COMUNE DI PONSACCO

Provincia di Pisa

Piano di Sicurezza Informatica

Allegato D del Manuale di Gestione Documentale

Sommario

Premessa

Il presente allegato, riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali, ai sensi dell'art. 4, comma 1, lettera c) e dell'art. 7 del DPCM 03 dicembre 2013, "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".

Obiettivi

Il piano di sicurezza garantisce che:

a) i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
b) 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.

1. Formazione dei documenti informatici

1.1 Contenuti

Per agevolare il processo di formazione dei documenti informatici e consentire la trattazione automatica dei dati in essi contenuti, l'Amministrazione rende disponibili per via telematica, in modo centralizzato e sicuro, moduli e formulari elettronici validi ad ogni effetto di legge.
Al fine di tutelare la riservatezza dei dati personali, il Responsabile del procedimento Amministrativo si assicura che i certificati e i documenti trasmessi all'esterno contengano solo i dati utilizzati ai fini del procedimento amministrativo e nei termini previsti dalla legge.

1.2 Formati

Per l'invio/ricezione di documenti in modalità telematica sono ammessi i seguenti formati di file:
PDF/A, XML, ODF, JPG, TXT, SHAPEFILE,DWF.

1.3 Riferimenti temporali opponibili ai terzi

Al fine di conferire al documento informatico firmato digitalmente il riferimento temporale opponibile ai terzi, ci si avvale del servizio di protocollo informatico, ovvero del servizio di conservazione sostitutiva, ovvero dell'utilizzo di posta elettronica certificata, ai sensi dell'art. 41, del D.P.C.M. 22 febbraio 2013.

2. Gestione dei documenti informatici

2.1. Registrazione

Tutti i documenti informatici ricevuti o prodotti dall'Amministrazione sono soggetti a registrazione obbligatoria, ai sensi dell'art. 24 del Manuale di gestione, ad esclusione di quelli espressamente esclusi, ai sensi dell'art. 25 del Manuale di gestione, ovvero soggetti a registrazione particolare, ai sensi dell'art.26 del Manuale di gestione.

2.2. Sistema di gestione informatica del protocollo e dei documenti

Il sistema operativo dell'elaboratore, su cui è realizzato il sistema di gestione informatica del protocollo e degli atti amministrativi, quali Determinazioni, Deliberazioni e Ordinanze, è conforme alle specifiche previste dalla normativa vigente. Esso assicura:

a) l'univoca identificazione ed autenticazione degli utenti;
b) il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
c) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
d) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
e) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette da modifiche non autorizzate;
f) il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate.

Per i documenti informatici generati con strumenti diversi dall'attuale sistema di gestione documentale (Sicr@Web) gli utenti si devono accertarsi di salvare gli stessi in apposite aree del File Server (Cluster) messe a disposizione e dedicate esclusivamente al proprio Settore. Nei casi in cui tali documenti richiedono un livello di riservatezza maggiore è necessario presentare formale richiesta al Responsabile del Sistema Informatico il quale provvederà a creare un'apposita area ad accesso limitato.

2.3. Registro informatico di protocollo

Il sistema di protocollo informatico adottato dal Comune di Ponsacco è Sicr@web di Maggioli S.p.A.. La manualistica di descrizione e funzionamento del sistema è resa disponibile telematicamente all'indirizzo: http://sicrawebhelp.saga.it/index.php/Settore_Affari_Generali

Il sistema consente di generare i seguenti tipi di registri:
- Registro di protocollo
- Registro giornaliero di protocollo

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico giornaliero di protocollo è trasmesso entro la giornata successiva al sistema di conservazione, ai sensi dell'art. 7, comma 5, D.P.C.M. del 3 dicembre 2013.

2.4. Sicurezza fisica e sicurezza logica dei documenti

La prima area di sicurezza è la "sicurezza fisica". Con questo si intende la sicurezza delle apparecchiature hardware. Tutti i dispositivi classificati "di sistema" (server, apparati attivi di rete, firewall.) sono coperti da un servizio di manutenzione che garantisce tempi di intervento adeguati per il ripristino degli apparati.
La seconda area di sicurezza è la "Sicurezza Logica". Per sistema di sicurezza logica si intende il sottosistema di sicurezza finalizzato alla implementazione dei requisiti di sicurezza all'interno dell'architettura informatica. Per quanto riguarda il sistema informatico dell'Amministrazione, questo fine è perseguito mediante l'attivazione di:
a) Meccanismi per il controllo degli accessi. Il controllo degli accessi consiste nel garantire che tutti gli accessi agli oggetti del sistema informatico documentale gestito con Sicr@web avvengano secondo le modalità prestabilite (login, password). Di tutti gli accessi effettuati si tiene traccia in un file di registrazione degli accessi (file di log).
b) Funzioni per la realizzazione dell'integrità logica. Ogni utente, superata la fase di autenticazione, ha accesso solo ai dati residenti nella propria area di lavoro (scrivania virtuale) e non può accedere ad altre aree di lavoro.

c) Il sistema antivirus, che risiede sia sul server centrale che sulle stazioni di lavoro utente, controlla tutti i files in entrata ed in uscita da ciascuna macchina. Il sistema antivirus viene aggiornato tramite collegamenti automatici al server dedicato in modo trasparente all'utente.
d) *Funzioni per la realizzazione dell'integrità fisica*. L'integrità fisica dei dati viene garantita sia da un'adeguata configurazione hardware sia dal sistema di backup. Tutti i dati del sistema documentale sono memorizzati su un server virtuale centralizzato i cui dischi sono in configurazione RAID.
I backup sono schedulati e vengono effettuati con cadenza giornaliera nelle ore serali/notturne. Ogni giorno sono effettuati tre tipologie di backup, quali:

- Copia totale del server virtuale su un server adibito a storage NFS
- Copia incrementale con apposita procedura del server virtuale su un dispositivo storage NFS ubicato in altra stanza dell'edificio comunale
- Copia incrementale con soluzione Barracuda Backup (distinta e diversa dalla precedente) su un apposito server ubicato nel medesimo locale dove si trova il sistema di storage che ospita la macchina virtuale. Tale backup viene replicato su un ulteriore dispositivo Barracuda Backup che è ospitato in altra stanza dell'edificio comunale

Quotidianamente il personale preposto allo scopo controlla l'avvenuto salvataggio.
Con cadenza settimanale una copia completa del server virtuale viene riversata su nastro.

Per ogni operazione di backup effettuata sul sistema che ospita la base documentale e sul sistema di protocollo informatico è generato un file di log quotidianamente inviato via mail al responsabile del Servizio Sistema Informatico.

3. Accesso ai documenti informatici

3.1 Gestione della riservatezza

A ogni documento, all'atto della registrazione nel sistema di protocollo informatico, è possibile associare una Access Control List (ACL) che consente di stabilire quali utenti o gruppi di utenti hanno accesso ad esso.
Per default il sistema segue la logica dell'organizzazione, ciascun utente può accedere solamente ai documenti che sono stati assegnati alla sua struttura di appartenenza, o agli uffici ad esso subordinati.
L'amministrazione adotta regole per l'accesso ai documenti sulla base della normativa vigente in materia di privacy.

3.2. Accesso al sistema di gestione informatica

Il livello di autorizzazione all'utilizzo del sistema di gestione informatica dei documenti è attribuito secondo quanto disposto dagli art. 62 e 63 del Manuale di gestione.

4. Trasmissione e interscambio dei documenti informatici

4.1. Riservatezza

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.
Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

4.2. Sistema di posta elettronica

L'Amministrazione si avvale di un servizio di "posta elettronica certificata" offerto da un soggetto accreditato, in grado di assicurare la riservatezza e la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti, facendo ricorso al "time stamping" e al rilascio di ricevute di ritorno elettroniche.

4.3 Interoperabilità e cooperazione applicativa

Lo scambio di documenti informatici soggetti a registrazione di protocollo avviene mediante messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-8221, RFC 2045-20492 e successive modificazioni o integrazioni.
I dati della segnatura informatica di protocollo di un documento informatico trasmesso ad un'altra Pubblica Amministrazione sono inseriti in un file conforme allo standard XML.
Le modalità di composizione dei messaggi protocollati, di scambio degli stessi e di notifica degli eventi sono conformi alle specifiche riportate nella circolare AgID n. 60 del 23.01.2013.
L'operazione di ricezione dei documenti informatici comprende i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi.
I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica. L'operazione di spedizione include la verifica della validità amministrativa della firma.

5. Conservazione dei documenti informatici

La struttura e la gestione del sistema di conservazione, la definizione dei ruoli e delle interazioni con i soggetti esterni con i quali interagisce è definita nel Manuale della Conservazione.