DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

anci

Finanziato
dall'Unione europea
NextGenerationEU

PIANO DELLA SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

Il sistema Anci a supporto della digitalizzazione dei Comuni

La presente linea guida è stata curata dallo staff del progetto

“Il sistema ANCI a supporto della digitalizzazione dei Comuni”

Redattrici: **Maria Catanese e Rosamaria Santacaterina,**
con la collaborazione di Francescomaria Loriga e Maurizio Piazza

Supervisione del progetto: **Antonella Galdi,** Responsabile Area Innovazione tecnologica, Cultura, Politiche Giovanili, Mobilità sostenibile, TPL, Transizione energetica ANCI

Si ringraziano gli esperti del Transformation Office del DTD per la consulenza tecnica

Sommario

Premessa

Le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (2021) prevedono che il *responsabile della gestione documentale* ovvero, ove nominato, il coordinatore della gestione documentale, *in accordo con il responsabile della conservazione, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali*, predisponga misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio anche in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR)

Il Piano conterrà altresì la descrizione della proceduta da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 679/2016.

Nel caso in cui il Comune adotti atti di regolamentazione e indirizzo di carattere generale (ad es. *il piano generale della sicurezza, o il Regolamento IT, o altri atti adottati in conformità alle Misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017), contenenti la descrizione delle misure di sicurezza riferibili al sistema di gestione informatica dei documenti, il manuale di gestione può rimandare a questi documenti.*

La redazione del Piano e la sua diffusione possono considerarsi misure di sicurezza, in quanto strumenti di consolidamento della consapevolezza sulle criticità e sui corretti comportamenti da tenere.

Pertanto, affinché le indicazioni contenute nel Piano sicurezza siano efficaci, è importante che siano definite partendo dallo specifico contesto organizzativo del Comune e siano caratterizzate da concretezza, semplicità e chiarezza.

Esempio di struttura/contenuti di un Piano della Sicurezza, da redigere nel caso in cui l'Ente non abbia già adottato un Regolamento IT o altri documenti di indirizzo in materia di digitalizzazione.

1. Obiettivi

Il Piano per la Sicurezza è finalizzato a garantire che:

- i documenti e le informazioni trattate dall'Area Organizzativa Omogenea siano *disponibili, integri e riservati;*
- i dati personali siano custoditi in modo tale 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.

[gli obiettivi generali possono essere integrati da obiettivi specifici del Comune]

2. Descrizione sintetica del contesto

[devono essere descritte le caratteristiche tecniche del sistema di gestione documentale e le attribuzioni delle responsabilità in merito agli aspetti relativi alla sicurezza. Si tratta di un sistema "on premise" o erogato in modalità "in cloud – SaaS"? Chi è responsabile del Database? Chi è responsabile della componente infrastrutturale? Chi impartisce le direttive sulla sicurezza? Come vengono gestiti i log di accesso?

Chi ha accesso al server del protocollo informatico? È prevista la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso? Queste registrazioni sono protette al fine di non consentire modifiche non autorizzate?

Il Sistema di gestione documentale

- *garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo?*
- *assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita?*
- *fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale e della formazione del relativo fascicolo?*
- *consente il reperimento delle informazioni riguardanti i documenti registrati?*
- *consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di protezione dei dati personali?*
- *garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato]?*

3. Formazione dei documenti amministrativi informatici aspetti attinenti alla sicurezza

[Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono l'identificabilità del soggetto che ha formato il documento, la sottoscrizione dei documenti, quando prescritta, con una delle tipologie di firma elettronica adottate nell'AOO. Possono essere fornite le sintetiche indicazioni operative su come sono garantiti questi requisiti, anche facendo riferimento ad eventuali parti del manuale di gestione che già trattano il tema]

4. Componente organizzativa della sicurezza

[i ruoli sono definiti nell'ambio del Manuale di Gestione, cui si può rinviare. Può essere esplicitata l'eventuale presenza nel Comune di un Responsabile per la Sicurezza e le modalità di interazione con le altre figure che caratterizzano la Gestione Documentale]

5. Componente fisica e infrastrutturale della sicurezza

[da prevedere nel caso in cui il Sistema di Gestione Documentale sia gestito con applicativi on premise installati in datacenter nella disponibilità giuridica del Comune, devono essere descritte le misure adottate a presidio della sicurezza dei luoghi e delle infrastrutture che consentono l'erogazione dei servizi informatici. Nel caso in cui la gestione documentale è gestita tramite servizi CLOUD, la componente fisica e infrastrutturale in linea di principio nella sfera di responsabilità del fornitore del servizio; il Piano può fare riferimento alle clausole contrattuali che disciplinano questo aspetto]

6. Componente logica della sicurezza

[Come vengono garantiti i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi? Come viene gestita l'identificazione, l'autenticazione e l'autorizzazione degli addetti dell'AOO e degli operatori dell'erogatore del Servizio per la tenuta del protocollo informatico? Con quali strumenti avviene la registrazione delle attività (Accounting)?]

7. Postazioni di lavoro

8. Formazione e gestione dei documenti

1. Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:
   - l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;
   - la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
   - l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
   - l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
   - la leggibilità dei documenti nel tempo;
   - l'interscambiabilità dei documenti all'interno della stessa AOO [eventuale] *e con AOO diverse*.
2. I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o text editor che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Per il formato finale del documento si adottano preferibilmente i formati PDF, XML e TIFF, in accordo con le regole tecniche individuate dal CAD (Codice dell'Amministrazione Digitale) D.lgs 82/2005.
3. I documenti informatici prodotti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nel formato standard PDF/A come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.
4. Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.
5. Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).
6. L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza.
7. Il sistema di gestione informatica dei documenti:
   - garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
   - garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
   - fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
   - consente il reperimento delle informazioni riguardanti i documenti registrati;
   - consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
   - garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

9. Trasmissione e interscambio dei documenti amministrativi informatici (esempio di indicazioni)

1. 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 consentito il trattamento e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.
2. Il sistema di protocollo informatico si interfaccia con il sistema di posta certificata del fornitore esterno (provider) di cui si avvale l'amministrazione, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:
   - accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;
   - tracciamento delle attività nel file di log della posta;
   - gestione automatica delle ricevute di ritorno.
3. Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e articolo 15 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale del 21 novembre 2000, n. 272).
4. Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.
5. Ai sensi del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000, il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi.
6. La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dal decreto del 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata". Inoltre, nella circolare n. 60 del 23 gennaio 2013, emanata dall'Agenzia per l'Italia digitale, vengono definiti il formato e la tipologia di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni.

10. Condotte per la protezione dei documenti amministrativi informatici

Corretto uso delle credenziali di autenticazione

[descrizione di indicazioni pratico/operative e delle condotte da tenere per la protezione dei documenti amministrativi informatici]

Il sistema Anci a supporto della digitalizzazione dei Comuni

Via dei Prefetti, 46 - 00186 Roma
trasformazionedigitale@anci.it

www.sistemacomunidigitali.anci.it

DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

anci

Finanziato
dall'Unione europea
NextGenerationEU