

ALLEGATO D

Piano per la sicurezza dei documenti informatici

I - Formazione dei documenti informatici

1 - Contenuti

In ogni documento informatico deve essere obbligatoriamente riportata, in modo facilmente leggibile, l'indicazione del soggetto che lo produce e gli altri elementi relativi alla formazione del documento.

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.

2 - Formati

Per la predisposizione dei documenti informatici si adottano formati che al minimo possiedono requisiti di leggibilità, interscambiabilità, non alterabilità durante le fasi di accesso e conservazione, immutabilità nel tempo del contenuto e della struttura. In via preferenziale si adottano i formati XML, PDF/A, HTML, TIFF, ecc.

3 - Sottoscrizione

La sottoscrizione dei documenti informatici è eseguita con una firma digitale, basata su un certificato rilasciato da un certificatore accreditato e generata con un dispositivo sicuro.

Per i documenti informatici che non necessitano di sottoscrizione, l'identificazione dei soggetti che li producono è assicurata dalla sistema informatico di gestione dei documenti oppure dal sistema di posta elettronica certificata.

4 - Datazione

Per attribuire una data certa al documento informatico ci si avvale del servizio di marcatura temporale (time stamping) fornito dal certificatore accreditato.

II - Gestione dei documenti informatici

5 - Registrazione

Tutti i documenti informatici ricevuti o prodotti dall'amministrazione sono soggetti a registrazione obbligatoria ad esclusione di quelli soggetti a registrazione particolare da parte dell'ente il cui elenco è allegato al manuale di gestione (Allegato B) ai sensi dell'art. 53, comma 5 DPR 445/2000.

6 - 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 dei documenti, è conforme alle specifiche previste dalla normativa vigente. Esso assicura:

- a. l'univoca identificazione ed autenticazione degli utenti;
- b. la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- c. la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- d. 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.

Il sistema inoltre:

- 1) consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- 2) assicura 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 la generazione delle impronte dei documenti informatici il sistema utilizza la funzione di HASH.

7 - Registro informatico di protocollo

Conformemente a quanto stabilito nel manuale di Gestione, al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, al termine della giornata lavorativa, è inviato in conservazione sostitutiva al Polo Archivistico Regionale dell'Emilia Romagna, che ne è responsabile della conservazione.

8 - Modifica o annullamento delle registrazioni di protocollo

L'operazione di modifica o di annullamento di una registrazione di protocollo è eseguita con le modalità di cui all'art. 4.7 del manuale e come di seguito specificato:

- a. La necessità di modifica di una delle informazioni generate, o assegnate, automaticamente dal sistema e registrate in forma non modificabile (numero di protocollo, data della registrazione), determina l'annullamento dell'intera registrazione;
- b. La necessità di modifica delle informazioni registrate in forma non modificabile (mittente, destinatario, oggetto) al fine di correggere errori intercorsi in sede di immissione di dati, comporta l'annullamento dell'intera registrazione di protocollo
- c. Solo al responsabile del servizio protocollo competono le funzioni di autorizzazione all'annullamento del protocollo.

9 - Registro di emergenza

In condizioni di emergenza si applicano le modalità di registrazione e di recupero dei dati descritte all'articolo 63 del DPR 445/2000 e secondo quanto previsto nel manuale di gestione del protocollo informatico.

- a. sul registro di emergenza sono riportate la causa, la data e l'ora d'inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema;
- b. per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate;
- c. la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'ente;
- d. le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico utilizzando un'apposita funzione di recupero dei dati, senza ritardo rispetto al ripristino delle funzionalità del sistema; durante la fase di recupero, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero in emergenza, pertanto i documenti registrati in emergenza avranno due numeri: uno quello di emergenza e l'altro quello del protocollo generale.

10 - Sicurezza fisica dei documenti

L'accesso in lettura e scrittura alle directory di rete utilizzate come deposito dei documenti è gestito in modo trasparente dal software applicativo del protocollo informatico. Le directory di rete non sono direttamente visibili alle postazioni client.

III - Accessibilità ai documenti informatici

11 - Gestione della riservatezza

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, è associata 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, nel senso che 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.

12 - Accesso da parte degli utenti interni all'amministrazione

- a. Il livello di autorizzazione all'utilizzo del sistema di gestione informatica dei documenti è attribuito dal Responsabile del Servizio Archivistico;
- b. il controllo degli accessi ai dati di protocollo e alla base documentale da parte del personale dell'amministrazione è assicurato utilizzando UserID e la Password assegnata ad ogni utente;

IV - Trasmissione e interscambio dei documenti informatici

13 - Sistema di posta elettronica

La trasmissione dei documenti informatici avviene attraverso un servizio di posta elettronica certificata conforme agli standard della rete nazionale delle pubbliche amministrazioni.

L'Amministrazione si avvale di un servizio di posta elettronica certificata offerto da un soggetto abilitato ad erogare tale servizio, secondo le regole tecniche imposte dalla normativa vigente.

14 - 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 821-822, RFC 2045-2049 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 AIPA 28/2001.

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.

15 - Cifratura dei messaggi

a. Lo scambio di dati e documenti attraverso reti non sicure avviene con l'utilizzo dei sistemi di autenticazione e cifratura.

b. Lo scambio di dati e documenti attraverso reti sicure, come la Rete nazionale delle pubbliche amministrazioni o le reti interne, può avvenire anche senza adottare le misure di sicurezza di cui al precedente comma in quanto esse non sono ritenute necessarie.

V - Conservazione dei documenti informatici

16 - Procedure di conservazione

La conservazione dei documenti digitali e dei documenti analogici (che comprendono quelli su supporto cartaceo) avviene nei modi e con le tecniche specificate nel piano di conservazione (Allegato *Piano per la sicurezza dei documenti informatici*) e nelle deliberazioni CNIPA 11/04.

Il riferimento temporale, inteso come l'informazione, contenente la data e l'ora in cui viene ultimato il processo di conservazione digitale, associata ad uno o più documenti digitali, è generato secondo i canoni di sicurezza.

I documenti digitali, organizzati in fascicoli digitali, una volta inseriti nel sistema di gestione documentale dell'Ente, vengono giornalmente inviati al Polo Archivistico Regionale dell'Emilia-Romagna, che si occupa quindi della conservazione di tali documenti a norma di legge