PIANO PER LA SICUREZZA DEI DOCUMENTI INFORMATICI
Documento n. 8 – Allegato al manuale di gestione

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 di cui all'art. 7 del manuale di gestione.
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, i certificati e i documenti trasmessi all'esterno contengono solo i dati utilizzati ai fini del procedimento amministrativo e nei termini previsti dalla 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, come specificato anche nell'art. 8 del manuale di gestione.
Si adottano quindi i formati XML, PDF-A, TXT.

3 Sottoscrizione

La sottoscrizione dei documenti informatici è eseguita con una firma elettronica/digitale, basata su un certificato rilasciato da un certificatore accreditato e generata con un dispositivo sicuro, come specificato anche nell'art. 9 del manuale di gestione.
Per i documenti informatici che non necessitano di sottoscrizione, l'identificazione dei soggetti che li producono è assicurata della 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 (Documento n. 4) ai sensi dell'art. 53, co. 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

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, al termine della giornata lavorativa, è riversato su supporti riscrivibili e conservato a cura del Responsabile dell'Archivio; trimestralmente è riversato su supporti non riscrivibili; alla chiusura delle registrazioni il contenuto annuale del registro informatico di protocollo è riversato, in triplice copia, su un supporto informatico non riscrivibile e conservato secondo le modalità previste dal manuale di gestione del protocollo informatico, art. 26.

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'articolo 8 del DPCM 31/10/2000 e all'art. 23 del manuale di gestione, come di seguito specificato:

a) il tentativo 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'automatico e contestuale annullamento dell'intera registrazione;
b) Le informazioni registrate in forma non modificabile (mittente, destinatario, oggetto) possono essere annullate per correggere errori intercorsi in sede di immissione di dati. In questo caso l'annullamento deve comportare la rinnovazione del campo stesso con i dati corretti e la contestuale memoriz-

zazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica.

c) Solo al responsabile del servizio archivistico competono le funzioni di annullamento dei protocollo, come previsto dal manuale di gestione.

9 Registro di emergenza

In condizioni di emergenza si applicano le modalità di registrazione e di recupero dei dati descritte all'art. 63 del DPR 445/2000 e a quanto previsto nel manuale di gestione del protocollo informatico e dalla Guida per l'attivazione del registro di emergenza allegata al manuale di gestione (Documento n. 19).

1. 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;
2. per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate;
3. 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;
4. 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 risorse destinate alla memorizzazione dei documenti è effettuato dal processo server dell'applicativo di protocollo informatico, mai dalle stazioni di lavoro.
Il responsabile del Servizio informatico garantisce la puntuale esecuzione delle operazioni di salvataggio dei dati e dei documenti registrati, su supporti informatici non riscrivibili, da parte di personale appositamente autorizzato, come previsto dal manuale di gestione artt. 25 e 26 e dal piano di conservazione (Documento n. 5).
Le copie di sicurezza annuali dei dati e dei documenti prodotte in almeno tre copie sono conservate a cura del Responsabile del servizi informativi, dal Responsabile dell'archivio e in un luogo diverso dalla sede dell'amministrazione a cura di un soggetto terzo con il quale si è stabilita la convenzione per la conservazione, come previsto dal manuale di gestione art. 25 e 26.

III Accessibilità ai documenti informatici

11 Gestione della riservatezza

1 A ogni documento, all'atto della registrazione nel sistema di protocollo informatico, è associata un livello di sicurezza che consente di stabilire quali utenti o gruppi di utenti hanno accesso ad esso. Di norma 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;
2 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 dell'archivio;
b il controllo degli accessi ai dati di protocollo e alla base documentale da parte del personale dell'amministrazione è assicurato utilizzando apposite credenziali assegnata ad ogni utente;
c Il servizio informatico prevede, come previsto dal Documento programmatico sulla sicurezza, la possibilità di modificare periodicamente le parole chiave assegnate agli utenti per l'accesso alle funzioni del sistema di protocollo informatico.

13 Accesso da parte di altre pubbliche amministrazioni

L'accesso al sistema da parte di altre pubbliche amministrazioni avviene secondo gli standard ed i modelli architetturali di SPC ed RTRT ed in conformità all'art. 52 del manuale di gestione.

14 Accesso da parte di utenti esterni

L'accesso per via telematica al sistema di protocollo informatico da parte di utenti esterni all'amministrazione è consentito solo con strumenti tecnologici che permettono di identificare in modo certo il soggetto richiedente, e comunque limitamente ai procedimenti da questo attivati, conformemente all'art. 51 del manuale di gestione;

IV Trasmissione e interscambio dei documenti informatici

15 Sistema di posta elettronica

La trasmissione dei documenti informatici avviene attraverso un servizio di posta elettronica certificata conforme agli standard previsti dalla normativa. L'Amministrazione si avvale quindi di un servizio di "posta elettronica certificata" offerto da un soggetto 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: .

16 Interoperabilità e cooperazione applicativa

Lo scambio di documenti informatici soggetti a registrazione di protocollo tramite soluzioni di interoperabilità in ambito SPC-CA ed RTRT avviene conformemente alle specifiche tecniche previste dalla suddette reti.
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 relative specifiche tecniche adottate a livello nazionale e regionale.
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.

17 Cifratura dei messaggi

a Per lo scambio di dati e documenti attraverso reti è raccomandato l'utilizzo dei sistemi di autenticazione e cifratura.

b Lo scambio di dati e documenti attraverso reti sicure, come SPC ed RTRT 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

18 Supporti di memorizzazione

Per l'archiviazione sostitutiva dei documenti si utilizzano supporti di memorizzazione digitale non riscrivibili (es. WORM, CD-R, DVD-R, ecc.).

19 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 (Documento n. 5) e nella 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.

20 Tenuta dell'archivio informatico

Il Responsabile dell'Archivio sulla base di quanto specificato nel manuale di gestione e nel piano di conservazione:

a) adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza;

b) definisce i contenuti dei supporti di memorizzazione e delle copie di sicurezza;

c) verifica periodicamente con cadenza non superiore ai cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

Per la protezione dal rischio di intrusione e quanto non espressamente previsto dal presente Piano si rimanda al Documento programmatico sulla sicurezza.