Comune di Fano

ALLEGATO AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DEIFLUSSI DOCUMENTALI.

Piano di Sicurezza dei Documenti Informatici (V. 1.0)

Sommario

Introduzione

Le Pubbliche Amministrazioni, ai sensi dell'art. 4, comma 1, lett. c del DPCM 3 dicembre 2013, nell'ottica di sviluppare concretamente il Sistema di gestione informatica dei documenti, devono predisporre il Piano per la sicurezza informatica relativo alla formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici, nel rispetto delle misure minime di sicurezza.
Il suddetto Piano deve essere predisposto dal Responsabile della gestione documentale, d'intesa con il Responsabile della conservazione, il Responsabile dei sistemi informativi e il Responsabile del trattamento dei dati personali.
La sicurezza di un sistema informativo è da intendersi come:
- La protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali.
- La limitazione degli effetti causati dall'eventuale occorrenza delle cause sopraindicate.
La sicurezza informatica è una caratteristica globale in grado di fornire il desiderato livello di disponibilità, integrità e riservatezza dei dati, informazioni, documenti e dei servizi erogati.

Gli aspetti principali:
- L'analisi dei rischi, cioè la valutazione dello stato attuale della sicurezza del sistema informativo, al fine di individuare le vulnerabilità del sistema, stimare l'esposizione al rischio e individuare le possibili misure di protezione.
- Le politiche di sicurezza, che specificano gli obiettivi, individuano le responsabilità e dichiarano l'impegno dell'Ente relativamente alla messa in sicurezza del sistema informativo.
- La gestione del rischio, cioè la ricerca dell'equilibrio tra i costi dei controlli individuati e il valore dei beni da proteggere (analisi costi/benefici), al fine di determinare il giusto livello di sicurezza da perseguire.

Normativa di riferimento

La fonte normativa di riferimento é il D.P.C.M. 3-12-2013. "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005"
1. In attuazione dell'art. 61 del DPR 445/2000, le pubbliche amministrazioni di cui all'art. 2, comma 2, del Codice definiscono le attribuzioni del responsabile della gestione documentale ovvero, ove nominato, del coordinatore della gestione documentale. In particolare, al responsabile della gestione e assegnato il compito di:
a) predisporre lo schema del manuale di gestione di cui all'art. 5;
b) proporre i tempi, le modalità e le misure organizzative e tecniche di cui all'art. 3, comma 1,lettera e);
c) predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico, d'intesa con il responsabile della conservazione, il responsabile dei sistemi informativi o il responsabile dell'ufficio di cui all'art. 17 del Codice e con il responsabile del trattamento dei dati personali, di cui al GDPR n. 679/2016 e al DPR 196/2003 e ss.mm.ii..
2. Il coordinatore della gestione documentale definisce e assicura criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione, nonchè di comunicazione interna tra le aree organizzative omogenee, ai sensi dell'art. 50 , comma 4, del DPR 445/2000"

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, l'estensione della validità temporale. I dati, in relazione delle conoscenze acquisite in base al progresso tecnologico e informatico, 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.

Architettura delle Infrastrutture e gestione della Sicurezza

Descrizione generale

La U.O.C. Sistema Informativo del Comune di FANO si occupa di:

- Gestione dei sistemi informatici e telematici dell'Ente (con relativi processi di acquisto)
- Attività di analisi e ricerca degli aspetti tecnologici legati alla fonia mobile e fissa ed al wifi pubblico
- Sviluppo e gestione del Sistema Informativo Territoriale
- Supporto allo sviluppo dell'agenda digitale locale.

Il servizio spazia dall'organizzazione dei servizi di mantenimento e analisi degli applicativi e dei sistemi di base, ad attività di progettazione di nuovi aggiornamenti e di potenziamenti tecnologici, fino al governo e alla gestione delle relazioni, sia interne che esterne.
Il servizio informativo si occupa sia della gestione delle infrastrutture tecnologiche che della gestione dei sistemi applicativi, in particolare delle 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 dell'analisi funzionale, test, configurazione, assistenza e formazione delle procedure gestionali utilizzate dai vari servizi dell'Ente (avvalendosi del supporto delle software house che sviluppano gli applicativi), oltre allo sviluppo di siti web e procedure di supporto. Inoltre supporta il servizio organizzazione nell'analisi, ottimizzazione e digitalizzazione dei processi.

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

Le misure minime di sicurezza ICT per le Pubbliche Amministrazioni, definite dalla Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015, 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.
Il funzionario P.O. responsabile dell'attuazione, in data 21.12.2017 ha provveduto a redigere e firmare il documento "Misure minime di Sicurezza ICT", che descrive le modalità con cui vengono attuate all'interno dell'Ente.
Si rimandano quindi a tale documento, alcune parti del presente, già descritte in esso.

La rete comunale

Le principali sedi e uffici del Comune sono collegati tramite collegamenti in fibra ottica alla LAN/MAN comunale.
I server sono tutti c/o la Sede del "Sistema Informativo Comunale" di Via San Francesco D'Assisi, 76 e, quelli con interfaccia di rete pubblica, sono su un ramo di rete separato tramite il firewall dai client.
Sugli apparati di rete vengono veicolate molteplici VLAN legate a vari servizi erogati su postazioni dell'Ente, oltre alla rete dati interna.

Su tutti gli apparati è veicolata una VLAN per la telefonia VOIP in modo da tenere separato il traffico dati da quello del VOIP.
Vd "Misure minime di Sicurezza ICT" quale integrazione/approfondimento.

La sala macchine e la protezione dei dispositivi

La sala macchine é situata presso Sede la Sede del "Sistema Informativo Comunale" di Via San Francesco D'Assisi, 76 . L'accesso ai locali dell' UOC SIC è protetto da un controllore di accessi con badge, in particolare l'ingresso della sala è autorizzato solo agli operatori dell'U.O.C. SIC autorizzati ad operare all'interno di essa.
Si rimanda al *Vd "Misure minime di Sicurezza ICT – Inventario dei dispositivi autorizzati e non autorizzati" quale integrazione/approfondimento.*

Gli amministratori di sistema e la gestione utenti

Il rilascio delle credenziali è gestito dal servizio Sistema Informativo Comunale, subordinato alla comunicazione del Dirigente del servizio responsabile del personale dipendente a tempo determinato o indeterminato, o alla compilazione della richiesta di accesso firmata dal Dirigente del servizio per i collaboratori esterni.
Le credenziali d'accesso sono nominative e sia nelle "Norme interne per il corretto utilizzo delle attrezzature e dei servizi informatici" che durante gli interventi formativi, viene ribadito che sono strettamente personali e che è fatto assoluto divieto di comunicarle a soggetti terzi.
La password di accesso (come previsto dalla normativa vigente) è di almeno 8 caratteri, e deve essere cambiata ogni 90gg.
Vd "Misure minime di Sicurezza ICT - INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI" quale integrazione/approfondimento.

Copie di sicurezza

Per prevenire il rischio di perdita dei dati è attivo un sistema di backup che, a seconda del tipo di dato e della sua variabilità, effettua una copia di sicurezza più volte al giorno. Queste copie, sempre a seconda del tipo di dato, vengono mantenute per un tempo ulteriore.
Conformemente a quanto previsto dalla politiche di continuità dei servizi di AGID, è in stato attivato un sistema di *disaster recovery* su un sito remoto identificato nel *datacenter* di FILIPPETTI SPA ad almeno 100 km dal data center comunale. Pertanto una copia viene archiviata nel data center citato in modo da permettere, in caso di danno grave ai sistemi presenti nei locali dell'U.O.C. Sistema Informativo Comunale di recuperare i dati.

Vd "Misure minime di Sicurezza ICT – Copie di Sicurezza" quale integrazione/approfondimento.

Protezione dei dati

Vd "Misure minime di Sicurezza ICT – Protezione dei dati" .

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 che, come già detto, governa e controlla gli accessi tra i pc degli uffici comunali ed i server che ospitano i dati e l'applicazione stessa ed impedisce anche l'accesso dall'esterno. Il firewall ha attivo un sistema di *Intrusion prevention systemp (IPS)* con politiche che permettono di prevenire e bloccare attacchi interni o esterni. Queste politiche vengono aggiornate automaticamente in modo che tengano conto delle ultime vulnerabilità rese note.

Il Firewall è implementati con prodotti di fascia *Enterprise* e dei maggiori marchi presenti sul mercato.
All'interno della rete, sia a protezione dei server che delle postazioni utente interne (che possono essere a loro volta un mezzo anche inconsapevole di intrusione), sono attivi due antivirus di tecnologie differenti e l'antispam. L'uso ditecnologie diverse e/o produttori diversi aumenta il grado di protezione poichè una minaccia puo essere intercettata di un sistema ma non da un altro.
Vd "Misure minime di Sicurezza ICT - DIFESE CONTRO I MALWARE"

Analisi delle minacce e delle vulnerabilità dell'infrastruttura informatica di rete

Vd "Misure minime di Sicurezza ICT - VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ"
7

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; in particolare l'introduzione della firma digitale necessita l'adeguamento dei processi documentali istituzionali per garantire la certezza giuridica dei documenti prodotti e archiviati e l'aderenza alla norma dei procedimenti, garantendo in particolare:

- Conservazione a norma dei documenti
- Obbligo alla Trasparenza amministrativa
- Integrabilità informatica dei documenti nei flussi della organizzazione
- Rispetto della normativa della privacy

Tutto ciò si rende possibile avviando un progetto di infrastruttura documentale centralizzata e definendo una metodologia di integrazione graduale degli applicativi documentali che segua standard di interoperabilità.
Il Comune di Fano ha valutato che alla base di un'architettura di questo tipo sia fondamentale avere un sistema documentale strutturato: si è scelto il sistema Alfresco Community Edition con una serie di connettori finalizzati a colloquiare con i singoli gestionali, finalizzata ad avere un raccoglitore "centrale" di tutti i documenti digitali dell'Ente.

L'architettura della piattaforma documentale

Il sistema documentale è installato su un Server Virtuale contenti il database e l'applicativo che ne permette la ricerca e il recupero.
L'applicazione permette la conservazione a norma integrata con il polo regionale DIGIP della Regione Marche.
Per tale gestione è attiva una procedura di conservazione per documenti digitali conforme alla normativa italiana in grado di produrre automaticamente e manualmente i volumi di conservazione, e colloquia con il sistema DIGIP della Regione Marche.
Si basa sul concetto di volume di conservazione quale contenitore logico dei documenti in grado di dare certezza di integrità (non modifica) a tutto il contenuto. I volumi, che sono specifici per le tipologie di documenti trattati, incapsulano le regole di conservazione dettate da Agid e svolgono automaticamente sui contenuti una serie di controlli di aderenza alla norma.
Il sistema DIGIP è corredato da una pratica interfaccia web per svolgere le operazioni del processo di conservazione, controllarne l'andamento, rilevare eventuali errori sui volumi di conservazione e l'eventuale stato della loro spedizione ai conservatori esterni, recuperare volumi in conservazione.

Questa attività viene eseguita prevalentemente dalla software house incaricata e il sistema informativo comunale ha la possibilità di verificare e controllare il buon andamento del processo, oltre alla possibilità di ricercare la documentazione conservata.

Applicazioni che confluiscono sul sistema documentale

Le principali applicazioni utilizzate per l'informatizzazione dei procedimenti fanno parte della SUITE CITYWARE e sono denominati "CITYMEDIA" (per la gestione delle determinazioni dirigenziali, delibere di Giunta e di Consiglio), "CITYFINANCING" (per la gestione delle fatture elettroniche attive e passive) e "IT@LPRO" (per la gestione del Protocollo generale) e Albo Pretorio Online.
Tali applicazioni sono già configurate, ed in parte attivate anche in produzione, 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 Alfresco.
Sono in fase di avviamento a partire dal 01 gennaio 2020 i collegamenti con nuovi gestionali:

- SUAE
- SUAP
- COMMERCIO

Caratteristiche e gestione delle procedure Atti e Protocollo

Le applicazioni della SUITE CITYWARE e "IT@LPRO" sono installate su server virtuali che operano su un'infrastruttura VMWARE. Questa scelta consente di avere un alto livello di disponibilità del servizio e di prevenire rischi che malfunzionamenti hardware o software impediscano al personale dell'Ente di utilizzare le applicazioni suddette.
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).
I dati gestiti dalle applicazioni sono memorizzati all'interno di un database "POSTGRES", mentre i documenti firmati digitalmente e gli allegati possono essere memorizzati in cartelle apposite sul file system non accessibili agli utenti (ma solo alle applicazioni e agli amministratori di sistema) e/o sul documentale Alfresco accessibile solo dalle procedure stesse o agli utenti autorizzati.
L'accesso ai server per attività diverse dall'utilizzo delle procedure suddette è consentito ai soli amministratori di sistema (personale addetto dell'U.O.C. Sistema Informativo Comunale) e dal personale autorizzato delle software house titolari del contratto di manutenzione delle applicazioni sopra citate, nominati come previsto dalla normativa vigente in materia di trattamento dei dati personali e sensibili.
Le applicazioni della SUITE CITYWARE e "IT@LPRO" sono fruibili **solo dalle postazioni all'interno degli uffici comunali e previo collegamento con le credenziali rilasciate** dal Servizio "Sistema Informativo Comunale".
L'utilizzo alle procedure della SUITE CITYWARE e "IT@LPRO" da parte del singolo dipendente/collaboratore deve essere esplicitamente richiesto dal Dirigente del servizio e sono previsti diversi ruoli a seconda delle competenze e funzionalità a cui l'operatore deve essere abilitato. Tale profilazione arriva al dettaglio di ogni singola operazione.
Le regole suddette permettono di tutelare l'accesso indesiderato alle informazioni all'interno delle procedure e la privacy delle stesse.
I programmi della SUITE CITYWARE e "IT@LPRO" prevedono inoltre un registro delle attivita (Log) accessibile solo agli amministratori che permette, in caso di necessità, di vedere il tipo di operazioni effettuate da un utente pur senza entrare nello specifico dei dati inseriti (es: vedere che in una certa data/ora e' stata creata una determina, ma senza conoscere il contenuto o le informazioni della determina stessa).

Utilizzo applicativo Protocollo Informatico IT@LPRO

L'applicativo di gestione del Protocollo Informatico riferito in oggetto è realizzato nel rispetto delle indicazioni fornite dalla normativa vigente, ed in particolare tenendo a riferimento quanto previsto dalle "Regole Tecniche sul Protocollo Informatico" (**DPCM 3 Dicembre 2013).**
Il sistema di protocollo, lato utente, funziona in modalità web, l'utilizzo del tipo di browser non è vincolante.
Le responsabilità delle azioni compiute nella fruizione del servizio di protocollo è dell'utente fruitore del servizio. Gli utenti autorizzati ad accedere al servizio di protocollo dispongono di una propria credenziale personale (userid e password), rilasciata a seguito di una richiesta effettuata dal dirigente/responsabile, il quale definisce il profilo di accesso e le relative autorizzazioni in merito alla visibilità ed alla gestione delle informazioni che l'utilizzatore deve avere.
Le credenziali di accesso non devono mai essere cedute a terzi e la responsabilità delle operazioni compiute tramite un'utenza è sempre del legittimo titolare, anche se compiute in sua assenza.
Per la corretta fruizione del servizio di protocollo informatico e di gestione documentale e al fine di tutelarne l'accesso, è necessario che l'utente adotti almeno le seguenti buone norme di comportamento relative alla gestione del proprio posto di lavoro:

- La stazione di lavoro non deve essere lasciata incustodita con la sessione attiva, anche per brevi periodi;
- Prima di allontanarsi, anche momentaneamente, devono essere attivati i sistemi di protezione esistenti relativamente alla postazione di lavoro (ad esempio blocco tramite Ctrl-Alt-Canc).