CAMERA DI COMMERCIO DEL VCO

Piano della Sicurezza dei documenti informatici

Versione	1.0	Data Versione:	maggio 2019
Descrizione modifiche			
Motivazioni			

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.

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.

1.2 Livello di riservatezza

	Livello	Ambito di diffusione consentito
	Pubblico	Il documento può essere diffuso **all'esterno** dell'Ente.
X	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 .

1.3 Precedenti emissioni

Prima emissione

Versione:	n. 1	Data Versione:	20/05/2019
Descr. modifiche:			
Motivazioni :			

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

1.5 Riferimenti documentali

CAD CO	Codice dell'Amministrazione Digitale, Decreto legislativo 7 marzo 2005, n. 82, art. 50 bis
DPS	Documento Programmatico della Sicurezza
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
MANUALE	Manuale di Gestione documentale della Camera di commercio del Verbano Cusio Ossola
MCF CLIENT	<xxxcodice servizio gedoc> MCF/CLIENT, Manuale di configurazione della postazione di lavoro client
TESTO UNICO	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa

1.6 Termini e definizioni

SGQ	Sistema di Gestione della Qualità

2. ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

2.1. PREMESSA

Il sistema di gestione documentale adottato dall'Ente, denominato GEDOC, è stato realizzato dalla società consortile Infocamere. Essendo l'infrastruttura basata su tecnologia web, la gestione in termine di servizi di connettività, hardware e applicazione software, rientra nelle modalità di gestione di tutti i servizi di Infocamere di cui l'ente usufruisce, pertanto gli aspetti di sicurezza e di continuità operativa correlati al Sistema di gestione documentale sono demandati alla società Infocamere.

2.2 Analisi del rischio IT

Individuazione degli asset

asset	descrizione
Personale coinvolto	Utenti del Sistema di gestione documentale
Servizio	Servizio di Gestione Documentale offerto agli utenti
Documenti	documenti gestiti dal Sistema
Dati personali	dati personali presenti nei documenti, registrazioni di protocollo, metadati
Metadati relativi alle registrazioni di protocollo ed ai documenti	Informazioni obbligatorie e facoltative di identificazione del documento informatico tramite adozione di regole, procedure e tecnologie idonee a garantirne le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.
Registro di protocollo	Registro di protocollo informatico creato dal sistema giornalmente
Credenziali di accesso	Identificativo di accesso, profilo di abilitazione associato, password
Processi di gestione documentale	processi e attività di gestione della protocollazione e dei flussi documentali: protocollazione (attribuzione di un numero progressivo), classificazione (attribuzione al documento della classifica prevista dal titolario di archivio), fascicolazione (inserimento del documento in un fascicolo informatico), inoltro (assegnazione del documento all'ufficio competente)
Copia per immagine su supporto informatico di documenti analogici	Inserimento nel sistema informatico di un documento analogico tramite scansione e attestazione di conformità all'originale cartaceo
Infrastruttura IT	infrastruttura tecnologica che ospita il Sistema
Postazioni di lavoro	personal computer / altri apparati mobili tramite i quali gli utenti accedono al sistema
Dispositivi di firma	dispositivi di firma digitale e autenticazione

Analisi delle minacce e vulnerabilità

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 questo accadimento provocherebbe una perdita di efficienza e di motivazione all'utilizzo.	M	M
	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; questo accadimento provocherebbe la consultazione di informazioni riservate / l'impossibilità di utilizzare le funzionalità necessarie.	B	A
Servizio/Sistema Registro di protocollo/Processi di gestione documentale	Poiché il Sistema informatico è di recente adozione, ne consegue che il servizio e le sue funzioni (come la generazione del registro di protocollo) potrebbero presentare inizialmente malfunzionamenti che possono provocare danneggiamenti, perdita di dati e inefficienze	M	A
	Nel tempo i processi di gestione documentale potrebbero discostarsi dalla prassi effettiva	B	M
Documenti	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 questo accadimento provocherebbe difficoltà nelle successive ricerche.	M	M
	Poiché un documento potrebbe essere accidentalmente / intenzionalmente cancellato o sostituito, ne consegue che il personale potrebbe essere coinvolto in un procedimento amministrativo o giudiziario; questo accadimento potrebbe provocare un danno all'immagine istituzionale dell'Ente.	mB	mA
Dati personali	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al personale potrebbero essere sovradimensionati rispetto alle esigenze lavorative; questo accadimento provocherebbe la consultazione di informazioni personali da parte di personale non incaricato.	B	A
Metadati relativi alle registrazioni di protocollo ed ai documenti	I metadati inseriti potrebbero essere incoerenti con le registrazioni di protocollo o i documenti archiviati	B	A
Credenziali di accesso	Le credenziali potrebbero diventare non allineate alle effettive necessità	B	M
Copia per immagine su supporto informatico di documenti analogici	Durante la fase di trasformazione del documento analogico in documento digitale è possibile alterare il risultato finale ottenendo una copia non conforme all'originale.	mB	M
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.	M	A

Asset	Minacce e vulnerabilità	P (probabilità)	I (impatto)
	Poiché potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di InfoCamere, ne consegue che l'infrastruttura IT potrebbe venire distrutta e questo accadimento provocherebbe l'indisponibilità del servizio per un lunghissimo periodo.	mB	mA
Postazioni di lavoro	Le postazioni di lavoro potrebbero essere infettate da malware	M	mA
	Durante le pause di lavoro le postazioni di lavoro potrebbero consentire l'interazione con il Sistema da parte di personale non autorizzato	M	A
	Le postazioni di lavoro potrebbero essere inadeguate rispetto alle caratteristiche richieste dal Sistema	mB	M
Dispositivi di firma	L'utente a cui viene assegnato il dispositivo di firma è l'unico responsabile del suo utilizzo. In caso di smarrimento o furto, è possibile un utilizzo improprio dei certificati di sottoscrizione o di autenticazione in esso contenuti.	B	mA

Individuazione delle contromisure
Per ogni asset vengono indicate le contromisure adottate.

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 individuali con il personale che ne manifesti la necessità per raccogliere le problematiche e individuare soluzioni condivise	80%
	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; questo accadimento provocherebbe la consultazione di informazioni riservate / l'impossibilità di utilizzare le funzionalità necessarie.	- Verifica periodica dell'adeguatezza dei profili	50%
documenti	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 questo accadimento provocherebbe difficoltà nelle successive ricerche.	- Piano di formazione adeguato - Incontri individuali con i responsabili ufficio per raccogliere le problematiche e individuare soluzioni condivise	50%
	Poiché un documento potrebbe essere accidentalmente / intenzionalmente cancellato o sostituito, ne consegue che il personale potrebbe essere coinvolto in un procedimento amministrativo o giudiziario; questo accadimento potrebbe provocare un danno all'immagine istituzionale dell'Ente.	- Verificare che la soluzione proposta soddisfi ai requisiti di tracciatura delle operazioni	100%
dati personali	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al personale potrebbero essere sovradimensionati rispetto alle esigenze lavorative; questo accadimento provocherebbe la consultazione di informazioni personali da parte di personale non incaricato.	- Verifica periodica dell'adeguatezza dei profili	0%

asset	minacce e vulnerabilità	contromisure	grado di copertura
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.	- Verificare il livello di disponibilità garantito da InfoCamere per il Sistema di gestione documentale (vedi paragrafo "Livelli di Servizio" del Piano della sicurezza)	100%
	Poiché potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di InfoCamere, ne consegue che l'infrastruttura IT potrebbe venire distrutta e questo accadimento provocherebbe l'indisponibilità del servizio per un lunghissimo periodo.	- Verificare se il Sistema di gestione documentale sia inserito nella soluzione di Disaster Recovery di InfoCamere (vedi paragrafo "Continuità operativa del Sistema" del Piano della sicurezza)	100%

Calcolo del Rischio (vedi note finali)

asset	minacce e vulnerabilità	Rischio intrinseco	Rishio residuo
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.	Medio	Medio
	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; questo accadimento provocherebbe la consultazione di informazioni riservate / l'impossibilità di utilizzare le funzionalità necessarie.	Medio	Medio
documenti	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 questo accadimento provocherebbe difficoltà nelle successive ricerche.	Medio	Basso
	Poiché un documento potrebbe essere accidentalmente / intenzionalmente cancellato o sostituito, ne consegue che il personale potrebbe essere coinvolto in un procedimento amministrativo o giudiziario; questo accadimento potrebbe provocare un danno all'immagine istituzionale dell'Ente.	Medio	Basso

asset	minacce e vulnerabilità	Rischio intrinseco	Rishio residuo
dati personali	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al personale potrebbero essere sovradimensionati rispetto alle esigenze lavorative; questo accadimento provocherebbe la consultazione di informazioni personali da parte di personale non incaricato.	Medio	Medio
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
	Poiché potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di InfoCamere, ne consegue che l'infrastruttura IT potrebbe venire distrutta e questo accadimento provocherebbe l'indisponibilità del servizio per un lunghissimo periodo.	Medio	Basso

Trattamento del rischio residuo (per il calcolo vedere note finali)

asset	minacce e vulnerabilità	rischio residuo	strategia di risposta	azione di trattamento
Personale coinvolto	Poiché il Sistema informatico è di recente adozione, ne consegue che il personale potrebbe incontrare difficoltà ...	Medio	Accettazione	Formazione mirata sulla base delle difficoltà manifestate
	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al personale potrebbero essere sovra / sottodimensionati ...	Medio	Mitigazione	Sei mesi dopo l'avvio verifica dell'adeguatezza dei profili (anche intervistanto il personale e i responsabili) Successivamente, verifica annuale.
Documenti	Poiché la classificazione e fascicolazione dei documenti è un'operazione complessa ...	Basso	Accettazione	Controllo da parte dei responsabili ufficio
	Poiché un documento potrebbe essere accidentalmente / intenzionalmente cancellato o sostituito ...	Basso	Accettazione	

asset	minacce e vulnerabilità	rischio residuo	strategia di risposta	azione di trattamento
Dati personali	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al personale potrebbero essere sovradimensionati ...	Medio	Rimozione	Dopo l'avvio verificare all'inizio dei sei mesi successivi l'adeguatezza dei profili (anche intervistando il personale e i Responsabili). Ripetere poi la verifica ogni anno.
Infrastruttura IT	Poiché l'infrastruttura IT potrebbe essere coinvolta da malfunzionamenti ...	Basso	Accettazione	Si individuano con Infocamere con soluzioni condivise
	Poiché potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di InfoCamere ...	Basso	Accettazione	

1.7 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.

1.8 Continuità operativa del sistema di gestione documentale

2.1.1 Continuità Operativa del Sistema

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.

3. MONITORAGGIO E CONTROLLI

1.9 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]

1.10 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.

RTO /Recovery Time Objective): indica quanto a lungo è possibile rimanere senza il servizio. Questo è associato con la massima interruzione ammissibile o tollerabile.

RPO (Recovery Point Objective): indica il periodo di tempo in cui la perdita di dati è ammissibile.

1.11 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 email) entro due ore all'interno dell'orario di servizio dal lunedì al venerdì.

1.12 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:

3.1.1 Procedure operative

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

3.1.2 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.

3.1.3 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.

4. POLITICHE DI SICUREZZA

1.13 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.

4.1.1 Inventario degli asset IT

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

Gli asset devono essere censiti, catalogati e valutati in relazione alla loro importanza per il business; devono essere quindi assegnati ad un responsabile. La valutazione deve essere effettuata in base al valore, alle normative cui sono assoggettati, ai requisiti di riservatezza, integrità e disponibilità, alla criticità per l'organizzazione.

4.1.2 Installazione dei sistemi

L'integrità dei sistemi di produzione è un requisito di sicurezza essenziale per InfoCamere; pertanto devono essere attuate procedure per controllare l'installazione del software sui sistemi di produzione.
Devono inoltre essere stabilite e attuate regole (limitazioni) per il governo dell'installazione del software da parte degli utenti.

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.

4.1.3 Resource Capacity Management

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

Il Processo è strutturato nelle seguenti fasi:

- 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.

4.1.4 Configurazione dei sistemi

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

4.1.5 Backup

Devono essere effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi; le copie devono essere sottoposte a test periodici di restore.

Il Processo che regola l'esecuzione del backup garantisce che la modalità di salvataggio sia selezionata in base ai parametri: tipologia del dato (dato di produzione / non produzione, dato strutturato / non strutturato), frequenza, ubicazione copie, periodo di retention, supporto fisico, ambiente tecnologico.
Le copie di backup dei dati di produzione sono replicate nel datacenter secondario (Disaster Recovery).

4.1.6 Amministratori di Sistema

Devono essere minimizzati i rischi di:

- 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.

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

La politica per il controllo degli accessi logici al Servizio di Gestione Documentale limita l'accesso alle informazioni ed ai servizi di elaborazione delle informazioni ai cosiddetti "need to access" ovvero alle effettive e legittime necessità operative, è considerato obiettivo fondamentale della Sicurezza delle Informazioni nell'Ente.

Tutto il personale dell'Ente e le terze parti interessate 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.

4.1.7 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 utente 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.

4.1.8 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 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.).

4.1.9 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.

4.1.10 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, è dotato di:

- procedure di log-on sicure
  L'accesso a sistemi e applicazioni è 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 è progettato e realizzato in base al principio di necessità
- password di accesso
  La strumentazione tecnica utilizzata da InfoCamere per la gestione delle password di accesso ai servizi forniti, è coerente con la politica.

1.15 Politica di gestione delle postazioni di lavoro

La politica (definita nel Piano Generale della Sicurezza delle Informazioni dell'Ente) si applica anche al caso specifico del Servizio di Gestione Documentale; pertanto devono essere rispettate le seguenti regole:

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 dispositivi 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 delle funzioni di sicurezza.

Configurazione delle postazioni di lavoro

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

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.

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

La politica (definita nel Piano Generale della Sicurezza delle Informazioni dell'Ente) si applica anche al caso specifico del Servizio di Gestione Documentale; pertanto 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 alla postazioni di lavoro mobili:
in genere le postazioni di lavoro mobili sono assegnate personalmente al personale, in alcuni casi possono essere intestate ad una P.O. 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 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

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.

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.

1.17 Politica di protezione dal malware e dallo spamming

La politica (definita nel Piano Generale della Sicurezza delle Informazioni dell'Ente) si applica anche al caso specifico del Servizio di Gestione Documentale; pertanto devono essere rispettate le seguenti regole:

- Le informazioni di proprietà dell'Ente o da essa gestite e le infrastrutture IT preposte alla loro elaborazione 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 tutte gli apparati con sistema operativo Windows, siano essi server dedicati ad erogare servizi che postazioni di lavoro dalle quali si accede ai servizi; l'antivirus è installato sia sui sistemi fisici (server, personal computer) che virtuali utilizzati dall'Ente.

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; 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.

1.18 Scrivania e schermo puliti

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

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).

NOTE FINALI

*Calcolo del **rischio "intrinseco"** che ogni minaccia o vulnerabilità comporta per l'asset; tale rischio esiste indipendentemente dalle contromisure applicate:*
rischio intrinseco = probabilità X impatto.
Nel caso di scala "mB / B / M / A / mA" utilizzare la seguente tabella che 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*

*Calcolare il **rischio "residuo"**: rischio che permane considerando l'efficacia delle contromisure in essere.*
Per il calcolo utilizzare una tabella simile alla seguente:

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

Predisporre il "Piano di trattamento dei rischi"; per ogni rischio:

1) *decidere quale strategia di risposta adottare:*
   - ***rimozione** (azione di eliminazione completa della minaccia o vulnerabilità; è una strategia di prevenzione sul problema potenziale)*
   - ***trasferimento** (azione che "ribalta" a terze parti, dietro pagamento, gli oneri e le responsabilità associate al rischio; es: contratto assicurativo)*
   - ***mitigazione** (azione di riduzione della probabilità o dell'impatto che riporta tali valori entro una soglia accettabile)*
   - ***accettazione** (si accetta che il rischio si presenti; in tal caso si intraprenderà un'azione a posteriori sul problema accaduto; l'azione può essere pianificata da subito oppure rimandata al momento nel quale accadrà l'evento)*
2) *identificare e descrivere l'azione di trattamento.*

Il Piano va ovviamente attuato ed il suo avanzamento deve essere verificato.
L'analisi del rischio va ripetuta con una certa periodicità.