82- Codice dell'Amministrazione Digitale;
- D.P.C.M. 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, co. 3 e 5-bis, 23-ter, co. 4, 43, co. 1 e 3, 44, 44-bis e 71, co. 1, del Codice dell'amministrazione digitale di cui al D. Lgs. n. 82 del 2005;
- D.P.C.M. 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, co. 1, 41, e 71, co. 1, del Codice dell'amministrazione digitale di cui al D. Lgs. n. 82 del 2005;
- Circolare n. 2/2017 del 18 aprile 2017 recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)";
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, adottate dall'AgID e pubblicate sulla G.U. n. 259 del 19 ottobre 2020 e s.m.i.;
- Regolamento (UE) Generale per la protezione dei dati personali n. 2016/679 (GDPR);
- Sistema di Conservazione e Servizio di Gestione Documentale gestiti ed erogati da Infocamere, certificati secondo gli standard ISO 9001 (Qualità), ISO 27001 (Sicurezza delle informazioni), ISO 20000 (Servizi), ISO 22301 (Continuità operativa).

### 1.5 Termini e definizioni

| Codifica | Descrizione |
|---|---|
| AOO | Area Organizzativa Omogenea, ovvero l'Ente camerale nel suo complesso |
| Gedoc | Sistema per la gestione dei flussi documentali, sviluppato e gestito da InfoCamere e utilizzato dalle Camere di Commercio |
| GDPR | Regolamento (UE) Generale per la protezione dei dati personali n. 2016/697 |
| RPO (Recovery Point Objective) | Indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto |
| RTO (Recovery Time Objective) | Tempo entro il quale un processo informatico ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili |

| Codifica | Descrizione |
|---|---|
| Servizio | Servizio di gestione documentale (Gedoc) e servizio per la conservazione dei documenti informatici |

### 1.6 Documenti di riferimento

Il presente Piano della sicurezza informatica rientra nel più generale Piano della Sicurezza della Camera di Commercio di Roma e ad esso sono collegati:

- Il Manuale di Gestione documentale della Camera di Commercio di Roma;
- Il Manuale della Conservazione Digitale della Camera di Commercio di Roma;
- Il Sistema di Gestione della Sicurezza delle Informazioni di InfoCamere;
- Il Manuale del Sistema di Conservazione di InfoCamere.

### 1.7 Gestione dei documenti informatici

Il sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico, di proprietà di InfoCamere e sviluppato internamente per rispondere agli standard qualitativi e di sicurezza, è conforme alle specifiche previste dalla normativa vigente.

Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in maniera da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;

- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy", con particolare riferimento al trattamento dei dati sensibili di cui al GDPR;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato. Per la gestione dei documenti informatici all'interno dell'AOO, il RPS fa riferimento alle norme stabilite dal responsabile del sistema informativo dell'AgID.

## 2 ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

La sicurezza complessiva del sistema di gestione e conservazione è garantita dall'insieme delle misure di sicurezza adottate dalla Camera di Commercio di Roma con il contributo di InfoCamere, nella sua qualità di soggetto fornitore del servizio di gestione informatica e di conservazione dei documenti digitali, per i rispettivi ambiti di responsabilità.

### 2.1 Descrizione degli asset

Per l'analisi del rischio informatico all'interno della Camera di Commercio di Roma sono stati individuati specifici asset in considerazione del fatto che:

- l'intera infrastruttura di rete della Camera di Commercio di Roma è realizzata nell'ambito dell'infrastruttura InfoCamere che, per la gran parte, ne gestisce gli aspetti tecnologici;
- i sistemi per la gestione dei flussi documentali e di conservazione sono sviluppati e gestiti da InfoCamere per l'utilizzo da parte della Camera di Commercio, come servizio, in modalità SAAS – software as a service;
- il processo di protocollazione dei flussi documentali in entrata è centralizzato su una specifica unità organizzativa.

| Asset | Descrizione |
|---|---|
| Personale interessato | Utenti del Sistema |
| Servizio | Servizio di Gestione Documentale offerto agli utenti |
| Documenti | Documenti gestiti dal Sistema |
| Dati personali | Dati personali presenti nei documenti, registrazioni di protocollo, metadati |
| Metadati relativi alle registrazioni di protocollo ed ai documenti | Informazioni associate a documenti e fascicoli informatici tramite l'adozione di regole, procedure e tecnologie idonee a garantirne le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità. |
| Registro di protocollo | Registro su cui si annota in ordine cronologico la corrispondenza in arrivo e in partenza |
| Credenziali di accesso | Identificativo di accesso, profilo di abilitazione associato, password |
| Processi di gestione documentale | Processi e attività di gestione della protocollazione e dei flussi documentali |
| Protocollazione | Attribuzione al documento di un numero progressivo |
| Fascicolazione | Inserimento del documento in un fascicolo informatico |
| Classificazione | Attribuzione al documento della classifica prevista dal titolario di archivio |
| Inoltro | Assegnazione del documento all'ufficio competente |

| Asset | Descrizione |
|---|---|
| Copia per immagine su supporto informatico di documenti analogici | Inserimento nel sistema informatico di un documento analogico tramite scansione e attestazione di conformità all'originale cartaceo |
| Infrastruttura IT | Infrastruttura tecnologica che ospita il Sistema |
| Postazioni di lavoro | Personal computer/altri apparati mobili tramite i quali gli utenti accedono al sistema |
| Dispositivi di firma | Dispositivi di firma digitale |

## 2.2 Analisi delle minacce e vulnerabilità [1]

Le minacce e vulnerabilità che insistono sugli asset sono state individuate in base a:

- standard di settore, best practice di sicurezza e livello tecnologico delle infrastrutture IT della Camera di Commercio di Roma;
- 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 e vulnerabilità dei singoli asset, indipendentemente dalle contromisure adottate/adottabili, sono stati valutati sia il rischio (probabilità) del suo verificarsi che il conseguente impatto, come meglio descritto nella tabella che segue.

| Asset | Minacce e vulnerabilità | Probabilità | Impatto |
|---|---|---|---|
| Personale interessato | Il personale potrebbe incontrare difficoltà nell'utilizzo di un nuovo software con conseguente perdita di efficienza e di motivazione all'utilizzo. | M | A |
| Personale interessato | I profili di abilitazione assegnati al personale potrebbero essere sovra/sottodimensionati rispetto alle effettive esigenze lavorative; ciò potrebbe provocare un limite alle effettive esigenze di utilizzo o un eccesso nella consultazione di informazioni riservate. | M | A |
| Documenti | La classificazione e fascicolazione dei documenti è un'operazione complessa, perciò un documento classificato e fascicolato in modo non corretto potrebbe creare difficoltà nella ricerca. | M | M |

[1] Legenda: A-Alto; B-Basso; M-Medio; mA-medioAlto; mB-medioBasso.

| Asset | Minacce e vulnerabilità | Probabilità | Impatto |
|---|---|---|---|
| Documenti | Un documento potrebbe essere accidentalmente o intenzionalmente cancellato o sostituito; tale azione comporterebbe il coinvolgimento del personale in un procedimento amministrativo o giudiziario con conseguente danno all'immagine istituzionale dell'Ente. | mB | mA |
| Dati personali | I profili di abilitazione assegnati al personale potrebbero essere sovradimensionati rispetto alle esigenze lavorative effettive, con la conseguenza che potrebbero essere acquisite informazioni personali da parte di chi non è incaricato. | M | mA |
| Metadati relativi alle registrazioni di protocollo ed ai documenti | I metadati inseriti potrebbero essere incoerenti con le registrazioni di protocollo o i documenti archiviati. | mB | A |
| Registro di protocollo | Il registro di protocollo potrebbe risultare danneggiato. | mB | mA |
| Registro di protocollo | Il registro di protocollo potrebbe venire alterato. | mB | mA |
| Credenziali di accesso | Le credenziali potrebbero diventare non allineate alle effettive necessità. | B | B |
| Processi di gestione documentale | I processi di gestione documentale potrebbero essere poco conosciuti al personale. | B | A |
| Protocollazione | Eventuale malfunzionamento del sistema può ritardare la protocollazione dei documenti. | M | M |
| Classificazione | Errore di classificazione può incidere sui tempi di conservazione di un fascicolo/documento. | M | mA |
| Fascicolazione | Fascicolazione non corretta di un documento provocherebbe difficoltà nelle successive ricerche. | M | M |
| Inoltro | L'inoltro non corretto può creare disguidi e rallentare l'attività lavorativa. | mB | mB |
| Copia per immagine su supporto informatico di documenti analogici | Una errata scansione fa sì che il documento informatico non sia leggibile, ma il sistema prevede l'attestazione della conformità del file al documento analogico e quindi un controllo. | M | B |
| Processi | Nel tempo i processi di gestione documentale potrebbero discostarsi dalle prassi effettive. | B | M |
| Infrastruttura IT | L'infrastruttura IT potrebbe essere oggetto di malfunzionamento, con la conseguenza che il servizio di gestione documentale potrebbe essere non | M | A |

| Asset | Minacce e vulnerabilità | Probabilità | Impatto |
|---|---|---|---|
| | disponibile, generando un blocco dei processi. | | |
| Infrastruttura IT | Potrebbe verificarsi un evento disastroso nel sito di erogazione dei servizi di InfoCamere, con la conseguenza che l'infrastruttura IT potrebbe venire distrutta e generare indisponibilità del servizio per un lunghissimo periodo. | mB | mA |
| Postazioni di lavoro | Postazioni di lavoro potrebbero essere infettate da malware. | M | mA |
| Postazioni di lavoro | Durante le pause di lavoro le postazioni di lavoro potrebbero consentire l'interazione con il Sistema da parte di personale non autorizzato. | M | A |
| Postazioni di lavoro | Postazioni di lavoro potrebbero essere inadeguate rispetto alle caratteristiche richieste dal Sistema. | mB | M |
| Dispositivi di firma | dispositivo di firma può non funzionare impedendo la firma del documento in tempo utile. | M | mA |

### 2.3 Individuazione delle contromisure

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

| Asset | Minacce e vulnerabilità | Contromisure | Grado di efficacia |
|---|---|---|---|
| Personale interessato | Quando viene adottato un nuovo software il personale potrebbe incontrare difficoltà nel suo utilizzo con conseguente perdita di efficienza e di motivazione all'uso. | • Piano di formazione adeguato<br>• Incontri mensili con il personale per raccogliere le problematiche e identificare soluzioni comuni. | 50% |
| Personale interessato | I profili di abilitazione assegnati al personale potrebbero essere sovra/sottodimensionati rispetto alle effettive esigenze lavorative; ciò potrebbe provocare un limite alle effettive esigenze di utilizzo o un eccesso nella consultazione di informazioni riservate. | Verificare periodicamente l'adeguatezza dei profili (anche intervistando il personale). | 90% |

| Asset | Minacce e vulnerabilità | Contromisure | Grado di efficacia |
|---|---|---|---|
| Documenti | La classificazione e fascicolazione dei documenti è un'operazione complessa, perciò un documento classificato e fascicolato in modo non corretto potrebbe creare difficoltà nella ricerca futura. | • Piano di formazione adeguato<br>• Incontri mensili con il personale per raccogliere le problematiche e identificare soluzioni comuni. | 50% |
| Documenti | Un documento potrebbe essere accidentalmente/intenzionalmente cancellato o sostituito, con la conseguenza che il personale potrebbe essere coinvolto in un procedimento amministrativo o giudiziario; ciò potrebbe provocare un danno all'immagine istituzionale dell'Ente. | Verificare periodicamente i backup sui server in base ai salvataggi pianificati | 100% |
| Dati personali | I profili di abilitazione assegnati al personale potrebbero essere sovradimensionati rispetto alle esigenze lavorative; questo evento provocherebbe la consultazione di informazioni personali da parte di chi non è incaricato. | Verificare periodicamente l'adeguatezza dei profili (anche intervistando il personale). | 100% |
| Infrastruttura IT | L'infrastruttura IT potrebbe essere oggetto di malfunzionamento con la conseguenza che il Servizio di gestione documentale potrebbe essere non disponibile, generando un blocco dei processi. | Verificare il livello di disponibilità garantito da InfoCamere per il Sistema di gestione documentale (vedi paragrafo "Livelli di Servizio" del Piano della sicurezza). | 100% |
| Infrastruttura IT | Potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di InfoCamere: se l'infrastruttura IT venisse distrutta si avrebbe l'indisponibilità del servizio per un lunghissimo periodo. | Verificare se il Sistema di gestione documentale sia inserito nella soluzione di Disaster Recovery di InfoCamere (vedi paragrafo "Continuità operativa del Sistema"). | 100% |

## 2.4 Calcolo del Rischio

| Asset | Minacce e vulnerabilità | Rischio intrinseco | Rischio residuo |
|---|---|---|---|
| Personale coinvolto | Quando viene adottato un nuovo software il personale potrebbe incontrare difficoltà nell'utilizzo e ciò comporterebbe una perdita di efficienza e di motivazione all'utilizzo. | Alto | Basso |

| Asset | Minacce e vulnerabilità | Rischio intrinseco | Rischio residuo |
|---|---|---|---|
| Personale coinvolto | I profili di abilitazione assegnati al personale potrebbero essere sovra/sottodimensionati rispetto alle effettive esigenze lavorative; ciò potrebbe provocare un limite alle effettive esigenze di utilizzo o un eccesso nella consultazione di informazioni riservate. | Alto | Alto |
| Documenti | La classificazione e fascicolazione dei documenti è un'operazione complessa, perciò un documento classificato e fascicolato in modo non corretto potrebbe creare difficoltà nella ricerca futura. | Medio | Basso |
| Documenti | Un documento potrebbe essere accidentalmente/intenzionalmente cancellato o sostituito, di conseguenza il personale potrebbe essere coinvolto in un procedimento amministrativo o giudiziario con conseguente danno all'immagine istituzionale dell'Ente. | Medio | Basso |
| Dati personali | I profili di abilitazione assegnati al personale potrebbero essere sovradimensionati rispetto alle esigenze lavorative, ciò provocherebbe la consultazione di informazioni personali da parte di personale non incaricato. | Altissimo | Altissimo |
| Infrastruttura IT | L'infrastruttura IT potrebbe essere coinvolta da malfunzionamenti e il Servizio di gestione documentale potrebbe essere non disponibile provocando un blocco dei processi. | Alto | Basso |
| Infrastruttura IT | Potrebbe verificarsi un evento disastroso nel sito di erogazione dei servizi di InfoCamere.<br>L'infrastruttura IT potrebbe venire distrutta con conseguente indisponibilità del servizio per un lunghissimo periodo. | Medio | Basso |

## 2.5 Trattamento del rischio residuo

| Asset | Minacce e vulnerabilità | Rischio residuo | Strategia di risposta | Azione di trattamento |
|---|---|---|---|---|
| Personale interessato | Quando viene adottato un nuovo software il personale potrebbe incontrare difficoltà nell'utilizzo e ciò comporterebbe una perdita di efficienza e di motivazione all'utilizzo. | Basso | Accettazione | Formazione mirata sulla base delle difficoltà manifestate. |

| Asset | Minacce e vulnerabilità | Rischio residuo | Strategia di risposta | Azione di trattamento |
|---|---|---|---|---|
| Personale interessato | I profili di abilitazione assegnati al personale potrebbero essere sovra/sottodimensionati rispetto alle effettive esigenze lavorative, ciò potrebbe provocare un limite alle effettive esigenze di utilizzo o un eccesso nella consultazione di informazioni riservate. | Alto | Mitigazione | Sei mesi dopo l'avvio verifica dell'adeguatezza dei profili (anche intervistando il personale e i Responsabili), poi verifica annuale. |
| Documenti | La classificazione e fascicolazione dei documenti è un'operazione complessa, perciò un documento classificato e fascicolato in modo non corretto potrebbe creare difficoltà nella ricerca futura. | Basso | Accettazione | Controllo da parte dei responsabili ufficio. |
| Documenti | Un documento potrebbe essere accidentalmente/intenzionalmente cancellato o sostituito con la conseguenza che il personale potrebbe essere coinvolto in un procedimento amministrativo o giudiziario. Ciò potrebbe provocare un danno all'immagine istituzionale dell'Ente. | Basso | Accettazione | Controllo da parte dei responsabili ufficio. |
| Dati personali | I profili di abilitazione assegnati al personale potrebbero essere sovradimensionati rispetto alle esigenze lavorative; questo evento provocherebbe la consultazione di informazioni personali da parte di personale non incaricato. | Altissimo | Rimozione | Sei mesi dopo l'avvio verifica dell'adeguatezza dei profili (anche intervistando il personale e i Responsabili), poi verifica annuale. |
| Infrastruttura IT | L'infrastruttura IT potrebbe essere oggetto di malfunzionamento con la conseguenza che il Servizio di gestione documentale potrebbe essere non disponibile, generando un blocco dei processi. | Basso | Accettazione | Si individuano con Infocamere soluzioni condivise. |
| Infrastruttura IT | Potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di InfoCamere; se l'infrastruttura IT venisse distrutta si avrebbe l'indisponibilità del servizio per un lunghissimo periodo. | Basso | Accettazione | Si individuano con Infocamere soluzioni condivise. |

### 2.6 Formazione del personale

Con riferimento al Piano di Formazione del personale, relativamente alla Gestione Documentale ed al trattamento e protezione dei dati personali, l'Ente garantisce che:

1) 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, nonché garantire la sicurezza e la protezione dei dati personali trattati nel rispetto della normativa vigente (GDPR);
2) 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.

Le attività formative del personale della Camera di Commercio di Roma vengono, quindi, programmate ed attuate, sentito il parere del Responsabile della gestione documentale, in funzione delle esigenze generali e specifiche dell'Ente.

### 2.7 Continuità operativa del sistema

Il Sistema di Gestione informatica dei documenti è ospitato su infrastruttura IT di InfoCamere ed è inserito**:**

1) nell'ambito del Sistema di Gestione della Continuità Operativa di InfoCamere;
2) nell'ambito della soluzione tecnologica di Disaster Recovery di InfoCamere; tale soluzione è dotata di una infrastruttura tecnologica dedicata e delle necessarie caratteristiche di ridondanza geografica.

In tal senso InfoCamere adotta un sistema di gestione certificato ISO/IEC 22301 che aiuta a proteggere e ridurre le probabilità di gravi incidenti del sistema, assicurando nel contempo la tempestiva ripresa delle attività in seguito ad eventuali interruzioni del servizio; gli ambienti server che ospitano la piattaforma applicativa sono, quindi, adeguatamente protetti.

# 3 MONITORAGGIO E CONTROLLI

## 3.1 Ripristino del Servizio

Il Responsabile del Servizio di Gestione documentale cura che le funzionalità del sistema, 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).

## 3.2 Livelli di servizio

In coerenza con il paragrafo precedente, InfoCamere garantisce che il Servizio sia erogato con i seguenti livelli di servizio:

| | |
|---|---|
| orario di servizio [2] | 08:00 / 21:00 - da lunedì a venerdì<br>08:00 / 14:00 - sabato |
| disponibilità del servizio | migliore del 99% |
| RTO | 72 ore |
| RPO | 24 ore |

## 3.3 Comunicazione con il fornitore InfoCamere

InfoCamere rende disponibile uno speciale 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 di 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.

## 3.4 Monitoraggio dell'infrastruttura IT

Il Sistema di Gestione informatica dei documenti:

1) è ospitato su infrastruttura IT di InfoCamere;
2) viene mantenuto sotto controllo da InfoCamere per quanto attiene l'infrastruttura IT tramite i processi e gli strumenti di seguito descritti.

[2] **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. È 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

### 3.4.1 Procedure operative

La Procedura di Operation & Event Management di InfoCamere:

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

### 3.4.2 Strumenti

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

1) sonde di rilevazione;
2) registrazione degli eventi;
3) console;
4) segnalazioni generate automaticamente.

### 3.4.3 Gestione dei log

InfoCamere mantiene sotto controllo gli eventi anomali legati a:

1) malfunzionamenti;
2) performance,

registrandoli ai fini di:

- riesame;
- audit.

I log sono classificati nelle tipologie:

1) log infrastrutturali: riguardano le componenti software (acquisite da fornitori) e i sistemi hardware che compongono l'infrastruttura IT;
2) 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.

# 4 POLITICHE DI SICUREZZA

Le politiche di sicurezza stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informatico, sia le misure consuntive per la gestione degli incidenti informatici. È compito del responsabile della sicurezza informatica e del responsabile della tutela dei dati personali procedere al perfezionamento, alla divulgazione, al riesame ed alla verifica delle politiche di sicurezza. II riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti attinenti alla sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste dall'AgID al RTI, o a seguito dei risultati delle attività di audit.

## 4.1 Politica di gestione della sicurezza dei sistemi

Il Sistema di gestione informatica dei documenti è costituito da infrastrutture, persone, processi e tecnologie in ambiente server e client secondo un approccio condiviso tra il fornitore dei Servizi InfoCamere, cui compete la gestione diretta dell'infrastruttura, e la Camera di Commercio di Roma.

Le sezioni che seguono descrivono, quindi, le principali azioni ed iniziative messe in atto da InfoCamere e dalla Camera di Commercio di Roma per quanto di rispettiva competenza ed in un'ottica di responsabilità condivisa, per l'amministrazione, gestione e manutenzione dell'ambiente server (ossia la piattaforma applicativa e l'infrastruttura IT su cui è ospitata) e degli ambienti client da cui viene utilizzato il servizio digitale.

In particolare, le attività in ambiente server sono regolamentate dal sistema di governo della sicurezza delle informazioni di InfoCamere, realizzando una serie di controlli che rispondono ai requisiti di sicurezza identificati (dall'analisi di rischio, dalla legislazione, dai regolamenti di riferimento, altre fonti) e che comprendono politiche, procedure, istruzioni, responsabilità, meccanismi e strumenti hardware e software aderenti agli standard internazionali ed alle buone pratiche riconosciute dal settore.

### 4.1.1 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 devono essere censiti, catalogati e valutati in relazione alla loro importanza per il business; devono essere quindi assegnati ad un responsabile. La valutazione deve essere

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

### 4.1.2 Installazione dei sistemi

L'integrità dei sistemi di produzione è un requisito di sicurezza essenziale per InfoCamere; pertanto devono essere attuate procedure per controllare l'installazione del software sui sistemi di produzione.

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

In particolare, riguardo a:

**1) cambiamento**

le modifiche alle componenti di software applicativo, hardware e software di sistema devono essere 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;

**2) documentazione**

i cambiamenti apportati all'infrastruttura IT devono essere opportunamente documentati.

### 4.1.3 Resource Capacity Management

Per poter garantire che l'infrastruttura tecnologica sia in grado di soddisfare i livelli di servizio richiesti, tutte le componenti hardware e software devono essere tenute sotto controllo; si devono fare proiezioni sui futuri requisiti di capacità per assicurare le prestazioni di sistema richieste.

Il Processo è strutturato nelle seguenti fasi:

1) analizzare i piani aziendali a breve e lungo termine;
2) 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;
3) valutare la crescita del carico di lavoro nel tempo;
4) avviare l'eventuale attività di approvvigionamento delle risorse in esame.

### 4.1.4 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.

### 4.1.5 Backup

Devono essere effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi; le copie devono essere 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).

### 4.1.6 Amministratori di Sistema

Devono essere minimizzati i rischi di:

1) violazione alla compliance relativa agli Amministratori di Sistema;
2) 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 va effettuata, da parte del Responsabile della competente Area di appartenenza della Struttura informatica, 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, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti, anche da parte del Garante della Privacy.

## 4.2 Politica per l'inserimento dell'utenza e per il controllo degli accessi logici

La politica per il controllo degli accessi logici si applica anche al caso specifico del Servizio di Gestione informatica dei documenti. Anche in tale ambito si deve limitare l'accesso alle informazioni ed ai servizi di elaborazione delle informazioni ai cosiddetti "need to access" cioè a

coloro che hanno effettive e legittime necessità operative. La sicurezza delle informazioni nell'Ente è considerato un obiettivo fondamentale.

Tutto il personale della Camera di Commercio di Roma e le terze parti interessate devono essere informati sulla esistenza di una politica specifica per la gestione ed il controllo degli accessi logici alle risorse e devono essere vincolati, in dipendenza delle loro responsabilità o competenze, a rispettarne le prescrizioni.

La strumentazione e le istruzioni per il controllo degli accessi devono essere 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.

**4.2.1 Gestione delle credenziali di accesso - assegnazione, riesame e revoca degli accessi degli utenti**

Riguardo al Servizio di Gestione Documentale:

1) l'accesso alle informazioni e funzioni di sistemi applicativi deve essere limitato alle effettive necessità degli uffici;
2) 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, oppure adattate ad ogni variazione;
3) in caso di cessazione verranno disattivati gli identificativi di accesso del personale non più in servizio e dei consulenti non più operativi;
4) nessun identificativo di accesso dovrà essere cancellato ma dovranno essere eliminate solo le abilitazioni;
5) gli "identificativi utente" assegnati una prima volta non potranno più essere riassegnati ad altre persone;
6) l'assegnazione e l'utilizzo delle utenze e dei privilegi amministrativi deve essere ristretto e controllato;
7) qualora si renda necessario accedere "in emergenza" a specifici dati o sistemi da parte di personale non ancora abilitato si deve richiedere un'abilitazione temporanea;
8) nel caso di definizione di nuove credenziali di accesso, o di modifica delle esistenti, viene inviata all'interessato una notifica che gli consente di accedere al sistema informativo nel quale consultare le credenziali assegnate e registrare la propria accettazione.

Le richieste relative ai diritti di accesso di cui sopra vengono inviate ad InfoCamere che provvede, tramite gli opportuni strumenti tecnici, a soddisfarle ed a fornire riscontro ai richiedenti.

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

### 4.2.2 Utilizzo delle password

Riguardo al Servizio di Gestione Documentale:

1) occorre evitare l'uso improprio delle password e delle credenziali di autenticazione;
2) le regole relative alla costruzione ed utilizzo delle password si applicano a tutto il personale e ai terzi che ne fanno uso per accedere agli asset dell'Ente;
3) l'utilizzo delle password ed in genere delle credenziali utente, deve essere controllato con un processo di gestione formale, anche automatizzato, fin ove possibile;
4) le credenziali sono personali e non cedibili, devono essere assegnate in base alla necessità di accesso ai dati o ai sistemi dell'Ente e devono essere gestite contemporaneamente alle abilitazioni, sulla base del principio del "minimo privilegio";
5) le password devono essere "robuste", ovvero costruite in modo da non essere facilmente individuabili (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 etc.).

### 4.2.3 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 del Servizio di Gestione Documentale è dell'utente fruitore del servizio.

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

### 4.2.4 Servizi informatici forniti da InfoCamere

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:

1) i sistemi di gestione delle password sono interattivi e assicurano password di qualità;

2) i sistemi di autenticazione impongono il rispetto della password policy.

L'accesso al Sistema di Gestione Documentale, realizzato su infrastruttura IT di InfoCamere e da questa gestito, è dotato di:

1) procedure di log-on sicure che garantiscono l'accesso ai sistemi applicativi;
2) controllo degli accessi alle applicazioni ed alle informazioni da parte degli utenti nel rispetto del principio di necessità;
3) password di accesso ai servizi fornite da Infocamere mediante strumentazione tecnica adeguata e coerente con la normativa.

**4.3 Politica di gestione delle postazioni di lavoro**

Il Servizio di Gestione Documentale prevede, in attuazione della politica di gestione delle postazioni di lavoro, il rispetto delle regole che seguono:

1) aggiornamenti del software
   a) l'Ente deve mantenere adeguato il livello di aggiornamento del software installato sulle postazioni di lavoro;
   b) il personale, da parte sua, non deve inibire gli eventuali strumenti di aggiornamento automatico o centralizzato previsti dall'Ente.
2) limitazione della connettività a supporti esterni

   l'utilizzo improprio di dispositivi rimovibili può aumentare il rischio di fuga di dati riservati aziendali. Il personale perciò deve tenere presente alcune regole fondamentali:
   a) non deve consentire ad altri di collegare dispostivi rimovibili alla propria postazione;
   b) non deve connettere alla propria postazione dispositivi rimovibili lasciandoli incustoditi;
   c) non deve lasciare incustodito il dispositivo all'esterno dell'Ente.
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 e di non modificare dispositivi mobili o supporti rimovibili affidati in dotazione individuale, senza specifica autorizzazione delle funzioni di sicurezza.
4) configurazione delle postazioni di lavoro

   il sistema di gestione documentale, lato utente, è reso disponibile in modalità di navigazione sul web; le postazioni di lavoro ed i browser devono pertanto essere configurati secondo le specifiche tecniche riportate nel Manuale di configurazione [MCF CLIENT].
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.

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

Anche al caso specifico del Servizio di Gestione Documentale devono essere rispettate le indicazioni che seguono:

1) gestione apparati e supporti informatici

   gli apparati e i supporti informatici devono essere protetti da accessi non autorizzati, utilizzi impropri, manomissioni, danneggiamento o furti:

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

   In genere le postazioni di lavoro mobili possono essere assegnate personalmente al dipendente o a una posizione organizzativa per poi essere utilizzate dal personale da essa dipendente.

   Il personale è autorizzato a portare con sé al di fuori delle sedi dell'Ente gli apparati mobili assegnati.

   La memorizzazione di dati personali su apparati mobili non è ammessa a meno di esplicita autorizzazione da parte dell'Ente (esempio: smartphone in comodato d'uso);

2) dismissione apparati e supporti informatici

   tutti gli apparati e i supporti informatici devono essere controllati per assicurare che ogni dato critico sia rimosso o sovrascritto in modo sicuro prima della dismissione o del riutilizzo;

3) gestione supporti cartacei

   i documenti e le informazioni in essi contenute non dovrebbero mai essere lasciati dal personale in luoghi al di fuori del proprio controllo.

   Le informazioni rilevanti o riservate, presenti sui supporti cartacei, non devono mai essere lasciate dal personale in luoghi accessibili ad estranei.

   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.

   Particolare cura e cautela deve essere usata per la documentazione riservata gestita all'esterno delle sedi dell'Ente nonché per i dispositivi di stampa, fotocopia, acquisizione ottica delle immagini;

4) dismissione supporti cartacei

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

   Nel caso di cessato utilizzo di documenti cartacei riservati, essi devono essere triturati con gli appositi apparecchi.

### 4.5 Politica di protezione dal malware e contromisure

La politica di protezione viene applicata anche al caso specifico del Servizio di Gestione Documentale attraverso l'attuazione delle seguenti azioni:

1) le informazioni di proprietà dell'Ente o da essa gestite e le infrastrutture IT preposte alla loro elaborazione devono essere protette contro il malware;
2) devono essere previsti ed attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware;
3) deve essere formato e promosso un idoneo grado di consapevolezza degli utenti per prevenire le minacce e le vulnerabilità derivanti dal malware.

Le contromisure per la protezione dal malware devono rispettare le seguenti condizioni:

1) la strumentazione software per la protezione dal malware (c.d. antivirus) è installata su tutte gli apparati con sistema operativo Windows, siano essi server dedicati ad erogare servizi che postazioni di lavoro dalle quali si accede ai servizi. L'antivirus è installato sia sui sistemi fisici (server, personal computer) che virtuali utilizzati dall'Ente;
2) nei sistemi "endpoint" su cui è installato, l'antivirus è sempre attivo e la scansione opera in tempo reale su ogni movimentazione di file, proteggendo così l'apparato dal malware.

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

### 4.6 Protezione dallo spamming e dal phishing

I sistemi che gestiscono la posta elettronica utilizzano una strumentazione software per la protezione dallo spamming con la funzione di:

1) controllare le informazioni di provenienza dei messaggi;
2) eliminare, inserire in quarantena o consegnare i messaggi al destinatario;
3) eliminare dai messaggi ricevuti eventuali programmi eseguibili in essi contenuti;
4) inviare ai destinatari l'elenco dei messaggi inseriti in quarantena.

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

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

Allo stesso modo, vengono costantemente pubblicati sul portale intranet Camerale avvisi sui rischi derivanti dal phishing, con l'indicazione dei comportamenti da adottare nei casi di potenziale minaccia e l'invito a segnalare l'evento.

### 4.7 Scrivania e schermo puliti

Anche per il Servizio di Gestione Documentale, i dipendenti della Camera di Commercio di Roma ed i terzi, devono adottare e applicare 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 e dei dati.

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.).

In particolare, riguardo a:

1) <u>scrivania pulita</u>

   le regole definite di "scrivania pulita" sono essenziali per proteggere le informazioni su supporto cartaceo e su supporti rimovibili di memorizzazione. Al termine del lavoro o durante lunghe pause, non deve essere lasciata sulle scrivanie alcuna documentazione riservata cartacea o su supporti rimovibili;

2) <u>schermo pulito</u>

   non lasciare accessibile la postazione di lavoro durante la propria assenza: occorre bloccarla, prevedendo lo sblocco con password e attivando comunque uno "screensaver" automatico protetto da password che pulisce la videata entro alcuni minuti in caso di inutilizzo.

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