

Piano di Sicurezza dei Documenti Informatici

Comune di LOANO

(Codice Amministrazione Digitale
decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni)

Sommario

Obiettivi	3
Infrastruttura della rete Comunale	3
La sala macchine e la protezione dei dispositivi	4
Gestione della Sicurezza	4
Il documento “Misure minime di Sicurezza ICT” del Comune di Loano	4
Il documento “Disciplinare di utilizzo delle risorse informatiche e di trattamento dei dati” del Comune di Loano	4
Gli amministratori di sistema e la gestione utenti	4
Copie di Sicurezza.....	5
Protezione da virus e malware e controllo delle intrusioni	5
I sistemi per la gestione dei documenti.....	5
L’architettura della piattaforma documentale.....	6
Applicazioni che confluiscono sul sistema documentale	6
La protezione dei documenti informatici	7
Applicativi in Cloud.....	7
Applicativi Locali	7

ALLEGATO

Modello generale di Atto di designazione ad Amministratore di Sistema

Obiettivi

Il piano di sicurezza garantisce che le informazioni siano disponibili, integre, riservate e che per i documenti informatici sia assicurata l'autenticità, la non ripudiabilità, la validità temporale.

I dati, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento, vengono 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.

Il Servizio Informatica del Comune di Loano si occupa principalmente di

- Gestione dei sistemi informatici e telematici dell'Ente (con relativi processi di acquisto)
- Gestione infrastruttura di rete e sicurezza informatica
- Gestione e implementazione di data center locale con cluster di server fisici e virtuali
- Gestione e sviluppo degli aspetti tecnologici legati alla fonia mobile e fissa (esclusi processi di acquisto)
- Supporto allo sviluppo dell'agenda digitale locale
- Supporto agli utenti interni

Il servizio spazia dall'organizzazione dei servizi di mantenimento e di sviluppo degli applicativi e dei sistemi di base ad attività di progettazione di nuovi aggiornamenti e di potenziamenti tecnologici; dal supporto per la gestione tecnica di tutta la fonia, fino al governo e alla gestione delle relazioni, sia interne che esterne, oggi sempre più importanti e necessarie.

Il Servizio Informatica si occupa in particolare della gestione delle infrastrutture informatiche dell'Ente (rete, interconnessione verso terzi, dispositivi attivi, apparati e politiche relative alla sicurezza, sistemi di monitoraggio, gestione dei PC e dei Server e dei Database, gestione utenti e credenziali ecc.), della gestione dell'infrastruttura "applicativa" ovvero della configurazione, assistenza e formazione delle procedure gestionali utilizzate dai vari servizi dell'Ente, oltre allo sviluppo della intranet e delle procedure di supporto. Inoltre supporta il servizio organizzazione nell'analisi, ottimizzazione e digitalizzazione dei processi.

Infrastruttura della rete Comunale

Le principali sedi del Comune sono collegate tramite fibra ottica e ponti radio.

All'interno del palazzo del Comune, le fibre ottiche sono implementate su 2 anelli fisici ridondanti che collegano ogni piano dell'edificio principale. Ogni piano è fornito di HUB di rete che fornisce connessione LAN a 10/100/1000 Mbps.

Le sedi distaccate sono connesse con ponti radio a banda 300Mbps o con fibra ottica monomodale.

Il Data Center è costituito da un cluster di due server fisici nei quali vengono virtualizzati i server logici.

I due server fisici sono ridondanti. I NAS che ospitano gli hard disk sono in raid 5.

I server principali sono c/o la Sede del "CED – Sistemi informativi" di Piazza Italia, 2, e sono su un ramo di rete separato dai client tramite il firewall. Vengono implementate le VLAN per permettere la condivisione o l'indipendenza di risorse di rete.

Il bilanciamento tra i due server consente, in caso di problemi su un server, di averne un secondo disponibile, mentre l'infrastruttura virtuale consente di evitare che problemi fisici su un server (es: guasti di parti) rendano indisponibile il servizio. La tecnologia utilizzata permette inoltre di poter aumentare le risorse fisiche a disposizione dell'applicazione qualora siano necessarie maggiori prestazioni (es: attivazione di nuove funzionalità e/o crescita degli utilizzatori/attività).

L'accesso ai server è consentito solamente agli amministratori di sistema e agli amministratori degli applicativi installati sui server, sotto diretta sorveglianza del personale del servizio informatica.

Sugli apparati di rete vengono veicolate molteplici VLAN legate a vari servizi erogati su postazioni dell'Ente oltre alla rete dati interna.

Sono state, pertanto, implementate VLAN adibite a:

- postazioni pubbliche presso Ufficio Relazioni con il Pubblico e biblioteca
- DHCP per connessioni di PC non in dominio
- Rete VOIP
- Rete di Videosorveglianza

La sala macchine e la protezione dei dispositivi

La sala macchine è situata presso Sede del "CED - Sistemi Informativi" di Piazza Italia.

L'accesso ai locali della sala è protetto da un doppio accesso a chiusura con serratura e porte tagliafuoco.

Sistema di allarme attivabile quando non c'è personale in loco e sistema antincendio ad argon.

Gestione della 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 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;
- Accessibilità ai documenti informatici tramite sistemi informativi automatizzati;
- Archiviazione dei documenti nel tempo;
- Cooperazione applicativa documenti all'interno dello stesso ente e con enti diversi.

Il documento "Misure minime di Sicurezza ICT" del Comune di Loano

Le misure minime di sicurezza ICT per le Pubbliche Amministrazioni costituiscono parte integrante delle Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni ed hanno lo scopo di fornire alle pubbliche amministrazioni dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponda alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento.

Nel 2021 il dirigente responsabile dell'attuazione, coordinandosi con il Sindaco, ha provveduto a redigere, approvare e firmare il documento "Misure minime di Sicurezza ICT", che descrive le modalità con cui queste vengono attuate all'interno dell'Ente. Si rimandano quindi a tale documento per alcune parti del presente già descritte in esso.

Il documento "Disciplinare di utilizzo delle risorse informatiche e di trattamento dei dati" del Comune di Loano

Con deliberazione n. 50 del 09 giugno 2021 la Giunta Comunale ha approvato il disciplinare di utilizzo delle risorse informatiche. Tale documento rappresenta una raccolta di istruzioni operative che permettono di effettuare una gestione dei sistemi a garanzia della sicurezza delle informazioni in conformità a quanto richiesto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (da ora in poi RGDP).

Gli amministratori di sistema e la gestione utenti

Il Regolamento UE 2016/679 ("GDPR"), in combinato disposto con il D.Lgs. 30 giugno 2003, n. 196 ed i Provvedimenti dell'Autorità Garante per la protezione dei dati personali, nell'ambito della disciplina relativa al Titolare del Trattamento ("Comune di Loano"), prevede espressamente la nomina del/degli Amministratori di Sistema, anche al fine di regolamentare il trattamento dei dati personali.

L'attribuzione delle funzioni di Amministratore di Sistema deve pertanto avvenire con designazione formale, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, secondo le prescrizioni normative vigenti, da parte del Titolare del trattamento, che individua all'interno della propria struttura i soggetti che svolgono le attività tipiche

dell'amministratore di sistema sui dati e sistemi di cui si avvale il Titolare medesimo nell'ambito della propria attività di trattamento, con particolare riferimento alla sicurezza dei dati trattati, anche incidentalmente ed indirettamente, nell'esercizio delle proprie funzioni.

Più in particolare l'Amministratore di Sistema, con riferimento alla gestione dei sistemi informativi, dovrà attenersi scrupolosamente alle prescrizioni impartite dal Titolare del Trattamento, così come dettagliate nell'atto di designazione ad Amministratore di Sistema, il cui modello generale si allega al presente Piano a costituirne parte integrante e sostanziale. Il predetto atto dovrà essere personalizzato in relazione alle specifiche funzioni attribuite a ciascun Amministratore di Sistema.

Per quanto concerne la gestione degli utenti il rilascio delle credenziali è gestito dal Servizio Sistemi Informativi subordinato a previa comunicazione del Servizio Organizzazione risorse umane per il personale dipendente o del dirigente del servizio competente negli altri casi.

Le credenziali d'accesso sono nominative e personali ed è fatto assoluto divieto di comunicarle a soggetti terzi, come riportato nel disciplinare di utilizzo delle risorse informatiche, approvato con deliberazione di Giunta n. 50 del 09 giugno 2021, e ribadito all'atto della comunicazione delle credenziali stesse.

La password di accesso (come previsto dalla normativa vigente) è di almeno 8 caratteri per l'utenza normale, mentre di 14 caratteri per utenze amministratori di sistema, con livello di complessità impostato attraverso l'utilizzo di caratteri numerici, speciali ecc. e deve essere cambiata ogni 3 mesi.

Copie di Sicurezza

Per prevenire il rischio di perdita dei dati locali è attivo un sistema di backup, presso la sede del comune in Piazza Italia 2 e in una sede separata, nel rispetto dei parametri di Disaster Recovery.

La cadenza dei backup e delle repliche viene effettuata giornalmente per i differenziali e settimanalmente per i full backup. Tali backup vengono mantenuti per una durata non inferiore ai 10 mesi.

Un test di ripristino dei backup viene eseguito mensilmente e vengono effettuate due azioni, la prima riguarda un test di recupero di file random mentre la seconda è il ripristino di una intera macchina virtuale.

Sia i test che le operazioni eseguite a seguito di una problematica reale, vengono descritte in ticket dall'Ufficio Informatica.

È in programma l'esternalizzazione in cloud del sistema di backup aderendo alle disposizioni del Piano Triennale per l'Informatica 2020/2022. Il fornitore offre la possibilità di utilizzare servizi cloud per ospitare i backup oppure si potrà utilizzare un servizio di cloud in convenzione consip che disporrà di server in territorio italiano.

Protezione da virus e malware e controllo delle intrusioni

Il rischio di intrusione o di accesso indesiderato sia dall'interno che dall'esterno è garantito da un firewall hardware che governa e controlla gli accessi alla rete Comunale, sia tra i PC in ogni postazione che i server e tutti i dispositivi di rete connessi.

È stato implementato un antivirus centralizzato su server che permette la protezione dei server stessi e delle postazioni utente.

È altresì presente un servizio di antivirus e antispam gestito direttamente dal gestore di posta elettronica ARUBA che monitora il traffico email.

L'utilizzo di più sistemi di protezione e controllo situati in diversi punti, permette una maggiore robustezza verso le minacce esterne.

I sistemi per la gestione dei documenti

Le disposizioni dettate dal Codice della Amministrazione Digitale richiedono alle amministrazioni di adeguare il proprio sistema informativo e l'insieme delle applicazioni preposte alla produzione ed alla gestione di documenti digitali.

Il comune è da tempo dotato di Firme Digitali, sia USB che remote, utilizzate nella maggioranza dei processi documentali.

Il sistema adottato per la gestione documentale permette:

- Conservazione a norma dei documenti.

- Obbligo alla Trasparenza Amministrativa.
- Integrabilità informatica dei documenti nei flussi della organizzazione.
- Rispetto della normativa della privacy.
- Protocollo Informatico a norma di legge.
- Versamento del registro di protocollo.

Tutto ciò si rende possibile l'interoperabilità dei sistemi e degli Enti.

È attualmente utilizzata la Cooperazione Applicativa attraverso infrastrutture come ANPR e SDI.

Il Comune di Loano ha valutato che alla base di un'architettura di questo tipo sia fondamentale avere un sistema documentale strutturato: si è scelto il sistema SISCOM al cui interno sono presenti una serie di connettori finalizzati a colloquiare con i singoli gestionali, permettendo quindi di avere un raccoglitore "centrale" di tutti i documenti digitali dell'Ente.

L'applicativo GisMaster, gestito su server locale, viene utilizzato per la gestione della documentazione tecnica.

Sarà considerata la migrazione verso tecnologia Cloud.

L'architettura della piattaforma documentale

Il sistema documentale è interamente gestito in cloud dalla ditta SISCOM e l'interfaccia è completamente WEB. Questa particolarità permette l'utilizzo di tutti i gestionali da qualsiasi browser e da qualsiasi postazione che abbia un accesso ad Internet. Le interfacce sono di tipo "responsive", pertanto si adattano al dispositivo utilizzato per l'accesso (PC, tablet, smartphone).

Ad esso si aggiunge un sistema di cloud gestito su server interno, denominato NEXTCLOUD, rispetto della normativa GDPR, e viene utilizzato per la condivisione verso l'esterno di documenti informatici.

Internamente i documenti che vengono scambiati tra gli uffici possono essere depositati in cartelle di transito, eventualmente con accesso esclusivo a seconda dell'ufficio di appartenenza, su un server interno di scambio oppure utilizzando gli applicativi gestionali che permettono la condivisione tra uffici ed utenti.

Applicazioni che confluiscono sul sistema documentale

Le principali applicazioni utilizzate per l'informatizzazione dei procedimenti fanno parte della Suite Gestionale "SISCOM" ed è così composta:

- Olimpo, è il sistema che si occupa della gestione documentale e dell'archiviazione corrente dei documenti informatici formati dal Comune;
- Egisto, è la componente Sistema di protocollo informatico del Comune;
- Venere, è il sistema che consente la gestione dell'iter di formazione degli atti degli organi collegiali del Comune e delle figure dirigenziali ;
- Saturn, è la componente del sistema "Venere" che consente la gestione degli obblighi di pubblicazione nell'Albo pretorio online e nella sezione Amministrazione trasparente del sito istituzionale del Comune;
- Giove, è l'applicativo che consente la gestione degli atti di natura finanziaria del Comune (contabilità, bilancio, programmazione economico-finanziaria, tesoreria, ecc.);
- Piranha, è l'applicativo che consente la gestione del servizio imposte e tasse del Comune;
- Mercurio, è l'applicativo per la gestione delle presenze del personale del Comune;
- Selene, è l'applicativo che consente la gestione del sistema demografico ed elettorale del Comune;
- Sesamo, è l'applicativo che consente la gestione degli atti di stato civile del Comune;
- Tombal, è l'applicativo che consente la gestione delle strutture e delle concessioni cimiteriali del Comune;

- Esatur, è l'applicativo che consente la gestione delle utenze (bollettazione e riscossione) per il Comune;
- PagoInterface, è l'applicativo che consente la gestione dei pagamenti del Comune in modo integrato con la piattaforma pagoPA.

Tali applicazioni alla stesura del documento sono in fase di migrazione verso la soluzione CLOUD e pertanto attualmente sono configurate in parte in modalità client server ed in parte in modalità CLOUD, per alimentare e colloquiare con il sistema documentale. Lo scenario di miglioramento, prevede l'integrazione di altri gestionali (che producono documenti digitali) con il sistema di gestione documentale utilizzando i connettori descritti nei paragrafi precedenti.

La protezione dei documenti informatici

Per quanto riguarda la protezione dei documenti informatici, bisogna distinguere due gestioni differenti:

- Gli applicativi in Cloud
- Gli applicativi locali

Applicativi in Cloud

Per i primi, la protezione informatica e la gestione dei backup è demandata interamente al fornitore del servizio in quanto amministratore del proprio sistema. A livello applicativo la protezione è definita dagli accessi che sono regolamentati direttamente dal software e le cui credenziali di accesso sono personali, nominative e gestite sia dall'amministratore di sistema che internamente dal CED.

Applicativi Locali

La protezione a livello locale avviene sia tramite cartelle non accessibili a tutti gli utenti.

Gli utenti sono forniti di credenziali personali (login e password) e profilati in base all'ufficio di appartenenza o al ruolo o a specifiche richieste.

L'accesso ai documenti locali viene quindi effettuato:

- Ai singoli applicativi che sono fruibili solo all'interno della rete comunale previo accesso con le credenziali rilasciate ed eventualmente agli amministratori di sistema.
- Alla profilazione dell'utente per l'accesso alle cartelle di interscambio.
- Ad un unico link privato e non condivisibile per i documenti posizionati sul cloud di interscambio (anche
- verso l'esterno).

ALLEGATO

MODELLO GENERALE DI ATTO DI DESIGNAZIONE AD AMMINISTRATORE DI SISTEMA

ART. 28 DEL GDPR

Il Comune di Loano, avente sede in Piazza Italia n. 2 17025 – Loano (SV), C.F. 00308950096, di seguito, per brevità, anche indicato come “Comune di Loano”, in qualità di Titolare del trattamento ai sensi del Regolamento (UE) 2016/679 (*General Data Protection Regulation*, “**GDPR**”)

PREMESSO CHE

- nell’ambito della propria attività il Titolare tratta dati personali, avvalendosi di strumenti elettronici;
- tale trattamento è soggetto alle disposizioni del GDPR, della normativa italiana di armonizzazione (decreto legislativo 30 giugno 2003, n.196 recante il “Codice in materia di protezione dei dati personali”), nonché ai Provvedimenti dell’Autorità Garante per la protezione dei dati personali (complessivamente “Normativa privacy”);
- in forza del provvedimento del 27 novembre 2008 e ss.mm.ii., l’Autorità Garante per la protezione dei dati personali ha prescritto ai soggetti pubblici e privati l’adeguamento delle misure di sicurezza già in uso con l’adozione di altre e ulteriori finalizzate al corretto svolgimento delle funzioni degli amministratori di sistema;
- l’attribuzione delle funzioni di amministratore di sistema deve avvenire, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato secondo le prescrizioni dell’Autorità Garante;
- il Titolare ha individuato nell’ambito della propria struttura i soggetti che svolgono le attività tipiche dell’amministratore di sistema sui dati e sistemi di cui si avvale il Titolare nell’ambito della propria attività di trattamento;
- la presente designazione, potrà essere modificata o revocata qualora le condizioni che ne giustificano la formalizzazione cambino oppure vengano meno.

Tanto premesso e considerato, il Titolare del trattamento, come in epigrafe individuato e rappresentato, con la presente La designa Amministratore di Sistema (di seguito, “ADS”).

L’ ADS con la presente designazione assume il dovere di compiere quanto si renderà necessario ai fini del rispetto e della corretta applicazione della Normativa privacy, specialmente sotto il profilo della sicurezza dei dati trattati, anche incidentalmente ed indirettamente, nell’esercizio delle sue funzioni di amministratore di sistema.

Nello specifico, le funzioni che riguardano l’ADS attengono alla gestione, sotto il profilo degli aspetti di sicurezza, dei sistemi deputati al trattamento dati gestiti dall’amministratore di sistema per conto del Titolare e secondo indicazione di quest’ultimo.

Specificamente, con riferimento alla gestione dei sistemi informativi utilizzati dal Comune di Loano, l’ADS sarà tenuto a:

- agire nell’ambito di operatività consentito in base al profilo di autorizzazione assegnato, potendo effettuare le operazioni necessarie a garantire il corretto funzionamento nonché la sicurezza di tali sistemi. Nello svolgimento delle funzioni assegnate, l’ADS prende atto che non è autorizzato a

svolgere attività di trattamento ulteriori rispetto a quelle necessarie per la messa in sicurezza e per la manutenzione;

- gestire, attenendosi alle disposizioni impartite dal Titolare, il sistema informatico nel quale risiedono le banche dati personali, in osservanza della Normativa privacy;
- accedere alle banche dati attenendosi alle disposizioni impartite dal Titolare;
- non creare banche dati nuove senza espressa autorizzazione del Titolare;
- mantenere l'assoluto riserbo sui dati personali di cui viene a conoscenza, anche incidentalmente o per caso fortuito, in ragione dell'esercizio delle funzioni/mansioni assegnate;
- evitare di asportare supporti di qualsivoglia natura contenenti dati personali senza autorizzazione del Titolare;
- rispettare scrupolosamente tutte le misure di sicurezza già adottate o che verranno adottate in seguito dal Titolare;
- individuare misure di sicurezza ulteriori a quelle già in uso, che dovessero ritenersi necessarie per garantire congruo livello di protezione dei dati personali;
- limitatamente alla titolarità tecnica dei sistemi operativi in uso, effettuare l'aggiornamento dei medesimi nel rispetto delle disposizioni comunque impartite dal Comune di Loano, al fine di evitare accessi non consentiti ovvero trattamenti illeciti e la perdita dei dati;
- mantenere segrete le credenziali di autenticazione assegnate per l'accesso alla rete del Titolare;
- in caso di problematiche concernenti la sicurezza dei dati e dei sistemi, è fatto obbligo all'ADS di segnalarle senza ritardo al Titolare, indicando tutti gli aspetti necessari a circoscrivere la vulnerabilità, fornendo poi tutto il supporto possibile per apportare i correttivi necessari.
- generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, gli account (quindi le parole chiave ed i Codici identificativi personali) da assegnare alle persone autorizzate al trattamento dei dati dal Titolare, svolgendo anche la funzione di custode delle copie delle credenziali;
- adottare i programmi antivirus, firewall ed altri strumenti software o hardware indicati dal Titolare atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dal GDPR;
- adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico degli stessi con copie di back-up, vigilando sulle procedure adottate dal Titolare;
- assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- provvedere alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 e ss.mm.ii. in materia di smaltimento degli strumenti elettronici;
- vigilare sugli interventi informatici diretti al sistema informatico della società effettuati da operatori esterni. In caso di anomalie, segnalarle direttamente al Responsabile ADS e/o al Titolare;
- rispettare le istruzioni ricevute dal Titolare anche contenute nei documenti che disciplinano l'uso della strumentazione elettronica e informatica, le misure di sicurezza e le relative procedure applicate.

L'ADS è fin d'ora reso edotto del fatto che il suo operato sarà oggetto di loggatura e registrazione e che, con cadenza almeno annuale, il suo profilo sarà oggetto di attività di monitoraggio al fine di verificare la rispondenza alle misure organizzative, tecniche e di sicurezza predisposte per l'esercizio delle funzioni dell'amministratore di sistema. Ciò conformemente al punto 4.4 del Provvedimento del 27 novembre 2008 e s.mm.ii..

È fatto presente che la presente designazione potrà essere liberamente revocata in qualunque momento dal Titolare.

Loano, lì _____

Comune di Loano

L'Amministratore di Sistema