CAMERA DI COMMERCIO
INDUSTRIA ARTIGIANATO E AGRICOLTURA
DI TORINO

Allegato A1) del Manuale del sistema di conservazione

Piano della sicurezza del sistema di conservazione e dei documenti informatici della Camera di commercio di Torino

Versione 1.0 – Dicembre 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.

Il documento costituisce un allegato al Manuale di Gestione Documentale [MANUALE] e al Manuale di Conservazione [MANUALE CONS] dell'Ente.

Esso riprende e approfondisce i contenuti del paragrafo "La sicurezza del sistema di gestione documentale" dei Manuali.

Riporta inoltre i criteri di Sicurezza di InfoCamere, cui è affidata la conservazione dei Documenti Informatici dell'Ente, secondo quanto previsto dalla normativa applicabile alla PA [SCN_IC].

1.2 Livello di riservatezza

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

Versione:	Prima emissione	Data Versione:	dicembre 2016
Descrizione modifiche:	Non applicabile		
Motivazioni:	Non applicabile		

1.4 Riferimenti normativi

Codifica	Descrizione
TESTO UNICO	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
CAD	D.Lgs. 82/2005 - Codice dell'amministrazione digitale
CODICE PRIVACY	Decreto Legislativo 196/03 e ss.mm.ii.
REGOLE TECNICHE	DPCM 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis, 23 -ter, comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del decreto legislativo n. 82 del 2005 e ss.mm.ii. Codice dell'amministrazione digitale (CAD)

1.5 Riferimenti documentali

Codifica	Descrizione
MANUALE	Manuale di Gestione documentale della Camera di commercio di Torino
MANUALE CONS	Manuale del Sistema di Conservazione della Camera di commercio di Torino
MCF CLIENT	MCF/CLIENT, Manuale di configurazione della postazione di lavoro client (documento InfoCamere utilizzato in fase di configurazione delle postazioni di lavoro Camerali) disponibile all'url: http://intranet.infocamere.it/web/gedoc/-/configurazione-client-per-gedoc?inheritRedirect=true
TESTO UNICO	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
SCN_IC	Sistema di Conservazione a Norma D.P.C.M. 3/12/2013 di InfoCamere. Rispondente ai "Requisiti di Qualità e Sicurezza" di AGID, presso cui InfoCamere è accreditata quale gestore. Il sistema è Descritto nel Manuale del Sistema di Conservazione di InfoCamere, redatto ai sensi dell'art. 8 del DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis, 23 -ter, comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (di seguito Regole Tecniche). Tale Manuale è pubblicato sul sito dell'AGID.
SGD_IC	Servizio di Gestione Documentale di InfoCamere, erogato alle CCIAA aderenti, in modalità SAAS (software as a service) e in conformità a quanto richiesto dal D.PC.M. 3 dicembre 2013 sul protocollo e dal D.P.C.M. 13 novembre 2014 sui documenti informatici.
ACCREDIA	Ente Italiano di Accreditamento – unico organismo nazionale autorizzato dallo Stato a svolgere attività di accreditamento, ossia l'unico ente riconosciuto in Italia ad attestare che gli organismi di certificazione e ispezione, i laboratori di prova, anche per la sicurezza alimentare, e quelli di taratura abbiano le competenze per valutare la conformità dei prodotti, dei processi e dei sistemi agli standard di riferimento.

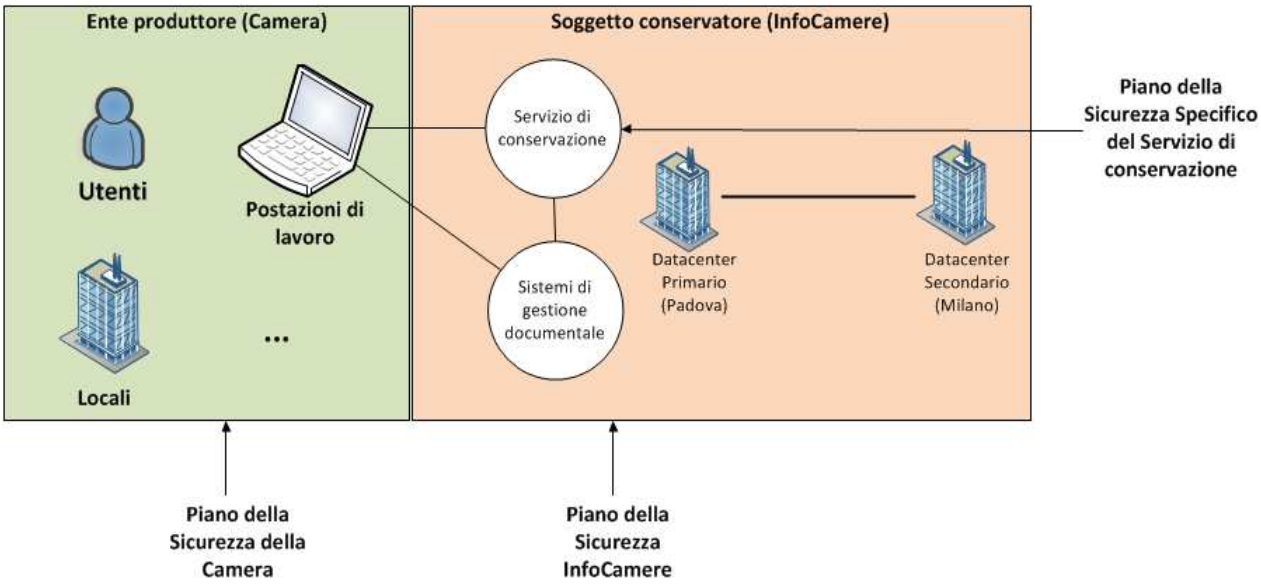
1.6 Termini e definizioni

Codifica	Descrizione
AOO	Area Organizzativa Omogenea ovvero l'Ente camerale
Servizio	Servizio di gestione documentale (Gedoc) e servizio per la conservazione dei documenti informatici.
GEDOC	Sistema per la gestione dei flussi documentali (SGD_IC), sviluppato e gestito da InfoCamere e utilizzato via internet/intranet dalle Camere di commercio, come servizio, in modalità SAAS – software as a service.
SCN_IC	Il Servizio InfoCamere per la conservazione dei documenti informatici della Camera di commercio.
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

Codifica	Descrizione
	del livello di servizio.
RTO	Tempo massimo di disallineamento dei dati che il servizio di Disaster Recovery garantisce in caso di disastro.
RPO	Tempo in cui la soluzione di Disaster Recovery garantisce il ripristino della disponibilità dei servizi in caso di disastro.

2. ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

La sicurezza complessiva del sistema di gestione e conservazione è garantita dall'insieme delle misure di sicurezza adottate dall'Ente produttore e dal Soggetto conservatore, per i propri ambiti di responsabilità, come sintetizzato dallo schema seguente:



2.1 Analisi del rischio IT

La sicurezza dei documenti elettronici formati, gestiti e conservati dall'Ente è assicurata da specifiche procedure organizzative, gestionali e operative che derivano in gran parte dalle politiche e procedure di sicurezza generali.

L'allegato 1 **"Analisi dei rischi"** descrive l'analisi sui rischi che insistono sugli asset dell'Ente e il Piano di trattamento del rischio residuo. In sintesi:

Gli **asset** individuati per l'analisi del rischio nell'ambito della Camere di commercio di Torino, tengono conto che:

- l'intera infrastruttura di rete dell'Ente è realizzata nell'ambito dell'infrastruttura InfoCamere (IC Rete) che, in gran parte, ne gestisce gli aspetti tecnologici;
- i sistemi per la gestione dei flussi documentali (SGD_IC) e di conservazione (SCD_IC) sono sviluppati e gestiti da InfoCamere e utilizzati via internet/intranet dalle Camere di commercio, come servizio, in modalità SAAS – software as a service;
- il processo di protocollazione dei flussi documentali in entrata è centralizzato su una specifica unità organizzativa.

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

- standard di settore, best practice di sicurezza e livello tecnologico delle infrastrutture IT dell'Ente;
- esperienza del personale e scelte organizzative interne;
- indicazioni provenienti da incidenti accaduti e audit interni;
- suggerimenti e condivisioni da parte di esperti del settore.

Per ogni minaccia o vulnerabilità e indipendentemente dalle contromisure applicate, è stato calcolato il **Rischio intrinseco attuale** come prodotto della probabilità (P) di accadimento per l'impatto (I) sull'Ente:

Rischio intrinseco attuale = P x I

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

Nell'allegato "Piano di trattamento", per ogni minaccia/vulnerabilità, è stata individuata l'azione ritenuta più idonea in termini di rimozione/mitigazione/accettazione del rischio.

2.2 Formazione del personale

Con riferimento al Piano di formazione del personale, relativamente ai servizi della Gestione Documentale, l'Ente garantisce che:

- le iniziative di formazione/aggiornamento siano finalizzate al mantenimento e sviluppo del patrimonio delle conoscenze dell'Ente in un'ottica di formazione continua in grado di recepire le esigenze formative e le evoluzioni normative, istituzionali e tecnologiche
- la formazione di ogni persona avvenga sulla base di una pianificazione che tenga conto del percorso formativo seguito, della figura professionale di appartenenza e quindi delle attività che la persona svolge o dovrà svolgere oltreché delle competenze e potenzialità espresse.

La formazione viene pianificata ed attuata, di concerto con il Responsabile della Gestione Documentale, secondo le attività:

- analisi dei bisogni formativi
- pianificazione
- diffusione delle informazioni sui corsi
- effettuazione degli interventi formativi
- valutazione degli interventi.

2.3 Continuità operativa

2.3.1 Continuità Operativa del Sistema

Poiché il Sistema di Gestione Documentale è ospitato su infrastruttura IT di InfoCamere, il Sistema di Gestione Documentale è inserito:

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

La soluzione di Disaster Recovery di InfoCamere garantisce un tempo massimo di disallineamento dei dati (RPO) di 24 ore ed il ripristino della disponibilità (RTO) dei servizi che InfoCamere eroga in outsourcing all'Ente entro 72 ore dal disastro.

In particolare sono gestiti nell'ambito della soluzione di Disaster Recovery di InfoCamere i seguenti Servizi:

- Sistema di Gestione Documentale
- Sistema di Conservazione

2.3.2 Continuità Operativa del Servizio

In caso di disastro ambientale, essendo le sedi camerali a breve distanza fra esse, e quindi soggetti a rischi analoghi, l'Ente valuterà l'opportunità di eventuali spostamenti del personale in altre sedi (non camerali), tenendo comunque in considerazione che le dotazioni di dispositivi mobili e l'architettura di rete possono offrire soluzioni tampone efficaci.

In caso di fermi prolungati di altra natura (quali danneggiamento o prolungata assenza di alimentazione elettrica), l'Ente valuterà l'opportunità di uno spostamento di personale tra le sedi camerali disponibili, sfruttando la flessibilità e ridondanza delle postazioni.

Se un evento disastroso (naturale o doloso) impattasse solo sulla sede di Palazzo Affari, sede del nodo provinciale della rete geografica InfoCamere, l'Ente potrà valutare di assicurare, anche se in misura contenuta e limitata alle attività prioritarie, la continuità del servizio di protocollazione attraverso soluzioni *mobile*, dato che i Servizi erogati sono accessibili in internet.

3. MONITORAGGIO E CONTROLLI

3.1 Ripristino del Servizio

Il Responsabile del Servizi di Gestione documentale, ovvero il soggetto che mantiene i sistemi di gestione e conservazione, cura che le funzionalità dei Sistemi, in caso di guasto o anomalia, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile [art. 61, comma 3 del TESTO UNICO].

3.2 Livelli di servizio

In coerenza con il paragrafo precedente, InfoCamere garantisce che i Servizi siano erogati 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

3.3 Comunicazione con il fornitore InfoCamere

InfoCamere rende disponibile uno specifico 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.

3.4 Monitoraggio dell'infrastruttura IT

I Sistemi di gestione e conservazione documentale sono ospitati su infrastruttura IT di InfoCamere la quale li mantiene sotto controllo tramite i processi e gli strumenti descritti nei punti seguenti.

3.4.1 *Procedure operative*

La Procedura di Operation & Event Management di InfoCamere:

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

3.4.2 *Strumenti*

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

- sonde di rilevazione
- registrazione degli eventi
- console
- segnalazioni generate automaticamente.

3.4.3 *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

4.1 Politica di gestione della sicurezza dei sistemi

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

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 strutture aziendali, previa una attenta valutazione delle caratteristiche soggettive, ovvero: è necessaria una valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Inoltre la designazione quale Amministratore di Sistema deve essere in ogni caso individuale e deve recare l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti, anche da parte del Garante della Privacy.

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

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

La politica per il controllo degli accessi logici definita nel documento sulle Misure minime di sicurezza e nelle lettere di incarico per il trattamento dati (Codice Privacy) si applica anche al caso specifico ai Servizi di gestione documentale e di conservazione; pertanto anche 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, 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.

4.2.1 Gestione delle credenziali di accesso

4.2.1.1 Assegnazione, riesame e revoca degli accessi degli utenti

Riguardo ai Servizi di Gestione e Conservazione 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.

4.2.1.2 Richieste effettuate al fornitore InfoCamere

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

4.2.3 Utilizzo delle password

Riguardo ai Servizi di Gestione e Conservazione 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.).

4.2.4 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 dei Servizi di gestione documentale e di conservazione è dell'utente fruitore del servizio.

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

4.2.5 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.

4.2.6 Esecuzione degli accessi

I Sistemi di Gestione e Conservazione documentale, realizzati su infrastruttura IT di InfoCamere e da questa gestiti, sono dotati di:

- Procedure di log-on sicure. L'accesso a sistemi e applicazioni è 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.

4.3 Politica di gestione delle postazioni di lavoro

La politica definita nel documento sulle Misure minime di sicurezza e nelle lettere di incarico per il trattamento dati (Codice Privacy) si applica anche al caso specifico dei Servizi di gestione e conservazione documentale; pertanto devono essere rispettate le regole descritte nei seguenti punti.

4.3.1 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.

4.3.2 Limitazione della connettività a supporti esterni

L'utilizzo improprio di dispositivi rimovibili può aumentare il rischio di fuga di dati riservati aziendali; pertanto il personale:

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

4.3.3 Modifica delle impostazioni

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

4.3.4 Configurazione delle postazioni di lavoro

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

4.3.5 Postazioni di lavoro virtuali

Quale elemento primario per la razionalizzazione delle risorse strumentali, progressiva riduzione delle spese di esercizio ed incremento delle caratteristiche di sicurezza, viene previsto l'utilizzo delle tecnologie di virtualizzazione del desktop.

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

La politica definita nel documento sulle Misure minime di sicurezza e nelle lettere di incarico per il trattamento dati (Codice Privacy) si applica anche al caso specifico dei Servizi di gestione e conservazione documentale; pertanto, devono essere rispettate le regole dei punti seguenti.

4.4.1 Gestione apparati e supporti informatici

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

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

Riguardo alla postazioni di lavoro mobili, in genere, sono assegnate personalmente al dipendente; in alcuni casi possono essere intestate ad una P.O. ed utilizzate dal personale ad essa afferente.

Tale personale è autorizzato a portare con sé al di fuori delle sedi dell'Ente gli apparati mobili assegnati e avendo ricevuto esplicite avvertenze sui comportamenti tesi a prevenire furti e/o danneggiamenti.

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).

4.4.2 Dismissione apparati e supporti informatici

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

4.4.3 Gestione supporti cartacei

In generale le informazioni presenti sui supporti cartacei (documenti, appunti) non dovrebbero mai essere lasciate dal personale in luoghi al di fuori del proprio controllo.

Nello specifico le informazioni rilevanti o riservate presenti sui supporti cartacei non devono mai essere lasciate dal personale al di fuori del proprio controllo.

Sulle scrivanie degli uffici, sui tavoli delle sale riunioni, o in altri luoghi, al termine del lavoro o al termine delle riunioni non deve essere lasciata documentazione riservata.

Sui dispositivi di stampa, fotocopia, acquisizione ottica delle immagini e nelle loro vicinanze non deve essere lasciata documentazione riservata.

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

4.4.4 Dismissione supporti cartacei

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

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

4.5 Politica di protezione dal malware

La politica definita nel documento sulle Misure minime di sicurezza e nelle lettere di incarico per il trattamento dati (Codice Privacy) si applica anche al caso specifico dei Servizi di gestione e conservazione 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.

4.5.1 Contromisure per la protezione dal malware

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

4.5.2 Contromisure per la protezione dallo spamming

I sistemi che gestiscono la posta elettronica utilizzano una strumentazione software per la protezione dallo spamming; le finalità della strumentazione sono:

- controllare le informazioni di provenienza dei messaggi
- a seconda della correttezza di tali informazioni, eliminare, inserire in quarantena o consegnare i messaggi al destinatario
- eliminare dai messaggi ricevuti eventuali programmi eseguibili in essi contenuti

- inviare ai destinatari l'elenco dei messaggi inseriti in quarantena.

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

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

4.6 Scrivania e schermo puliti

La politica definita nel documento sulle Misure minime di sicurezza e nelle lettere di incarico per il trattamento dati (Codice Privacy) si applica anche al caso specifico del Servizio di Gestione Documentale.

Pertanto 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.

Le regole di "scrivania pulita" sono essenziali per proteggere le informazioni su supporto cartaceo e su supporti rimovibili di memorizzazione:

- *scrivania pulita* 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 "screensaver" automatico protetto da password che pulisca la videata entro alcuni minuti (almeno 5) in caso di inutilizzo.

Sullo schermo della postazione, anche durante lo svolgimento della propria attività, non devono essere facilmente visibili o accessibili informazioni riservate ma 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).

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.

5. ALLEGATI

Analisi dei Rischi specifici del Sistema Documentale e della Conservazione