COMUNE DI
REGGIO EMILIA

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

ALLEGATO L

Piano di Sicurezza dei Documenti Informatici

Comune di Reggio Emilia

COMUNE DI
REGGIO EMILIA

Indice generale

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 previste nel disciplinare tecnico pubblicato in allegato B del D.Lgs. 196/2003 «Codice della Privacy»".
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 è 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" che all'Articolo 4 definisce nel seguente modo i compiti del Responsabile della gestione documentale e i contenuti del piano di sicurezza per i documenti informatici:

"Art. 4. Compiti del responsabile della gestione documentale

1. In attuazione dell'art. 61 del testo unico, 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 è 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 pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni, d'intesa con il responsabile della conservazione, il responsabile dei sistemi informativi o, nel caso delle pubbliche amministrazioni centrali, il responsabile dell'ufficio di cui all'art. 17 del Codice e con il responsabile del trattamento dei dati personali di cui al suddetto decreto.
2. Il coordinatore della gestione documentale definisce e assicura criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione, nonché di comunicazione interna tra le aree organizzative omogenee, ai sensi dell'art. 50 , comma 4, del testo unico."

Architettura delle Infrastrutture e gestione della Sicurezza

Descrizione generale

Il Servizio Tecnologie e sistemi informativi del Comune di Reggio Emilia si occupa di

- Gestione dei sistemi informatici e telematici dell'Ente (con relativi processi di acquisto)
- Gestione e sviluppo degli aspetti tecnologici legati alla fonia mobile e fissa (esclusi processi di acquisto), alla videosorveglianza 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 di sviluppo degli applicativi e dei sistemi di base, ad attività di progettazione di nuovi aggiornamenti e di potenziamenti tecnologici; alla 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 è suddiviso in due unità operative, una addetta alla gestione delle infrastrutture tecnologiche e l'altra addetta alla gestione dei sistemi applicativi.

La Unità "Gestione delle Strutture tecnologiche" si occupa in particolare delle gestione delle infrastrutture informatiche dell'Ente (rete, interconnessione verso terzi, dispositivi attivi, apparati e politiche relativi alla sicurezza, sistemi di monitoraggio, gestione dei PC e dei Server e dei Database, gestione utenti e credenziali ecc.)

L' Unità "Gestione dei Sistemi Informativi" si occupa invece della gestione dell'infrastruttura "applicativa"' ovvero dell'analisi funzionale, test, configurazione, assistenza e formazione delle procedure gestionali utilizzate dai vari servizi dell'Ente, 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 Reggio Emilia

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 29 Dicembre 2017 (provvedimento dirigenziale n. 1889 del 29/12/2017), il dirigente responsabile dell'attuazione, assieme al Sindaco, ha provveduto a redigere, approvare 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. Le fibre ottiche insistono su 5 anelli fisici della MAN cittadina. La maggioranza delle sedi sono connesse tramite doppio percorso e ogni anello può connettere una o più sedi.
I server sono tutti c/o la Sede del "Servizio Tecnologie e Sistemi Informativi" di Piazza Scapinelli e 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, come ad esempio Lan per Internetpoint, Lan per postazioni pubbliche, lan di servizio, ecc...
Su tutti gli apparati è veicolata una VLAN per la telefonia VOIP in modo da tenere separato il traffico dati da quello del VOIP.
Per ridurre i domini di broadcast all'interno della rete, le varie sedi periferiche sono state tutte divise in subnet differenti e tutte ruotate staticamente dal Black Diamond.
Vd "Misure minime di Sicurezza ICT" quale integrazione/approfondimento.

La sala macchine e la protezione dei dispositivi

La sala macchine è situata presso Sede del "Servizio Tecnologie e Sistemi Informativi" di Piazza Scapinelli.

L'accesso al Palazzo, ma anche ai locali della sala, è protetto da un controllore di accessi con badge, in particolare l'ingresso della sala abilitato solo agli operatori del Servizio Tecnologie 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 Tecnologie e Sistemi Informativi subordinato alla comunicazione del Servizio Personale per il personale dipendente a tempo determinato o indeterminato, o alla compilazione della richiesta di accesso firmata digitalmente dal Dirigente del servizio per i collaboratori esterni.
Le credenziali d'accesso sono nominative e sia nel Regolamento sull'ordinamento generale degli uffici e dei servizi (art.44 sez. C), 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, con alto livello di complessità (obbligo di caratteri numerici, speciali ecc.) e deve essere cambiata ogni 3 mesi con history di 11.
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. Una copia viene anche archiviata in un sito esterno in modo da permettere, in caso di danno grave ai sistemi presenti nei locali del Servizio gestione e sviluppo delle tecnologie, di recuperare i dati.
Conformemente a quanto previsto della politiche di continuità dei servizi di AGID, è in stato attivato un sistema di *disaster recovery* su un sito remoto identificato nel *datacenter* di Ravenna gestito da Lepida Spa (società in-house della Regione Emilia Romagna) di cui tutte la PA della Regione sono socie.
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.
Oltre al firewall, per governare e prevenire un accesso indesiderato dall'esterno, è presente un *Reverse Proxy* che utilizza una tecnologia diversa da quella del firewall e costituisce una seconda barriera per un eventuale tentativo di accesso.
Sia Firewall che Reverse Proxy sono 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 diverse e l'antispam. L'uso di tecnologie diverse e/o produttori diversi aumenta il grado di protezione poiché una minaccia può 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"

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 definire una metodologia di integrazione graduale degli applicativi documentali che segua standard di interoperabilità.

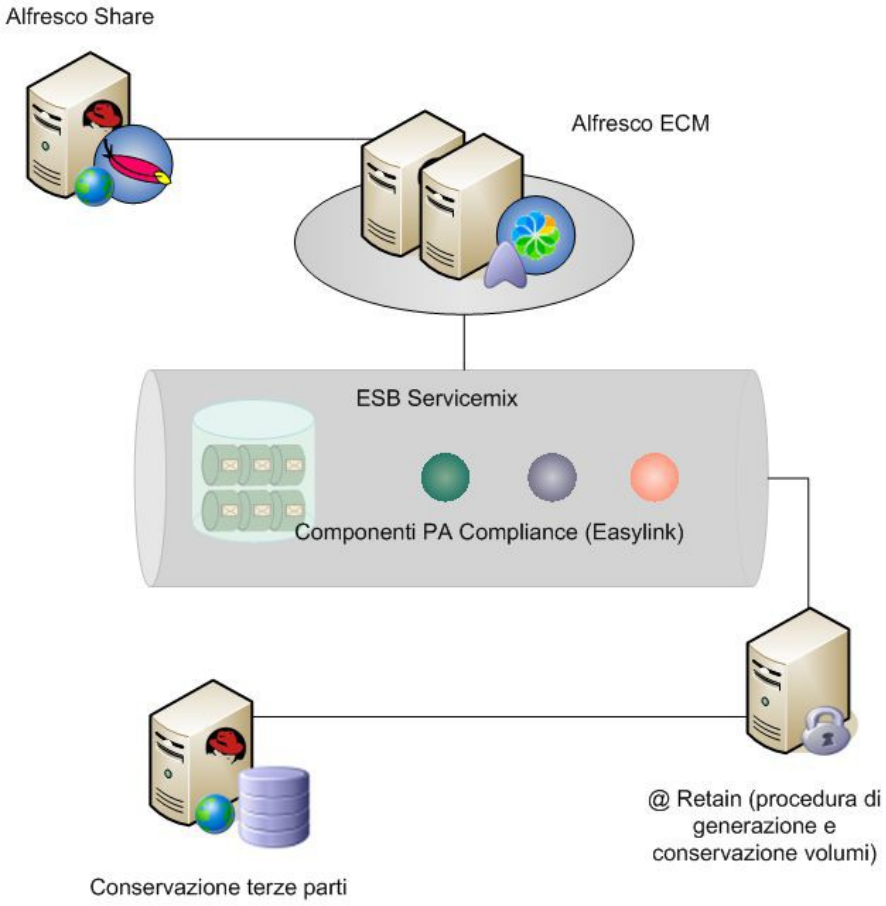
Il Comune di Reggio Emilia ha valutato che alla base di un'architettura di questo tipo sia fondamentale avere un sistema documentale strutturato: si è scelto il sistema Alfresco Community Edition con una serie di connettori finalizzati a colloquiare con i singoli gestionali, finalizzata ad avere un raccoglitore "centrale" di tutti i documenti digitali dell'Ente
I vari applicativi verticali, a regime, dovranno memorizzare i documenti digitali su questo raccoglitore.

L'architettura della piattaforma documentale

Il sistema documentale e l'ESB con i relativi connettori di colloquio è installato su 3 Server Virtuali contenti il database, SOLR (per l'indicizzazione dei testi), connettori di colloquio e l'applicazione che permette la conservazione a norma integrata con il polo regionale Parer.
Esiste anche un analogo ambiente di test utilizzato per prove, verifiche di aggiornamenti ecc.

Tecnicamente quindi esiste un Enterprise Service Bus (Apache Servicemix) che gestisce i connettori di colloquio con i vari gestionali e permette di ricevere in maniera trasparente i documenti prodotti dai vari applicativi sui repository del documentale Alfresco, completi di metadati di classificazione.
Su tale archivio opera @Retain, la suite per la gestione della Conservazione, che permette di generare e gestire i pacchetti di versamento per Parer.

A seguito uno schema che illustra l'architettura di tale sistema.



parer
POLO ARCHIVISTICO REGIONALE DELL'EMILIA ROMAGNA

Caratteristiche di @ Retain (suite per la gestione della Conservazione)

@-Retain è 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 Parer (Regione Emilia Romagna).
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 per proprietà transitiva. 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.
@-Retain 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.

Applicazioni che confluiscono sul sistema documentale

Le principali applicazioni utilizzate per l'informatizzazione dei procedimenti fanno parte del Gestionale “Inf.or” e sono denominati “jEnte Atti” (per la gestione delle determinazioni dirigenziali, delibere di Giunta e di Consiglio) e “jEnte Protocollo” (per la gestione del Protocollo generale) e Albo Pretorio

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 utilizzando i connettori descritti nei parametri precedenti.

Sono in fase di avviamento o analisi i collegamenti con nuovi gestionali:

- Edilizia
- Contabilità
- Entrate

Caratteristiche e gestione delle procedure Atti e Protocollo

Le applicazioni “jEnte Atti” e “jEnte Protocollo” sono installate su due server virtuali in bilanciamento 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.
Il bilanciamento tra i due server consente infatti, in caso di problemi software 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).

I dati gestiti dalle due applicazioni sono memorizzati all'interno di un database “Oracle”, 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.

Tutti i server su cui sono memorizzati dati e/o le applicazioni stesse, sono collegati ad un ramo di rete separato rispetto a quello in cui si trovano le postazioni pc degli utilizzatori e con un livello di sicurezza maggiore. L'accesso da parte dei pc all'applicazione e' governato dal firewall. Questo permette di evitare che azioni maligne o compromissioni delle postazioni utente possano mettere a rischio la sicurezza delle applicazioni “jEnte Atti” e “jEnte Protocollo” e delle informazioni in essa contenute.

L'accesso ai server per attività diverse dall'utilizzo delle procedure jEnte è consentito ai soli amministratori di sistema (personale addetto del Servizio Gestione e Sviluppo delle Tecnologie e dei Sistemi Informativi) nominati come previsto dalla normativa vigente in materia di trattamento dei dati personali e sensibili.

Le applicazioni “jEnte Atti” e “jEnte Protocollo” sono fruibili **solo dalle postazioni all'interno degli uffici comunali e previo collegamento con le credenziali rilasciate** dal Servizio Gestione e Sviluppo delle Tecnologie e dei Sistemi Informativi.

L'utilizzo alla procedura “jEnte – Atti” e “jEnte – Protocollo” 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 “jEnte – Atti” e “jEnte – Protocollo” prevedono inoltre un registro delle attività (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).

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).**