Piano per la Sicurezza dei Documenti Informatici della Camera di commercio di Bolzano

Sommario

1 INTRODUZIONE

Il Piano per la Sicurezza descrive le misure di sicurezza relative al processo di gestione dei documenti informatici adottate al fine di garantire la riservatezza, la disponibilità e l'integrità dei dati/documenti e di 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 presente Piano per la sicurezza informatica allegato al Manuale di Gestione Documentale della Camera di Commercio I.A.T.A. di Bolzano e approfondisce i contenuti in materia di sicurezza del sistema di gestione documentale.
I titolari del trattamento dei dati sono tenuti ad osservare le misure minime di sicurezza previste dal d.lgs. n. 196/2003 e circolare AGID n.2/2017 e quindi a adottare tutti gli accorgimenti tecnici e organizzativi idonei a garantire protezione, privacy e riservatezza.

2 ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

2.1 Analisi dei rischi

L'analisi propedeutica effettuata per poter identificare le opportune misure idonee a contenere i rischi ad un livello ritenuto accettabile ha portato all'individuazione delle seguenti tipologie di rischio:
rischi relativi alla riservatezza, ovvero la possibilità che le informazioni e i documenti siano accessibili ed utilizzati da soggetti non autorizzati a prenderne visione o ad operarvi e per fini non conformi alle finalità della raccolta e agli obiettivi dell'Ente. - rischi relativi alla integrità, ovvero la possibilità che i dati e i documenti siano alterati o danneggiati, accidentalmente o dolosamente;
rischi relativi alla disponibilità, ovvero l'impossibilità temporanea o definitiva di accedere e utilizzare i dati e i documenti ogni qual volta ve ne sia necessità in conformità alle esigenze dei trattamenti;
rischi di uso improprio/rischi organizzativi, ovvero che l'accesso ai dati avvenga non esclusivamente per i fini definiti dal Titolare e da parte di soggetti non adeguatamente autorizzati e/o istruiti / mancato rispetto di norme e di procedure / utilizzo scorretto o illecito dei trattamenti e delle attrezzature.

2.2 Formazione del personale

Il contenimento dei rischi non può prescindere da una adeguata formazione del personale coinvolto.

Con riferimento al Piano di Formazione del personale, anche relativamente alla 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, secondo le attività:

analisi dei bisogni formativi;

pianificazione;

diffusione delle informazioni sui corsi;

effettuazione degli interventi formativi;

valutazione degli interventi.

2.3 Continuità operativa

Per la Camera di Commercio I.A.T.A. di Bolzano il Sistema di Gestione Documentale è ospitato su infrastruttura IT di InfoCamere e, pertanto, è inserito nell'ambito del Sistema di Gestione della Continuità Operativa di InfoCamere; 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.

2.4 Controllo degli accessi fisici

Gli accessi fisici alla sede camerale sono controllati. L'edificio della sede della Camera di Commercio, sono dotati di servizio di portierato e di vigilanza svolto da un istituto di vigilanza.

Le apparecchiature informatiche o gli archivi cartacei non specificatamente identificati per essere destinati all'utilizzo da parte del pubblico non sono, di norma, collocati in aree aperte al pubblico o comunque accessibili al pubblico.

In ogni caso le aree aperte al pubblico in cui sono presenti apparecchiature informatiche o archivi cartacei sono presidiate dal personale camerale.

Gli apparati di rete sono collocati in locali accessibili tramite una porta con serratura a chiave/elettronica. Le chiavi sono in possesso del personale camerale abilitato. Gli archivi operativi devono normalmente essere mantenuti chiusi.

Gli archivi del personale (fascicoli cartacei personali) sono custoditi in apposito locale chiuso a chiave il cui accesso è consentito solo agli incaricati dei settori competenti.

2.5 Sistema antincendio

Tutti gli edifici camerali sono protetti da sistemi antincendio mobili azionabili manualmente dal personale camerale operante in ciascuna sede, appositamente incaricato, addetto alla gestione dell'emergenza ed al primo soccorso (ai sensi del D. Lgs. n. 81/2008).

3 MONITORAGGI 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.

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 (Intervallo temporale entro il quale Infocamere garantisce al cliente l'erogazione del "servizio" sulla base di quanto previsto dal 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)
dal lunedì al venerdì dalle 08:00 alle 19:00
sabato dalle 08:00 alle 14:00
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 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 e-mail) entro due ore all'interno dell'orario di servizio dal lunedì al venerdì.

3.4 Monitoraggio dell'infrastruttura IT

Il Sistema di Gestione Documentale è ospitato su infrastruttura IT di InfoCamere; - viene mantenuto sotto controllo da InfoCamere per quanto attiene l'infrastruttura IT tramite i processi e gli strumenti sotto descritti.

3.4.1 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.

3.4.2 Strumentazione

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.

4.3 Gestione dei log

InfoCamere mantiene sotto controllo gli eventi anomali legati a: malfunzionamenti e performance registrandoli ai fini di: riesame e 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.

4 POLITICHE DI SICUREZZA

4.1 Politica di gestione della sicurezza dei sistemi

Poiché il Sistema di Gestione Documentale è ospitato su infrastruttura IT di InfoCamere ed è gestito dal punto di vista infrastrutturale sempre da InfoCamere, le politiche di sicurezza descritte nel presente paragrafo riguardano il fornitore (Infocamere).

4.1.2 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 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.

4.1.3 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.

– 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.

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

4.1.4 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:
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.

4.1.5 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.

4.1.6 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).

4.1.7 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 va effettuata 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.

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.

L'operato degli amministratori di sistema deve essere 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.

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

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. Tutto il personale dell'Ente 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, in particolare per quanto attiene a:

- Gestione delle credenziali di accesso;
- Utilizzo password;
- Responsabilità degli utenti.

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:

- L'accesso alle informazioni e funzioni di sistemi applicativi deve essere limitato alle effettive necessità.
- Rimozione o adattamento dei diritti di accesso: i diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni devono essere rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate ad ogni variazione.
- A fronte della cessazione verranno disattivati gli identificativi di accesso del personale non più in servizio e dei consulenti non più operativi.
- Nessun identificativo di accesso dovrà essere cancellato ma dovranno essere eliminate le abilitazioni.

– Gli identificativi 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.
Richieste effettuate al fornitore InfoCamere:
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:
- 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 alle risorse e ai programmi dell'Ente.
- L'utilizzo delle password ed in genere delle credenziali utente deve essere controllato con un processo di gestione formale, anche automatizzato, fin ove possibile. Le credenziali sono personali e non cedibili, devono essere assegnate in base alla necessità di accedere ai dati o ai sistemi aziendali e devono essere gestite contemporaneamente alle abilitazioni, sulla base del principio del "minimo privilegio".
- 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, 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:

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

Esecuzione degli accessi Il Sistema di Gestione Documentale realizzato su infrastruttura IT di InfoCamere e da questa gestito, dotato di:

- procedure di log-on sicure, che controllano l'accesso a sistemi e applicazioni.
- controllo degli accessi alle applicazioni ed alle informazioni, per cui 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.

4.3 Politica di gestione delle postazioni di lavoro

Il trattamento delle informazioni e dei documenti informatici nelle postazioni di lavoro deve avvenire nel rispetto delle buone pratiche di sicurezza. Con riferimento alla gestione delle postazioni di lavoro, devono essere rispettate le regole di seguito indicate.

4.3.1 Aggiornamento del software

L'Ente deve mantenere adeguato il livello di aggiornamento del software installato sulle postazioni di lavoro. Il personale da parte sua deve consultare l'ufficio Informatica e CED e/o il referente Infocamere prima di procedere ad aggiornamenti che potrebbero interferire con i software in uso e non deve inibire gli eventuali strumenti di aggiornamento automatico o centralizzato previsti dall'Ente.

4.3.2 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.

4.3.4 Modifica delle impostazioni delle postazioni di lavoro

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 dell'ufficio Informatica e CED.

4.3.5 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.

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

Nella gestione, dismissione e smaltimento delle postazioni di lavoro dell'Ente (inclusi gli apparati mobili) e dei supporti di memorizzazione (anche removibili), devono essere rispettate le regole di seguito indicate.

4.4.1 Gestione apparati e supporti informatici

Gli apparati e i supporti informatici devono essere protetti da accessi non autorizzati, utilizzi impropri, manomissioni, danneggiamento o furti:
- 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 (esempio: smartphone):
In genere le postazioni di lavoro mobili sono assegnate personalmente al personale ed utilizzate dal personale assegnatario.
- Il personale è autorizzato a portare con sé al di fuori delle sedi dell'Ente gli apparati mobili assegnati.
- La memorizzazione di dati personali non aziendali da parte del personale su apparati mobili è ammessa sotto la diretta responsabilità dell'assegnatario che deve comunque garantire la funzionalità dello strumento e la sicurezza dello stesso e dei sistemi a cui si collega.

Per il dettaglio di questi aspetti il personale deve fare riferimento al regolamento interno sull'utilizzo dei dispositivi ICT.

4.4.2 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.

4.4.3 Gestione supporti cartacei:

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

4.4.4 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 Politiche di protezione dal malware

Per la protezione dal malware, 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.
- Deve essere formato e promosso un idoneo grado di consapevolezza degli utenti per prevenire le minacce e le vulnerabilità derivanti dal malware.

4.5.1 Contromisure per la protezione dal malware

La strumentazione software per la protezione dal malware (c.d. antivirus) è installata su tutte gli apparati, 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. 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.

4.5.2 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 programmi eseguibili in essi contenuti - inviare ai destinatari l'elenco dei messaggi inseriti in quarantena. Il personale dell'Ente, qualora ritenga che un messaggio ricevuto sia indesiderato, lo può inviare al sistema che aumenta così la base di conoscenza per l'individuazione dello spamming. Le componenti sopra descritte sono periodicamente aggiornate per assicurare adeguate misure di protezione.

4.6 Scrivania e schermo pulito

Devono essere adottate e rispettate le seguenti regole di "scrivania pulita" e "schermo pulito", 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.

4.6.1 Scrivania pulita

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

4.6.2 Schermo pulito

Durante la propria assenza, non lasciare accessibile la postazione di lavoro: bloccarla, prevedendo lo sblocco con password, e attivare comunque un salvaschermo (screen saver) automatico protetto da password che pulisca 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 durante o alla ripresa della sessione).