Camera di Commercio
Pavia

ALLEGATO 8

AL MANUALE DI GESTIONE DOCUMENTALE CCIAA PAVIA

Approvato con

Determinazione del Commissario Straordinario

n. 9 del 23 marzo 2022

PIANI DELLA SICUREZZA

Piano della sicurezza informatica

Sommario

1 Premessa

Il Piano per la sicurezza informatica (art.4, comma 1, lett. C, del D.P.C.M. 3 dicembre 2013) è redatto in ottemperanza delle misure minime ai sensi del CAD e del Regolamento 2016/679 - GDPR - Garante Privacy.

Occorre premettere che la gestione informatica dei dati di cui la Camera è titolare è realizzata, in modo prevalente, tramite i prodotti e i servizi erogati da Infocamere S.c.p.A., società consortile di informatica delle Camere di Commercio italiane, o da società ad essa collegate nominate dalla Camera come Responsabili del trattamento ai sensi del GDPR e sulla rete di trasmissione dati IC rete gestita da Infocamere in ambito nazionale per l'archiviazione e la trasmissione dei dati facenti parte del patrimonio informativo delle Camere di Commercio. La Camera opera nella rete Infocamere che la società gestisce sotto tutti i profili, compreso quello della sicurezza. Si rinvia pertanto ai documenti prodotti dalla Società per la descrizione di tutti i relativi aspetti.

2 Misure di sicurezza

Nella presente sezione sono illustrate le misure individuate ai fini di garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità.

In quanto tale si intende descrivere, con le misure di sicurezza in essere, un quadro di riferimento organico che possa risultare utile per il perfezionamento e l'aggiornamento nel tempo di procedure, modalità, regole e prescrizioni in materia e per operazioni di verifica e controllo da attuarsi periodicamente.

La Camera di Pavia, al fine di incrementare il livello di sicurezza e semplificare la gestione degli strumenti informatici, ha adottato la tecnologia Virtual Desktop Infrastructure (VDI) che consente di avere postazioni di lavoro sempre performanti e configurate in modo idoneo alle sole attività lavorative. Al desktop virtuale si accede, con user-id e password, attraverso il pc fisico.

2.1 Definizione dell'ambito con riferimento al trattamento elettronico dei dati

Gli archivi gestiti elettronicamente con strumenti informatici comprendono sia banche dati gestite internamente che banche dati gestite dalla Società consortile Infocamere o da altre società del gruppo.

Per l'analisi dei rischi e le prescrizioni per la sicurezza delle banche dati gestite da Infocamere e dalle altre società del gruppo, e da Infocert spa si rinvia ai documenti redatti dalle società, nominate dalla Camera Responsabili del trattamento.

Rientrano nell'ambito sopradescritto i trattamenti gestiti con strumenti informatici da soggetti esterni, ma facenti capo all'Ente camerale.

2.2 Apparecchiature informatiche critiche

Sono considerate apparecchiature informatiche critiche quelle apparecchiature che vengono utilizzate per il trattamento di dati personali:

- ✓ computer (sia server che workstation);
- ✓ unità input/output accessorie a dischi ottici o magnetici, unità nastri e supporti USB;
- ✓ sistemi per la gestione delle LAN (router, switch, ecc.).

Tali apparecchiature sono collocate in aree ad accesso riservato.

2.3 Supporti di memorizzazione critici

Sono considerati supporti di memorizzazione critici i nastri magnetici, le cassette (cartridge), i dischi magnetici o ottici rimovibili, i CD-ROM e DVD, HD, supporti USB ecc. che contengono informazioni personali.

I supporti di memorizzazione critici devono essere custoditi in un'area ad accesso controllato o in un ufficio che è chiuso quando non presidiato e comunque in un armadio/cassetto chiuso a chiave.

2.4 Informazioni residue

Sono definite informazioni residue quei dati personali ancora leggibili dopo la cessazione di un trattamento (es. nastri, dischi magnetici, dischi ottici, HD, supporti USB ecc.).

Le informazioni residue devono essere rese inaccessibili e illeggibili quando non sia più necessario conservarle per gli scopi per cui i dati sono stati raccolti e trattati. In caso di dismissione di apparecchiature o supporti - sia che se ne preveda lo smaltimento sia il riciclo - vanno osservate le prescrizioni dettate dal Garante con provvedimento del 13 ottobre 2008 (Rifiuti di apparecchiature elettriche ed elettroniche -Raae e misure di sicurezza dei dati personali) e le misure tecniche suggerite negli allegati al provvedimento citato o successivamente indicate per la cancellazione sicura delle informazioni.

3 Sicurezza logica. Prescrizioni generali

Questa sezione disciplina i diversi aspetti del controllo dell'accesso logico alle informazioni personali. Quale principio generale sono regolamentati gli accessi ai server, alle workstation, alle LAN, alla rete e alle banche dati del sistema Informatico camerale attraverso funzioni di identificazione e autenticazione degli utenti.

Tali funzioni assicurano che ad ogni potenziale utente dei sistemi o delle banche dati siano associate delle credenziali di autenticazione consistenti in un codice per l'identificazione (userid) ed una parola chiave riservata (password), conosciuta solo dall'utente medesimo, oppure di un dispositivo di autenticazione in possesso e uso esclusivo dell'utente. Tali credenziali o dispositivi di autenticazione consentono, ad ogni accesso dell'utente alla rete, al sistema o alla banca dati, di verificarne l'identità e di garantirne l'accesso ai dati di cui è incaricato tramite il sistema di autorizzazione agli accessi.

3.1 User-id

L'accesso ai sistemi, alle banche dati contenenti informazioni personali, o alla rete deve essere basato sulle effettive necessità del trattamento. Per ragioni meramente tecniche, ad ogni utente possono essere assegnate una o più credenziali per l'autenticazione. In ogni caso, le user-id assegnate devono sempre essere riconducibili ad un singolo individuo e non possono essere assegnate ad altri utenti neppure in tempi diversi.

Le credenziali ed i dispositivi di autorizzazione sono custoditi con particolare perizia e cautela sotto la responsabilità personale degli utenti consegnatari.

Le credenziali ed i dispositivi di autorizzazione non utilizzati, ad eccezione di quelli creati per scopi tecnici, devono essere disattivati.

3.2 Assegnazione e revoca delle user-id ed abilitazioni

La procedura tecnica per l'assegnazione delle user-id che permettono l'accesso ai sistemi, alle banche dati ed alla rete del Sistema Informatico camerale viene normalmente gestita da Infocamere. Può essere gestita propriamente dall'Ente nel caso in cui si tratti di accessi a sistemi e banche dati gestiti direttamente dall'Ente. Parimenti, per i sistemi e banche dati gestiti da terzi (diversi da Infocamere), questi normalmente provvedono all'assegnazione delle relative credenziali di autorizzazione all'accesso. L'abilitazione, con la connessa individuazione di uno specifico profilo di autorizzazione all'accesso, avviene in ogni caso su richiesta diretta del responsabile della struttura cui appartiene l'incaricato che ne deve essere titolare.

Quando un utente non ha più la necessità di accedere ad una banca dati, lascia l'Ente o comunque non utilizza da almeno sei mesi le credenziali, il diretto superiore dell'utente interessato provvede a richiedere al soggetto che ha rilasciato le credenziali di autorizzazione la disabilitazione dell'utenza.

Le user-id attribuite da Infocamere, per l'accesso alla rete o per procedure gestite dalla stessa o da società del gruppo, e da Infocert, qualora siano inutilizzate per più di 6 mesi, vengono automaticamente disattivate.

Non è consentito il riutilizzo di una user-id personale già assegnata ad altro utente.

3.3 Password

La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati ed un corretto utilizzo delle stesse rappresenta un pilastro fondamentale nella gestione complessiva della sicurezza, anche nell'ottica di garanzia e tutela degli utenti. Le regole di seguito elencate sono vincolanti per tutti i sistemi e le workstation tramite le quali si può accedere alla rete ed alle banche dati contenenti dati personali.
Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo.

3.4 Regole delle password

- La lunghezza minima della password è di 8 caratteri.
- Deve contenere almeno un carattere alfabetico ed uno numerico.
- Non deve essere simile alle due password precedenti.
- Non deve contenere l'user-id come parte della password.
- Non deve contenere riferimenti agevolmente riconducibili all'utente;
- Deve essere cambiata al primo utilizzo ed almeno ogni 6 mesi (3 mesi se afferente dati sensibili o giudiziari).
- Non deve essere comunicata ad altri utenti.

Dove la tecnologia lo permette, tali regole sono rese obbligatorie dal software altrimenti è responsabilità dell'utente rispettarle.

3.5 Ripristino della password

Laddove i sistemi non consentano automatismi per il ripristino o nel caso di impossibilità, il ripristino della password, in caso di blocco della stessa, deve essere effettuato solo a fronte di una diretta richiesta da parte dell'intestatario, rispettando le istruzioni e nei casi all'uopo previsti. La password dovrà essere cambiata subito dopo a cura del richiedente.

3.6 Utilizzo delle password

Nell'utilizzo dei sistemi informatici sono definiti più livelli di password:

- richiesta dal sistema operativo nella fase di avvio del computer;
- richiesta quando si intende accedere alla rete (sia Intranet che Internet);
- richiesta per l'utilizzo di specifiche applicazioni;
- richiesta dal salvaschermo per i momenti in cui si lascia incustodita la postazione di lavoro.

Si devono utilizzare tutti questi livelli di password. Tutte le operazioni inerenti l'utilizzo delle password (digitazione, cambiamento, ecc.) devono essere compiute con estrema cautela e discrezione avendo cura di controllare che tali operazioni non siano visibili a terzi.

3.7 Accesso agli elaboratori in caso di prolungata assenza o impedimento dell'incaricato

Ferma l'effettuazione della custodia delle copie delle credenziali, con le caratteristiche, anche di segretezza ai fini dell'accesso da parte del titolare in caso di prolungata assenza o impedimento dell'incaricato si è ritenuto confacente alle esigenze di sicurezza prevedere una procedura consistente in:

- disabilitazione della componente riservata della credenziale per l'autenticazione dell'incaricato assente;
- abilitazione di una nuova credenziale che consenta l'accesso al titolare;
- configurazione di una nuova credenziale per l'accesso da parte dell'incaricato autorizzato.

Tale procedura potrà essere attuata dando notizia, come prescritto, all'incaricato, dell'evenienza occorsa, e solo in casi di indifferibile necessità di accesso ai dati, su richiesta scritta del titolare o del responsabile. La custodia delle password degli amministratori di sistema è realizzata su supporto cartaceo e formalmente affidata al Provveditore.

4 Prescrizioni particolari per la sicurezza logica dei sottosistemi del Sistema Informativo camerale

4.1 Rete

In un sistema integrato, quale quello in cui opera l'Ente, la sicurezza deve essere trattata in modo uniforme, in quanto l'insicurezza di una singola parte si può ripercuotere generando insicurezza in tutto il sistema. Questo vale in particolare per gli aspetti di sicurezza della rete. ICRete, rete geografica del Sistema Informatico Camerale, è gestita da InfoCamere ed InfoCamere stessa ha primariamente il compito di assicurarne la sicurezza.
La Camera di Commercio di Pavia collabora con Infocamere per la gestione in sicurezza della parte di rete di propria pertinenza, assicurando che le direttive generali di Infocamere siano rispettate e che siano adottate tutte le ulteriori specifiche fissate dall'Ente.
Per garantire la sicurezza di una rete è fondamentale controllare gli accessi alla rete stessa. Per questo qui di seguito sono formulate alcune prescrizioni particolari per le connessioni di ICRete. Sono considerate connessioni con l'esterno i collegamenti di ICRet e con altre reti, in particolare:

- interconnessioni tra i servizi informatici e telematici di InfoCamere e quelli di altre aziende, incluso Internet;
- accesso remoto da parte di dipendenti della Camera o di InfoCamere, secondo le procedure e le stringenti misure di sicurezza stabilite da Infocamere e solo per i soggetti espressamente abilitati.

4.2 Accesso remoto e uso dei modem

Le connessioni via modem tra i sistemi e la rete del Sistema Informatico camerale con reti e sistemi esterni possono rappresentare un serio rischio per la sicurezza del Sistema stesso.
Come conseguenza diretta di collegamenti non corretti dal punto di vista della sicurezza, è possibile che si esponga a rischio l'intero sistema informativo ed i dati in esso contenuti; nei fatti ciò può avvenire senza che il dipendente se ne renda conto.
Per tale motivo ogni collegamento dall'interno verso l'esterno (e viceversa) deve rispettare i criteri di sicurezza qui esposti. In particolare, nel caso in cui il collegamento sia di tipo TCP/IP tramite modem, non è permesso il suo uso simultaneamente al collegamento interno. Si fa preciso divieto di installare modem o di eludere la connessione ufficiale IC salvo casi espressamente autorizzati.
In caso di collegamento dall'esterno al Sistema Informatico camerale è necessario l'utilizzo della connessione sicura fornita da Infocamere ScpA tramite il servizio VPN (Virtual Private Network) o Virtual desktop (VDI).

4.3 Ridondanza nelle apparecchiature di rete e collegamento

Al fine di garantire la massima continuità di servizio possibile tutte le apparecchiature di rete che consentono l'interconnessione con ICRete sono ridondate e manutenute da Infocamere. È presente ed attivo un collegamento ausiliario di backup sia per bilanciare il carico in caso di intenso traffico di rete sia per soprassedere ad indisponibilità del collegamento principale. Tutti gli apparati di rete

sono collegati a gruppi di continuità per assicurarne la disponibilità in caso di brevi blackout elettrici nonché per proteggerle da sbalzi di tensione elettrica.

4.4 Sistemi e stazioni interconnesse

A livello di singole stazioni interconnesse la gestione della sicurezza è affrontata seguendo due principali filoni:

1. Server di dati;
2. Personal Computer.

4.5 Server

La CCIAA di Pavia non dispone di server di applicazioni. Gli applicativi sono infatti forniti da Infocamere tramite servizio web e utilizzabili quindi tramite browser oppure in modalità client/server. Altre applicazioni sono invece installate sui singoli PC.

Il server di dati è fornito da Infocamere tramite servizio di hosting remoto replicato in modo da garantire la continuità operativa e la gestione di "disaster recovery". Tale servizio comprende attività di help desk, backup e restore di dati, protezione mediante firewall, sistemi IPS e anti-DDOs, patching dei sistemi operativi, antivirus.

L'accesso ai server dati è possibile solo da parte di personale autorizzato. In base a quanto previsto dal Provvedimento del 27.11.2008 del Garante, riguardante gli amministratori di sistema, le operazioni di accesso sono tracciate in appositi file di log. In essi è installato un antivirus sempre attivo.

I sistemi operativi sono costantemente aggiornati in modo coerente alle applicazioni che mettono a disposizione, in modo da garantire il più alto livello di sicurezza possibile.

4.6 Personal Computer

I Personal Computer (o workstation), ossia le singole stazioni di lavoro degli utenti, devono avere le seguenti caratteristiche:

- in ogni caso, è fatto divieto al personale di installare o disinstallare applicazioni, nonché modificare le configurazioni delle stesse e di accesso al sistema senza darne preventiva comunicazione scritta all'Ufficio Provveditorato. L'Ufficio Provveditorato, valutate tutte le implicazioni in tema di sicurezza e compatibilità delle stesse con l'ambiente di lavoro, qualora non ritenga di dover provvedere in modo diretto, autorizza sotto la propria responsabilità le operazioni di installazione, disinstallazione e riconfigurazione per iscritto;
- qualora l'Ufficio Provveditorato verifichi la presenza sulle stazioni di software non autorizzato è tenuto a darne tempestiva comunicazione scritta alla Dirigenza competente, al fine dell'adozione dei più opportuni provvedimenti. Le informative e comunicazioni per iscritto possono essere effettuate anche tramite messaggi di posta elettronica;
- le stazioni sono protette da un sistema di antivirus di rete che deve essere sempre attivo e aggiornato. Nel caso in cui l'utente verifichi la temporanea indisponibilità del servizio di antivirus, deve darne tempestiva comunicazione all'Ufficio Provveditorato che individuerà

ed attuerà tutte le azioni necessarie per il ripristino nel tempo più celere possibile delle normali condizioni di sicurezza;

- i sistemi operativi sono aggiornati con tutte le patch di sicurezza testate e compatibili con le applicazioni installate, mediante procedure automatiche ricomprese nel servizio di hosting del server (WSUS).

4.7 Applicazioni

L'utilizzo di applicazioni che consentano di gestire informazioni e dati personali deve avvenire in maniera consapevole e sicura da parte del personale incaricato. Tali requisiti sono soddisfatti attraverso l'effettuazione di peculiari azioni formative sul personale e la strutturazione opportuna delle caratteristiche di funzionamento del software utilizzato.
In particolare, al fine di prevenire al massimo errori accidentali di cancellazione o modifica dei dati le applicazioni che gestiscono informazioni e dati personali devono sempre segnalare adeguatamente la criticità di particolari operazioni effettuate (schema richiesta e successiva conferma).

4.8 Posta elettronica

L'utilizzo di applicazioni di posta elettronica rappresenta un forte fattore di rischio per i sistemi sui quali sono installate, in quanto espone gli stessi a minacce dirette derivanti dalle comunicazioni con l'esterno. Per questo è necessario disciplinare l'utilizzo della stessa in modo da ridurre al massimo i rischi connessi. Pertanto, quale principio generale, è fatto divieto al personale dell'Ente di utilizzare la rete e le applicazioni installate sulle postazioni di lavoro per finalità diverse da quelle inerenti l'attività dell'ufficio.
La posta elettronica assegnata al personale viene filtrata da un servizio di antivirus centralizzato presente sui sistemi del fornitore di posta elettronica. Inoltre, su tutte le stazioni di lavoro è installato ed attivo il servizio di antivirus locale fornito da Infocamere. Ciò detto, si raccomanda di cancellare immediatamente (anche dal "Cestino") tutti i messaggi provenienti da mittenti non precisamente identificabili e con oggetto non pertinente l'attività dell'ufficio senza visualizzarli direttamente o in anteprima.
Nel caso in cui l'utente rilevi dubbi circa la pertinenza o meno di un messaggio alla propria attività deve informare l'Ufficio Sistema informatico che provvederà a verificare il contenuto dello stesso in un ambiente sicuro ed isolato da ICRete.
È importante ricordare che la contraffazione dell'indirizzo del mittente nei messaggi di posta elettronica è un'operazione molto semplice. Quindi in generale è opportuno non aprire né tanto meno installare file o programmi ricevuti via posta elettronica da fonti non conosciute o dalle quali non si attendono comunicazioni. Per l'apertura di questi allegati è necessario utilizzare la stessa procedura sopra descritta per la verifica della pertinenza all'attività dell'ufficio dei messaggi ricevuti.

4.9 Dati

Quale principio generale le informazioni contenenti dati personali devono essere archiviate sulle aree del server camerale (servizio di hosting remoto replicato di Infocamere). I dati sono protetti indirettamente anche attraverso la creazione di appositi profili di gestione degli stessi nelle applicazioni e la protezione dell'accesso logico e fisico al repository finale (cartella) in cui sono collocati.

É fatto divieto di salvare dati sui singoli PC, salvataggio dati e conservazione devono avvenire sulle apposite aree del server.

4.10 Web filtering

Nel rispetto dello Statuto dei lavoratori e rispettando le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, al fine di ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività), la Camera di Commercio ha adottato il sistema di "webfiltering" fornito da Infocamere al mondo camerale che consente di inibire l'accesso a categorie di siti reputati non pertinenti con l'attività lavorativa o poco sicuri.

Le attività sull'uso del servizio di accesso ad internet (LOG) vengono automaticamente registrate in forma elettronica da Infocamere (PROVIDER) e da questa conservate nei termini di legge.

5 Criteri e modalità di ripristino della disponibilità dei dati

5.1 Introduzione

La presente sezione si pone come obiettivo quello di descrivere i criteri e le procedure adottate per il salvataggio dei dati e per il loro ripristino in caso di danneggiamento o di inaffidabilità della base dati.

Il principio generale adottato dall'Ente in tal ambito è che tutti i dati devono essere archiviati esclusivamente sui server dati appositamente creati e predisposti allo scopo. Su di essi devono confluire anche tutti gli elenchi, query e report estratti da banche dati gestite da Infocamere o terzi che contengano dati personali ed anche le informazioni interne riservate e confidenziali prodotte dagli uffici.

Sulle singole workstation possono essere memorizzate informazioni e dati di lavoro temporanei di non particolare rilevanza (purché non siano dati personali) in modo tale che la loro eventuale perdita, distruzione o alterazione non comporti alcun pregiudizio al rispetto delle politiche di sicurezza adottate.

Per le finalità del presente documento si definisce "insieme omogeneo di dati" ogni singola cartella generale collocata sui server che può contenere basi dati, sottocartelle contenenti dati o semplici file aventi una qualche relazione definita fra loro e quindi collocati nel medesimo ambito.

5.2 Backup

Le procedure di backup agiscono sul server camerale e non sui singoli PC. Tali procedure, così come previsto dal servizio di hosting remoto replicato di Infocamere, avvengono con cadenza giornaliera in modalità incrementale/differenziale ed una volta a settimana (solitamente sabato e/o domenica) tramite backup completo. I dati di backup vengono mantenuti disponibili per 12 settimane.

5.3 Ripristino

Il servizio di hosting remoto replicato di Infocamere garantisce il ripristino/restore dei dati con granularità fino al singolo file. La restore di singoli oggetti verrà eseguita a fronte di una richiesta da eseguire direttamente al supporto IC. É inoltre possibile provvedere al recupero di dati in modo autonomo tramite la funzionalità delle Shadow Copy.

Piano della Sicurezza
dei documenti informatici

VERSIONE LUGLIO 2016

Indice

1 INTRODUZIONE AL DOCUMENTO

1.1 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, con riferimento a quanto previsto nell'allegato B del Decreto legislativo 30 giugno 2003 n. 196.

Il documento costituisce un allegato al Manuale di Gestione Documentale (d'ora in avanti "Manuale") dell'Ente.
Esso approfondisce i contenuti del paragrafo "Sicurezza relativa alla gestione dei documenti informatici" del Manuale.

1.2 Ambito del Servizio di Gestione Documentale

Per la documentazione gestita dalla Camera di Commercio vengono utilizzati prevalentemente gli applicativi di Infocamere. La gestione documentale è effettuata a decorrere dall'8 settembre 2015 con l'applicativo Gedoc, che ha sostituito il precedente sistema di protocollazione informatica Prodigi. Fanno eccezione le tipologie documentarie individuate nel Manuale di Gestione.
Nello schema seguente si evidenziano i flussi documentali gestiti con applicativi forniti da altri soggetti:

Classe di Servizi	Servizio	Descrizione Classe / Servizio	Fornitore
Gestione Rilevazione Presenze (TEAMWEB)	Rilevazione presenze	Gestione delle timbrature di presenza	Selesta Ingegneria SPA
Portale prezzi	www.paviaprezzi.it	Portale che raccoglie le rilevazioni dei prezzi dei mercati di Pavia, Voghera, Mortara, Broni	Digicamere
Sito Istituzionale	www.pv.camcom.gov.it	Sito istituzionale	Digicamere

1.3 Livello di riservatezza

Livello	Ambito di diffusione consentito
Uso interno	Il documento può essere diffuso solo **all'interno** dell'Ente. E' consentito darne comunicazione a terzi con clausola di non diffusione.

1.4 Riferimenti normativi

CAD CO	Codice dell'Amministrazione Digitale, Decreto legislativo 7 marzo 2005, n. 82, art. 50 bis
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
TESTO UNICO	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
CODICE PRIVACY	Codice in materia di protezione dei dati personali, Decreto legislativo 30 giugno 2003 n. 196

1.5 Riferimenti documentali

SFT ENTE	Studio di Fattibilità Tecnica "Continuità operativa" – CAD art. 50 bis della Camera di Commercio di Pavia
MANUALE	Manuale di Gestione documentale dell'Ente
MCF CLIENT	Manuale Infocamere di configurazione della postazione di lavoro client

2 ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

2.1 Analisi del rischio IT

Individuazione degli asset

asset	descrizione
personale coinvolto	personale dipendente, personale con altre tipologie contrattuali
servizio	il Servizio di Gestione Documentale offerto agli utenti
documenti	documenti gestiti dal Sistema
dati personali	dati personali presenti nei documenti, registrazioni di protocollo
metadati relativi alle registrazioni di protocollo ed ai documenti	dati presenti nel sistema; esempio: dati di classificazione e fascicolazione
registro di protocollo	presente nel sistema
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
processi: protocollazione e classificazione	registrazione in entrata effettuata in modo centralizzato; protocollazione in uscita decentrata
processi: fascicolazione	gestiti dalle u.o. responsabili dei procedimenti
processi: copia per immagine su supporto informatico di documenti analogici	gestiti dall'ufficio protocollo
funzionalità del sistema	aree di usabilità del sistema in modalità autonoma e ambiti che comportano l'intervento del fornitore
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

Analisi delle minacce e vulnerabilità

Sono state ipotizzate le minacce e le vulnerabilità che insistono sugli asset in base ai seguenti criteri:

- standard di settore e best practice di sicurezza
- esperienza del personale
- indicazioni provenienti dagli audit interni
- suggerimenti e condivisioni da parte di esperti del settore

Per ogni minaccia o vulnerabilità valutare qualitativamente la probabilità di accadimento e l'impatto sull'Ente. La probabilità e l'impatto sono espressi dai livelli:

mB = molto Basso; **B** = Basso; **M** = Medio; **A** = Alto; **mA** = molto Alto

Le minacce e vulnerabilità che insistono sugli asset sono:

asset	minacce e vulnerabilità	P - probabilità	I - impatto
personale coinvolto	Poiché il Sistema informatico è di recente adozione, ne consegue che il personale potrebbe incontrare difficoltà nell'utilizzo e ciò provocherebbe una perdita di efficienza e di motivazione all'utilizzo.	M	A
	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al personale potrebbero essere sovra / sottodimensionati rispetto alle esigenze lavorative; ciò provocherebbe la difficoltà nell'utilizzo delle funzionalità necessarie.	M	A
documenti	Poiché un documento potrebbe essere accidentalmente o intenzionalmente cancellato o sostituito, ne potrebbero scaturire conseguenze negative per l'Ente (mancato avvio di un procedimento nei termini di legge, impossibilità di esibire l'originale del documento, ecc., con esiti di ordine civile e penale)	mB	mA
dati personali	Poiché alcuni documenti contengono dati sensibili, ne deriva che tali dati potrebbero essere indebitamente consultati; ciò provocherebbe la violazione del Codice Privacy, esponendo l'Ente a conseguenze risarcitorie nei confronti di terzi.	M	mA
Processi di protocollazione - metadati relativi alle registrazioni di protocollo – classificazione e fascicolazione	Poiché la classificazione e fascicolazione dei documenti è un'operazione complessa, ne consegue che un documento potrebbe venir classificato e fascicolato in modo non corretto e ciò provocherebbe difficoltà nelle successive ricerche; essendo in una fase di definizione di nuove regole di fascicolazione i metadati inseriti	M	M

asset	minacce e vulnerabilità	P - probabilità	I - impatto
	potrebbero essere incoerenti con le registrazioni di protocollo o i documenti archiviati		
registro di protocollo	Poiché l'applicativo di gestione documentale è di recente adozione, i sistemi di difesa dagli attacchi informatici potrebbero non essere adeguati, e il registro di protocollo potrebbe risultare danneggiato o alterato	B	A
processi di gestione documentale	In relazione alla necessità di modificare il workflow i processi di gestione documentale potrebbero essere poco conosciuti al personale	M	M
processi: copia per immagine su supporto informatico di documenti analogici	fino a quando non sarà quasi azzerato il flusso cartaceo si possono presentare rischi di malfunzionamento della strumentazione o errore da parte degli operatori	B	M
funzionalità del sistema	Poiché il Sistema è di recente produzione, ne consegue che alcune funzionalità potrebbero essere troppo complesse dal punto di vista operativo oppure potrebbero richiedere l'intervento dell'assistenza, provocando una scarsa tempestività dell'operatività degli Uffici.	M	A
infrastruttura IT	Poiché l'infrastruttura IT potrebbe essere coinvolta da malfunzionamenti, ne consegue che il Servizio di gestione documentale potrebbe essere non disponibile e ciò provocherebbe un blocco dei processi.	M	A
	Poiché potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di InfoCamere e degli altri fornitori, ne consegue che l'infrastruttura IT potrebbe venire distrutta e ciò provocherebbe l'indisponibilità del servizio per un lunghissimo periodo.	mB	mA
postazioni di lavoro	le postazioni di lavoro potrebbero essere infettate da malware; Data la sistemazione logistica di alcuni uffici aperti al pubblico durante le pause di lavoro le postazioni di lavoro potrebbero consentire l'interazione con il Sistema da parte di personale non autorizzato	M	A
dispositivi di firma	In caso venissero custoditi non correttamente i dispositivi di firma potrebbero essere sottratti indebitamente e utilizzati per la produzione di documenti apocrifi	B	A

Individuazione delle contromisure

Per ogni minaccia o vulnerabilità che insiste su un asset sono state individuate le misure da applicare, valutandone il grado di attuazione allo stato attuale, come sintetizzato nella tabella seguente. Il valore percentuale esprime l'entità di attuazione della singola misura per far fronte al rispettivo rischio; es. 100% indica una misura completamente attuata, 50% attuata parzialmente, ecc.).

Le contromisure individuate confluiscono nel " Piano di trattamento dei rischi".

Contromisure e stato di attuazione			
asset	**minacce e vulnerabilità**	**contromisure**	**grado di copertura**
personale coinvolto	Poiché il Sistema informatico è di recente adozione, ne consegue che il personale potrebbe incontrare difficoltà nell'utilizzo e questo accadimento provocherebbe una perdita di efficienza e di motivazione all'utilizzo.	- Piano di formazione adeguato - Incontri con il personale per raccogliere le problematiche e identificare soluzioni comuni	50%
	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al personale potrebbero essere sovra / sottodimensionati rispetto alle esigenze lavorative; ciò provocherebbe la difficoltà nell'utilizzo delle funzionalità necessarie	- verificare ogni 6 mesi l'adeguatezza dei profili (anche intervistando il personale)	50%
documenti	Poiché un documento potrebbe essere accidentalmente o intenzionalmente cancellato o sostituito, ne potrebbero scaturire conseguenze negative per l'Ente (mancato avvio di un procedimento nei termini di legge, impossibilità di esibire l'originale del documento, ecc., con conseguenze di ordine civile e penale)	- Piano di formazione adeguato - Invio da parte del personale di richieste di assistenza	50%
dati personali	Poiché alcuni documenti contengono dati sensibili, ne consegue che tali dati potrebbero essere indebitamente consultati; questo accadimento provocherebbe la violazione della normativa sulla Privacy esponendo l'Ente a conseguenze risarcitorie nei confronti di terzi.	- segnalazione almeno annuale da parte dei responsabili degli uffici e dei servizi circa la sussistenza e l'adeguatezza delle condizioni per la conservazione dei profili di autorizzazione; - verifica a campione la corretta archiviazione dei documenti contenenti dati sensibili	0%
Processi di protocollazione - metadati relativi alle registrazioni di protocollo –	Poiché la classificazione e fascicolazione dei documenti è un'operazione complessa, ne consegue che un documento potrebbe venir classificato e fascicolato in modo non corretto e	- Piano di formazione adeguato - Controlli a campione effettuati dall'ufficio protocollo sulla coerenza dei dati di	25%

Contromisure e stato di attuazione			
asset	**minacce e vulnerabilità**	**contromisure**	**grado di copertura**
classificazione e fascicolazione	ciò provocherebbe difficoltà nelle successive ricerche; essendo in una fase di definizione di nuove regole di fascicolazione i metadati inseriti potrebbero essere incoerenti con le registrazioni di protocollo o i documenti archiviati	classificazione e di fascicolazione	
registro di protocollo	Poiché l'applicativo di gestione documentale è di recente adozione, i sistemi di difesa dagli attacchi informatici potrebbe non essere adeguato, e il registro di protocollo potrebbe risultare danneggiato o alterato	Verifica del livello di disponibilità garantito da InfoCamere per il Sistema di gestione documentale in relazione ai livelli di servizio descritti nell'*Estratto delle Politiche e delle caratteristiche di sicurezza del Servizio di Gestione documentale*	100%
processi di gestione documentale	In relazione alla necessità di modificare il workflow i processi di gestione documentale potrebbero essere poco conosciuti al personale	Definizione di linee guida d'intesa con il Dirigente e diffusione dei contenuti del Manuale di Gestione	50%
processi: copia per immagine su supporto informatico di documenti analogici	fino a quando non sarà quasi azzerato il flusso cartaceo si possono presentare rischi di malfunzionamento della strumentazione o errore da parte degli operatori	Promozione dell'utilizzo della pec e della firma digitale da parte degli utenti	50%
funzionalità del sistema	Poiché il Sistema Gedoc è di recente produzione, ne consegue che alcune funzionalità potrebbero essere troppo complesse dal punto di vista operativo oppure potrebbero richiedere l'intervento dell'assistenza e questo accadimento provocherebbe una scarsa tempestività dell'operatività degli Uffici.	Definizione di una sequenza operativa per la segnalazione all'Ufficio Protocollo e a InfoCamere	0%
infrastruttura IT	Poiché l'infrastruttura IT potrebbe essere coinvolta da malfunzionamenti, ne consegue che il Servizio di gestione documentale potrebbe essere non disponibile e ciò provocherebbe un blocco dei processi.	Verifica del livello di disponibilità garantito da InfoCamere per il Sistema di gestione documentale in relazione ai livelli di servizio descritti nell'*Estratto delle Politiche e delle caratteristiche di sicurezza del Servizio di Gestione documentale*	100%
	Poiché potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di InfoCamere, ne consegue che l'infrastruttura IT potrebbe	Verifica circa l'inserimento de Sistema di gestione documentale nel Piano di Continuità operativa dell'Ente	100%

Contromisure e stato di attuazione			
asset	**minacce e vulnerabilità**	**contromisure**	**grado di copertura**
	venire distrutta e ciò provocherebbe l'indisponibilità del servizio per un lunghissimo periodo.		
postazioni di lavoro	le postazioni di lavoro potrebbero essere infettate da malware; data la sistemazione logistica di alcuni uffici aperti al pubblico durante le pause di lavoro le postazioni di lavoro potrebbero consentire l'interazione con il Sistema da parte di personale non autorizzato	Piano di formazione; verifica del grado di protezione degli antivirus	50%
dispositivi di firma	In caso venissero custoditi non correttamente i dispositivi di firma potrebbero essere sottratti indebitamente e utilizzati per la produzione di documenti apocrifi	Piano di formazione	50%

Calcolo del Rischio

Per la valutazione del **rischio "intrinseco"** che ogni minaccia o vulnerabilità comporta per i singoli asset si è considerato il prodotto tra i parametri della probabilità e quelli dell'impatto, tenendo conto dei valori sopraindicati. Il rischio intrinseco viene considerato indipendentemente dalle contromisure. La seguente tabella associa ai valori di probabilità e impatto il corrispondente valore di rischio:

probabilità . impatto	**rischio**
mB.mB	Basso
mB.B	Basso
mB.M	Basso
mB.A	Basso
mB.mA	Medio
B.mB	Basso
B.B	Basso
B.M	Medio
B.A	Medio
B.mA	Alto
M.mB	Basso
M.B	Medio
M.M	Medio
M.A	Alto
M.mA	Altissimo

A.mB	Basso
A.B	Medio
A.M	Medio
A.A	Alta
A.mA	Altissimo
mA.mB	Medio
mA.B	Medio
mA.M	Alto
mA.A	Altissimo
mA.mA	Altissimo

Per parametrare il **rischio "residuo"** si è considerato il grado di copertura del corrispondente rischio intrinseco come sopra individuato; lo strumento per la mappatura del rischio residuo è esposta nella tabella che segue:

rischio intrinseco	**grado di copertura**	**rischio residuo**
Altissimo	100%	Basso
Alto	100%	Basso
Medio	100%	Basso
Basso	100%	Basso
Altissimo	parziale	da valutare caso per caso
Alto	parziale	da valutare caso per caso
Medio	parziale	da valutare caso per caso
Basso	parziale	da valutare caso per caso
Altissimo	0%	Altissimo
Alto	0%	Alto
Medio	0%	Medio
Basso	0%	Basso

Sulla base della griglia sopra riportata sono stati individuati i valori dei rischi residui in relazione alle corrispondenti minacce rilevate per ciascun asset. Tenendo conto dei livelli di copertura attuale del rischio si sono programmate le contromisure secondo quanto descritto nella seguente tabella che costituisce il "Piano di trattamento dei rischi"

Piano di trattamento dei rischi				
Asset	**minacce e vulnerabilità**	**rischio intrinseco**	**rischio residuo**	**Programmazione contromisure**
personale coinvolto	Poiché il Sistema informatico è di recente adozione, ne consegue che il personale potrebbe incontrare difficoltà nell'utilizzo e ciò provocherebbe una perdita di efficienza e di motivazione all'utilizzo.	Alto	Basso	Mitigazione tramite il perfezionamento delle misure individuate nella tabella *Contromisure e stato di attuazione*
	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al personale potrebbero essere sovra / sottodimensionati rispetto alle esigenze lavorative; ciò provocherebbe la difficoltà nell'utilizzo delle funzionalità necessarie	Alto	Alto	Mitigazione tramite il perfezionamento delle misure individuate nella tabella *Contromisure e stato di attuazione*
Documenti	Poiché un documento potrebbe essere accidentalmente o intenzionalmente cancellato o sostituito, ne potrebbero scaturire conseguenze negative per l'Ente (mancato avvio di un procedimento nei termini di legge, impossibilità di esibire l'originale del documento, ecc., con	Medio	Basso	Mitigazione tramite il perfezionamento delle misure individuate nella tabella *Contromisure e stato di attuazione*

	conseguenze di ordine civile e penale			
dati personali	Poiché alcuni documenti contengono dati sensibili, ne consegue che tali dati potrebbero essere indebitamente consultati; ciò provocherebbe la violazione della normativa sulla Privacy esponendo l'Ente a conseguenze risarcitorie nei confronti di terzi.	Altissimo	Altissimo	Mitigazione tramite il perfezionamento delle misure già individuate nella tabella *Contromisure e stato di attuazione*
Processi di protocollazione - metadati relativi alle registrazioni di protocollo – classificazione e fascicolazione	Poiché la classificazione e fascicolazione dei documenti è un'operazione complessa, ne consegue che un documento potrebbe venir classificato e fascicolato in modo non corretto e ciò provocherebbe difficoltà nelle successive ricerche; essendo in una fase di definizione di nuove regole di fascicolazione i metadati inseriti potrebbero essere incoerenti con le registrazioni di protocollo o i documenti archiviati	Medio	Medio	Mitigazione tramite il perfezionamento delle misure individuate nella tabella *Contromisure e stato di attuazione*
registro di protocollo	Poiché l'applicativo di gestione documentale è di recente adozione, i sistemi di difesa dagli attacchi informatici	Medio	Basso	in caso di malfunzionamenti, verifica del rispetto dell'attuazione delle misure descritte nell'*Estratto delle Politiche e delle caratteristiche di sicurezza del Servizio di Gestione documentale di Infocamere*

	potrebbe non essere adeguato, e il registro di protocollo potrebbe risultare danneggiato o alterato			
processi di gestione documentale	In relazione alla necessità di modificare il workflow i processi di gestione documentale potrebbero essere poco conosciuti al personale	Medio	Basso	Perfezionamento delle misure individuate nella tabella *Contromisure e stato di attuazione*
processi: copia per immagine su supporto informatico di documenti analogici	fino a quando non sarà quasi azzerato il flusso cartaceo si possono presentare rischi di malfunzionamento della strumentazione o errore da parte degli operatori	Medio	Basso	Accettazione
funzionalità del sistema	Poiché il Sistema è di recente produzione, ne consegue che alcune funzionalità potrebbero essere troppo complesse dal punto di vista operativo oppure potrebbero richiedere l'intervento dell'assistenza e questo accadimento provocherebbe una scarsa tempestività dell'operatività degli Uffici.	Alto	Alto	Mitigazione tramite la definizione di verifiche sulla tempestività e sull'efficacia degli interventi risolutivi in risposta alle segnalazioni di malfunzionamento

infrastruttura IT	Poiché l'infrastruttura IT potrebbe essere coinvolta da malfunzionamenti, ne consegue che il Servizio di gestione documentale potrebbe essere non disponibile e questo accadimento provocherebbe un blocco dei processi.	Alto	Basso	in caso di malfunzionamenti, verifica del rispetto dell'attuazione delle misure descritte nell' *Estratto delle Politiche e delle caratteristiche di sicurezza del Servizio di Gestione documentale di Infocamere*
	Poiché potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di InfoCamere, ne consegue che l'infrastruttura IT potrebbe venire distrutta e ciò provocherebbe l'indisponibilità del servizio per un lunghissimo periodo.	Medio	Basso	Mitigazione tramite la verifica effettuata sull'inserimento del Sistema di gestione documentale nella soluzione di Disaster Recovery di InfoCamere
postazioni di lavoro	le postazioni di lavoro potrebbero essere infettate da malware; Data la sistemazione logistica di alcuni uffici aperti al pubblico durante le pause di lavoro le postazioni di lavoro potrebbero consentire l'interazione con il Sistema da parte di personale non autorizzato	Alto	Medio	Mitigazione tramite il perfezionamento delle misure individuate nella tabella *Contromisure e stato di attuazione*
dispositivi di firma	In caso venissero custoditi non correttamente i dispositivi di firma potrebbero essere sottratti indebitamente e	Medio	Basso	Mitigazione tramite il perfezionamento delle misure individuate nella tabella *Contromisure e stato di attuazione*

	utilizzati per la produzione di documenti apocrifi				

Il grado di attuazione del Piano di trattamento del rischio è soggetto a monitoraggio annuale al fine di aggiornare i contenuti del Piano stesso, con riferimento alle analisi del rischi e delle rispettive contromisure da programmare.

2.2 Formazione del personale

Uno degli interventi rilevanti per la gestione del rischio consiste nella formazione del personale, in particolare dei responsabili delle unità organizzative, che sono chiamati a loro volta a dare le opportune indicazioni ai propri collaboratori e a garantire che i comportamenti siano finalizzati alla corretta gestione dei documenti, segnalando tempestivamente le problematiche suscettibili di concretizzare situazioni di rischio. In particolare l'Ente prevede nel 2016 di effettuare una formazione nelle seguenti materie:

- misure per attuare la normativa sulla privacy;
- anticorruzione.

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.

2.3 Continuità operativa

La continuità operativa dell'Ente è trattata nel documento "Studio di fattibilità tecnica" [SFT ENTE] redatto secondo le linee guida di AGID [LG AGID DR].

3 MONITORAGGIO E CONTROLLI

3.1 Ripristino del Servizio

Il 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]. In relazione alle attività di monitoraggio e controlli in riferimento ai rapporti con i fornitori dei servizi in questione si specifica quanto segue

3.2 Fornitore InfoCamere

L'argomento viene descritto nel documento "Estratto delle Politiche e delle caratteristiche di sicurezza del Servizio di Gestione documentale Infocamere" allegato al presente Piano.

3.3 Altri fornitori

In relazione alla gestione documentale in capo a Digicamere l'Ente ha acquisito riguardo ai temi del monitoraggio e dei controlli il documento agli atti prot. CCIAA n. 10517 del 22.6.2016. Per quanto riguarda la gestione documentale riferita alla rilevazione presenze, verrà acquisita analoga documentazione dal fornitore Selesta Ingegneria spa.

4 POLITICHE DI SICUREZZA

4.1 Politica di gestione della sicurezza dei sistemi – fornitore InfoCamere

L'argomento viene descritto nel documento "Estratto delle Politiche e delle caratteristiche di sicurezza del Servizio di Gestione documentale Infocamere" allegato al presente Piano.

4.2 Politica di gestione della sicurezza dei sistemi – Altri fornitori

In relazione alla gestione documentale in capo a Digicamere l'Ente circa la politica di gestione della sicurezza dei sistemi ha acquisito il documento agli atti prot. CCIAA n. 10517 del 22.6.2016. Per quanto riguarda la gestione documentale riferita alla rilevazione presenze, verrà acquisita analoga documentazione dal fornitore Selesta Ingegneria spa.

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

Gli obiettivi generali del controllo degli accessi logici si applicano al Servizio di Gestione Documentale; in tale ambito si deve limitare l'accesso alle informazioni ed ai servizi di elaborazione delle informazioni ai cosiddetti "need to access" ovvero alle effettive e legittime necessità operative, obiettivo fondamentale della sicurezza delle informazioni nell'Ente.
Tutto il personale dell'Ente e le terze parti interessate devono essere informati sull' esistenza di obiettivi generali riguardanti 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 ncessità di sicurezza degli accessi, anche in relazione alle evoluzioni organizzative e tecnologiche.

4.3.1 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.
- le credenziali 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 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.
- Qualora sia necessario accedere "in emergenza" a specifici dati/sistemi, come ad esempio nel caso assenza prolungata o di impedimento degli incaricati che renda indispensabile e indifferibile intervenire per esclusive necessità operative, il responsabile dell'unità organizzativa informa il responsabile della gestione documentale, il quale provvede a chiedere al fornitore del servizio l'abilitazione temporanea dei collaboratori designati secondo i profili individuati.

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

4.3.2 Utilizzo delle password

Riguardo al Servizio di Gestione Documentale:

- L'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 lavorative 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.).

4.3.3 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.

Servizi informatici - richieste effettuate al fornitore

I processi organizzativi e la strumentazione tecnica utilizzata per la gestione delle richieste dell'Ente relative alle credenziali di accesso devono essere coerenti con la politica ed i processi dell'Ente.
La strumentazione tecnica utilizzata per la gestione delle password di accesso ai servizi forniti deve essere coerente con la politica dell'Ente, in quanto:

- i sistemi di gestione delle password devono essere interattivi e assicurare password di qualità.
- i sistemi di autenticazione devono imporre il rispetto della password policy.

Esecuzione degli accessi

Il Sistema di Gestione Documentale realizzato su infrastruttura IT dei fornitori e da questi gestita, deve essere dotata di:

- *procedure di log-on sicure*:
  l'accesso a sistemi e applicazioni deve essere controllato da procedure di log-on sicure;
- *controllo degli accessi alle applicazioni ed alle informazioni*:
  l'accesso alle informazioni ed alle funzionalità dei sistemi applicativi da parte degli utenti e del personale di supporto deve essere progettato e realizzato in base al principio di necessità;
- *password di accesso*:
  la strumentazione tecnica utilizzata dai fornitori per la gestione delle password di accesso ai servizi forniti deve essere coerente con la politica dell'Ente.

4.4 Politica di gestione delle postazioni di lavoro

Al fine di garantire un'adeguata sicurezza nella gestione delle postazioni di lavoro, devono essere rispettate le seguenti regole:

4.4.1 competenza dell'Ente

aggiornamenti 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 strumenti di aggiornamento automatico o centralizzato previsti dall'Ente.

limitazione della connettività a supporti esterni
L'utilizzo improprio di dispositivi rimovibili può aumentare il rischio di fuga di dati riservati aziendali, pertanto il personale:

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

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

4.4.2 competenze del fornitore InfoCamere

configurazione delle postazioni di lavoro
Il sistema di gestione documentale Gedoc, 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].

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.

4.4.3 competenze degli altri fornitori
Le tematiche del paragrafo precedente non sono applicabili agli altri fornitori in quanto non esistono particolari esigenze di configurazione delle postazioni di lavoro né soluzioni di postazioni virtuali.

4.5 Politica di gestione, dismissione e smaltimento degli apparati mobili e dei supporti
Per garantire che la gestione, dismissione e smaltimento degli apparati mobili e dei supporti garantiscano la sicurezza, devono essere rispettate le 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:

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

Riguardo alle postazioni di lavoro mobili:

- in genere le postazioni di lavoro mobili sono assegnate individualmente al personale, in alcuni casi possono essere intestate al responsabile dell'unità organizzativa ed utilizzate dal personale ad essa appartenente;
- 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 del Provveditore (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

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 della Gestione Documentale 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.

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.

4.6 Politica di protezione dal malware

Per assicurare che la protezione dal malware garantisca la sicurezza, devono essere rispettate le 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.

contromisure per la protezione dal malware

La strumentazione software per la protezione dal malware (c.d. antivirus) è installata su tutti 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.

Nei sistemi 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; 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.

4.7 Scrivania e schermo puliti

Per garantire che la gestione della scrivania e dello schermo avvenga nel rispetto della sicurezza, devono essere rispettate le seguenti direttive di "scrivania pulita", per i documenti ed i supporti di memorizzazione rimovibili, e di "schermo pulito", per i servizi di elaborazione delle informazioni.

Tali regole sono essenziali per proteggere tutti gli apparati di elaborazione delle informazioni sia in utilizzo individuale (postazioni di lavoro) sia condiviso (console di sistemi di controllo, server, cartelle di rete, etc.). Le regole devono essere rispettate dal personale dell'Ente, dai fornitori e dalle terze parti.

scrivania pulita

Essenziali per proteggere le informazioni su supporto cartaceo e su supporti rimovibili di memorizzazione, implicano che 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).