CAMERA DI COMMERCIO DI LUCCA

Piano della sicurezza informatica

Sommario

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 Responsabili del trattamento ai sensi 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.

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 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 alla rete camerale e, per quanto riguarda la posta elettronica, ai server della Camera di Lucca

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.

2.1 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 e unità nastri.
- sistemi per la gestione delle LAN (router, hub, switch, ecc.).

Tali apparecchiature sono collocate in aree ad accesso riservato.

Le apparecchiature delle LAN non facenti parte del backbone e che non possono essere situate nelle aree ad accesso controllato, sono riposte all'interno di armadi metallici chiusi.

2.2 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, chiavi 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.

2.3 Informazioni residue

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

3.4 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.

3.5 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.

3.6 Ripristino della password

Il ripristino della password, in caso di blocco della stessa, deve essere effettuato dagli amministratori di sistema 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.

3.7 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.

3.8 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, per il tramite dell'amministratore di sistema, 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.

3.9 Accesso degli amministratori

In adeguamento alle indicazioni del Garante contenute nel provvedimento del 27/11/2008 recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" si è proceduto, in data 15.12.2009, alla individuazione e nomina degli amministratori di sistema; con successivo provvedimento del 31.07.2015 si è provveduto ad aggiornarne i profili di autorizzazione; sono state adottate user-id nominali per l'autenticazione degli amministratori di sistema ed è stata implementata una procedura di registrazione degli accessi alla rete da parte degli stessi (access log) conforme alle prescrizioni contenute nel provvedimento citato.

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 Lucca 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 ICRete 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.

Si segnala che è in fase di avvio la sperimentazione della modalità di erogazione della prestazione lavorativa denominata "lavoro agile" (prevista dalla l. n.81/2017): un numero di dipendenti non superiore al 10% del totale potrà svolgere la propria attività lavorativa da remoto utilizzando una piattaforma di condivisione approntata da Infocamere ScpA tramite un servizio VPN (Virtual Private Network) che dovrebbe impedire ogni tentativo di accesso fraudolento alla rete camerale.

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. È altresì prevista la possibilità di attivare un collegamento ausiliario di backup nel caso in cui il collegamento principale sia per qualsiasi motivo indisponibile.

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 applicazioni e dati
2. Workstation

4.5 Server

I server di applicazioni e dati rappresentano nodi fondamentali e altamente strategici del Sistema Informativo Camerale. Ad essi pertanto è dedicata una particolare attenzione in tema di sicurezza. Sono collocati esclusivamente in locali ad accesso riservato.

L'accesso agli stessi per effettuare installazioni e configurazioni è possibile solo da parte di personale autorizzato. Fermo quanto previsto dal Provvedimento del 27.11.2008 del Garante, riguardante gli amministratori di sistema, le operazioni di installazione e configurazione dei sistemi 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. Per ragioni di sicurezza sono tracciati gli accessi (login/logout) alla rete camerale. Le unità dischi fisse sono ridondate in modo da consentire in maniera istantanea la contestuale scrittura delle informazioni su due diversi supporti fisici (RAID 1, Mirror, o RAID 5, stripe set con parità) e consentire in caso di rottura di uno di essi il ripristino trasparente per l'utente delle informazioni memorizzate.

I server sono collegati a unità atte ad immagazzinare i dati denominate librerie. La camera di commercio dispone di due librerie ridondate in alta affidabilità. Su di essi è effettuato un backup di sistema e dati attraverso apposite unità a nastro, di norma settimanale, salvo che per determinate tipologie di dati non sia stato previsto un timing minore (es giornaliero o infragiornaliero).

Sono collegati ad un gruppo di continuità che in caso di mancanza di alimentazione elettrica di rete procede all'arresto di tutte le funzioni degli stessi e allo spegnimento

4.6 Workstation

Le workstation, ossia le singole stazioni di lavoro degli utenti, devono avere le seguenti caratteristiche:

- gli utenti normalmente sono abilitati con un profilo USER salvo che per particolari esigenze o vincoli imposti dalle applicazioni installate non sia necessario attivare profili più potenti, quali Poweruser o Admnistrator.

- 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 Sistema informatico. L'Ufficio Sistema informatico 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 Sistema informatico 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 Sistema informatico 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. Tale attività deve essere svolta dall'Ufficio Sistema informatico in stretta concertazione con i sistemisti ed i responsabili della politica della sicurezza Infocamere.

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).

Tutte le applicazioni che comportano la gestione di informazioni e dati personali e i dati stessi devono essere installate ed archiviati su server posti in aree ad accesso riservato. Per ognuna di esse e per i relativi archivi devono essere individuati i profili utenti che a vario titolo e con diversi diritti possono interagire con la stessa. Qualora l'applicazione evidenzi malfunzionamenti od incongruenze nella gestione dei dati, gli incaricati del trattamento devono dare tempestiva comunicazione all'Ufficio CED, che provvederà a verificare gli stessi ed a porre in essere tutte le azioni correttive necessarie.

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 installato sui server che gestiscono la stessa. Inoltre, su tutte le stazioni gli utenti devono verificare che sia installato ed attivo il servizio di antivirus locale. 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 in server posti in locali ad accesso riservato. 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.

Qualora sia necessario archiviare i dati su singole workstation assegnate agli utenti, devono essere definite particolari misure di sicurezza logica analoghe a quelle adottate sui server, procedure di backup a cura dell'incaricato del trattamento e, sotto la responsabilità dello stesso, le apparecchiature devono essere collocate in uffici od aree chiuse se non presidiate.

4.10 Web filthering

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 un sistema di cd. "webfilthering" che si sostanzia in tali aspetti:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni – reputate inconferenti con l'attività lavorativa – quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

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 database contenenti dati personali, 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 in modo tale che la loro eventuale perdita, distruzione o alterazione non comporti alcun pregiudizio al rispetto delle politiche di sicurezza adottate.

Sui server è automaticamente implementata una politica di sicurezza con dischi ridondati (RAID 1, Mirror, o RAID 5, stripe set con parità) e di backup pianificato. 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 salvataggio delle banche dati avvengono con cadenza giornaliera; si è optato per un backup totale dei dati con quattro set di cassette. Ogni set ha la capienza di una settimana. I set vengono gestiti in rotazione in modo che sia a disposizione un salvataggio sino al mese precedente.

5.3 Ripristino

I backup effettuati tramite supporto a nastri sono soggetti, periodicamente ed a campione, ad una procedura di ripristino che verifichi la bontà del backup effettuato e l'effettiva accessibilità ai dati archiviati.