Piano della sicurezza del Sistema di gestione informatica dei documenti

Indice generale

Piano della sicurezza del Sistema di gestione informatica dei documenti

Il Piano della sicurezza del Sistema di gestione informatica dei documenti descrive le misure tecniche ed organizzative attuate al fine di garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento (UE) 679/2016 per i documenti formati e gestiti dal Comune di Verona.

Il presente documento costituisce l'allegato 18 al manuale di gestione documentale dell'Ente.

Sistema di gestione informatica dei documenti

Il Comune di Verona utilizza il software Sicraweb per la tenuta del Protocollo Informatico e della Gestione Documentale, software su licenza Maggioli s.p.a. conforme al D.P.R. del 28/12/2000 n. 445 (cd. TUDA) e adeguato alle regole per la protocollazione previste dalle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

Il Manuale operativo è disponibile per gli utenti dell'Ente e costantemente aggiornato.

Misure di sicurezza e protezione dei dati personali adottate

Accesso al Sistema di gestione informatica dei documenti

L'accesso al Sistema di gestione informatica dei documenti integrato con il protocollo informatico (d'ora in poi, Sistema) avviene utilizzando le credenziali (utenza e password) rilasciate ai dipendenti dell'Ente per l'accesso alle risorse della rete informatica comunale. Utenza e password sono rilasciate in modo sicuro, in busta chiusa – de visu – dalla Direzione ICT e Transizione Digitale.

Gli utenti sono profilati sul Sistema in base agli uffici di appartenenza e le competenze assegnate; hanno quindi autorizzazioni di accesso differenziate ai documenti dell'Ente.

Le abilitazioni all'utilizzo delle funzionalità del Sistema, ovvero l'identificazione degli uffici e del personale abilitato allo svolgimento delle operazioni di registrazione di protocollo, organizzazione e tenuta dei documenti all'interno dell'AOO, sono sottoposte a costante verifica, gestione e aggiornamento da parte del Servizio Gestione flussi documentali-Conservazione (d'ora in poi, Servizio).

Ogni operazione effettuata da un utente nel Sistema relativa all'inserimento, modifica, cancellazione e visualizzazione di informazioni è tracciata in modo permanente, compresa l'individuazione dell'autore, ai sensi del capitolo 3.1.6 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

L'accesso al Sistema è automaticamente disabilitato dopo un periodo di tre mesi di inattività dell'utente.

Le sessioni multiple con la stessa user ID sono proibite e impedite dal Sistema.

Policy di visualizzazione dei documenti nel Sistema di gestione informatica dei documenti

Ogni utente abilitato all'accesso al Sistema è autorizzato a vedere i *metadati* di tutte le registrazioni di protocollo dell'Ente (oggetto, mittenti e destinatari, classifica, numero fascicolo) tranne per i documenti definiti "Riservati".

Ogni utente è inoltre abilitato alla visualizzazione degli allegati delle registrazioni di protocollo:

- assegnate in carico (in originale o copia) alla/e Struttura Organizzativa a cui è autorizzato;
- registrate dalla Struttura Organizzativa a cui è stato espressamente autorizzato.

Sono esclusi dalle logiche di accesso appena descritte i documenti "Riservati".

Il responsabile del Servizio, su richiesta del Dirigente di riferimento, può autorizzare livelli di accesso diversi e ulteriori per singoli o per categorie di utenti, sulla base di motivate esigenze connesse al ruolo ricoperto.

Protocolli riservati

Il Sistema consente di gestire un attributo di riservatezza per documenti relativi a vicende di persone o a fatti privati, con specifico riferimento alla tutela di categorie particolari di dati personali (cd. dati sensibili).

In fase di registrazione di un documento o anche in un momento successivo, qualora il contenuto lo richieda, la visibilità dello stesso può essere ristretta, utilizzando la funzione "Riservato" di Sicraweb.

I metadati di registrazione e gli allegati di un documento definito “Riservato” sono visibili esclusivamente agli uffici e/o dipendenti esplicitamente indicati. Il carattere di riservatezza non si estende ai documenti non riservati contenuti nel fascicolo nel quale il documento riservato è inserito.

Analisi dei rischi operativi e di sicurezza inerenti il Sistema

Il Sistema è parte integrante del più ampio Sistema Informativo del Comune di Verona: ne condivide quindi parte dell’architettura e dei sistemi di sicurezza adeguati alla protezione di tutto il patrimonio informativo dell’Ente.

Il Comune di Verona ,con determinazione dirigenziale n. 6517 del 27 dicembre 2021, ha approvato la ricognizione delle valutazioni effettuate relativamente alle attività di trattamento svolte dall’Ente in qualità di Titolare. Nell’elenco delle attività valutate è presente la ‘Gestione Documentale’, che comprende anche il Protocollo Informatico e la gestione dei Registri particolari.

La valutazione di impatto sulla protezione dei dati (DPIA/Data), prevista dall’art. 35 del Regolamento (UE) 2016/679 è uno strumento fondamentale che permette di valutare e dimostrare la conformità delle attività di trattamento e valida le procedure da adottare per la mitigazione del rischio derivante.

Al capitolo 5.3 della *Ricognizione valutazioni di impatto sulla protezione dei dati* – registrato agli atti con protocollo n. 444312/2021 – è descritta la valutazione di impatto rischi relativa all’attività di Gestione Documentale.

Il *Regolamento sulle modalità d’uso delle risorse informatiche e di altri strumenti di lavoro e sulle misure di sicurezza per il trattamento dei dati* adottato dal Comune di Verona contiene le politiche adottate dall’Ente per il corretto utilizzo di software e hardware, politiche applicabili anche alla gestione dei documenti informatici.

Continuità operativa del Servizio e misure minime ICT

Come previsto dall’articolo 51 del decreto legislativo 82/2005 (cd. CAD), «al fine di ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta di dati» il Comune di Verona ha adottato con Determina dirigenziale n.

5179 del 3/12/2020 le *Misure minime di Sicurezza ICT* e costantemente aggiorna sistemi e procedure informatiche ed organizzative.

Formazione del personale

Una formazione adeguata del personale autorizzato all'utilizzo del Sistema riduce i rischi di errata gestione e classificazione dei documenti. Con questo scopo sono tenuti dall'Ente:

- corsi di formazione per i nuovi utenti;
- pubblicazione di manuali aggiornati sulla Intranet;
- assistenza telefonica in caso di problemi o dubbi sulle funzionalità del software Sicraweb.