CAMERA DI COMMERCIO INDUSTRIA E AGRICOLTURA DI POTENZA

PIANO DELLA SICUREZZA DEI DOCUMENTI INFORMATICI

Allegato n.2 MANUALE DI GESTIONE DOCUMENTALE

Versione	1	Data Versione:	23/10/2015
Descrizione modifiche	Prima emissione		
Motivazioni	Non applicabile		

Indice

INTRODUZIONE AL DOCUMENTO

1.0 Scopo e campo di applicazione del documento

Il Piano di sicurezza garantisce che:
- i documenti e le informazioni trattati dalla AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari 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] dell'Ente. Esso riprende e approfondisce i contenuti del paragrafo "La sicurezza del sistema di gestione documentale" del Manuale.

1.1 Livello di riservatezza

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

1.2 Riferimenti normativi

CAD CO	Codice dell'Amministrazione Digitale, Decreto legislativo 7 marzo 2005, n. 82, art. 50 bis
TESTO UNICO	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
LG AGID DR	Linee Guida AgID per la disaster recovery delle pubbliche amministrazioni - ai sensi del c. 3, lettera b) dell'art. 50bis del Codice dell'Amministrazione Digitale, Aggiornamento 2013

1.3 Riferimenti documentali

DPS	Documento Programmatico della Sicurezza
MDG	Manuale di Gestione documentale della Camera di Commercio di Potenza
MCF CLIENT	<xxxcodice servizio gedoc> MCF/CLIENT, Manuale di configurazione della postazione di lavoro client ????

1.4 Termini e definizioni

SGQ	Sistema di Gestione della Qualità

ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

Commento [A1]: Si tratta di valutazioni troppo complesse che non siamo in grado di fare in pochi giorni…

		-	
		-	
		-	
		-	
		-	
		-	
		-	

-

completare la tabella

Il presente piano prevede l'adozione di misure tecniche e organizzative, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti.
In particolare le misure di sicurezza adottate sono le seguenti:

- protezione dei sistemi di accesso e di conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione(password) e di un profilo di autorizzazione;
- obbligo di cambio delle password con frequenza almeno semestrale durante la fase di esercizio richieste dal dornitore Infocamere;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro assicurato dal fornitore Infocamere;
- conservazione, a cura del gestore Infocamere,delle copie di riserva dei dati e dei documenti negli stessi locali in cui è installato il sistema di elaborazione che ospita il programma di protocollo;
- impiego e manutenzione di un adeguato sistema antivirus;
- archiviazione giornaliera? delle copie del registro di protocollo.

2.0 Formazione del personale

Con riferimento al Piano di Formazione del personale, 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
- effettuazione degli interventi formativi
- valutazione degli interventi.

2.1 Continuità operativa

2.1.1 Continuità operativa del Servizio
2.1.2 Continuità Operativa del Sistema

La continuità operativa del Sistema di Gestione Documentale si basa sul Piano di Continuità Operativa e sul Piano di Disaster Recovery di Infocamere, in quanto il predetto Sistema di Gestione è ospitato su infrastruttura IT di InfoCamere.
, Pertanto, il Sistema di Gestione Documentale 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.

MONITORAGGIO E CONTROLLI

3.0 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]

3.1 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	08:00 – 21:00 Lunedì – Venerdì 08:00 – 14:00 Sabato
disponibilità del servizio	migliore del 99%
RTO	72 ore
RPO	24 ore

LEGENDA

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.

3.2 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 comunicareil problema riscontrato al Responsabile del Servizio di Gestione documentale.
La predetta comunicazione deve essere effettuata (anche tramite email) entro due ore all'interno dell'orario di servizio dal lunedì al venerdì.

3.3 Monitoraggio dell'infrastruttura IT

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

3.3.1 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 supporto24 ore x 365 giorni.

3.3.2 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.

3.3.3 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.

POLITICHE DI SICUREZZA

4.0 Politica di gestione della sicurezza dei sistemi

Il Sistema di Gestione Documentale, in quanto ospitato su infrastruttura IT di InfoCamere è gestito dal punto di vista infrastrutturale sempre da InfoCamere, anche con riferimento alle politiche di sicurezza.

4.0.1 Inventario degli asset IT
4.0.2 Inficamere garantisce che siano identificati gli asset associati ad informazioni e a strutture di elaborazione delle informazioni e cural'inventario di tali asset, assicurandone la pubblicazione ed il continuo aggiornamento. 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.

4.0.3 Resource Capacity Management

Infocamere, 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.

4.0.4 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.

4.0.5 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).

4.0.6 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 va effettuata, da parte dei Responsabili delle competenti S.O. 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, 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.

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

Obiettivo fondamentale della Sicurezza delle Informazioni nell'Ente.è assicurare una corretta politica per il controllo degli accessi logici ??limitando ll'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.
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.

4.1.1 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;
- 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;
- Nessun identificativo di accesso dovrà essere cancellato ma dovranno essere eliminate le abilitazioni;
- Gli identificativi utente assegnati una volta non potranno più essere assegnati successivamente a persone diverse;
- 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 abilitatosi occorre 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.

Le richieste relative alla gestione delle credenziali d'accesso sono indirizzate ad InfoCamere che provvede, 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.

4.1.2 Utilizzo delle password

Si precisano le seguenti regole che attengono all'utilizzo delle password:

- 'utilizzo e la gestione delle credenziali deve garantire di evitare utilizzi impropri delle password e delle credenziali di autenticazione.

- le regole relative alla costruzione ed utilizzo delle password si applicano a tutto il personale e terze parti che ne fanno uso per accedere agli asset 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.
- Le predette disposizioni valgono anche per i cosiddetti PIN dei dispositivi con a bordo certificati digitali. (smart card etc.).

4.1.3 Responsabilità degli utenti

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.

4.1.4 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:

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

Esecuzione degli accessi

InfoCamere garantisce anche la corretta gestione degli accessi prevedendo,

- procedure di log-on sicure.
- controllo degli accessi alle applicazioni ed alle informazioni
  n base al principio di necessità
- password di accesso
  Infine, la strumentazione tecnica utilizzata da InfoCamere per la gestione delle password di accesso ai servizi forniti, è coerente con la politica.

4.2 Politica di gestione delle postazioni di lavoro

La politica della gestione delle postazioni di lavoro con specifico riferimento al Servizio di gestione documentale prevede le seguenti azioni::

- **ggiornamenti del software:**

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

- **imitazione 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.

- **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,nonché neidispositivi mobili o supporti rimovibili affidati in dotazione individuale, senza specifica autorizzazione

- **configurazione delle postazioni di lavoro**

Il Sistema di Gestione Documentalelato utente è reso disponibile in modalità di navigazione sul web: pertanto le postazioni di lavoro ed i browser devono essere configurati secondo le specifiche tecniche riportate nel Manuale di configurazione [MCF CLIENT].

- **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.??

4.3 Politica di gestione, dismissione e smaltimento degli apparati mobili e dei supporti
4.4 La politica di gestione, dismissione e smaltimento degli apparati mobili e dei supporti prevede il rispetto delle seguenti regole

:

- **gestione apparati e supporti informatici**

Gli apparati e i supporti informatici devono essere protetti da accessi non autorizzati, utilizzi impropri, manomissioni, danneggiamento o furti siadurante il loro utilizzo all'interno e all'esterno delle sedi dell'Ente, che duranteil trasporto ed infine nei peridi di inattività.

In particolare, con riguardo alla postazioni di lavoro mobili esse

sono assegnate personalmente al personale
Il personale è autorizzato a portare con sé al di fuori delle sedi dell'Ente gli apparati mobili assegnati.
La memorizzazione di dati personali non aziendali da parte del personale su apparati mobili non è ammessa a meno di esplicita autorizzazione da parte dell'Ente (esempio: smartphone in comodato d'uso).

- **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.

- **gestione supporti cartacei**

le informazioni presenti sui supporti cartacei (documenti, appunti) non devoni essere lasciate dal personale in luoghi 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.
la documentazione riservata deve essere gestita con particolare cura anche all'esterno delle sedi dell'Ente.

- **dismissione supporti cartacei**

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

4.5 Politica di protezione dal malware

La politica di protezione dal malware preved il rispetto delle seguenti regole: (le informazioni di proprietà dell'Ente o da essa gestite e le infrastrutture IT preposte alla loro elaborazione devono essere protette contro il malware.

- devono essere 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.

Al riguardo sono introdotte le seguenti misure di sicurezza:

- **contromisure per la protezione dal malware**

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 sui sistemi virtuali in uso presso 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.

- **contromisure per la protezione dallo spamming**

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

- controllare le informazioni di provenienza dei messaggi
- , 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 Pulizia della scrivania e dello schermo

La politica relativa alla pulizia della scrivania e dello schermo prevede il rispetto delle segueni regole da parte
dal personale dell'Ente, dai fornitori e dalle terze parti.

scrivania pulita

Le regole 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, 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 "savescreen" 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).