COMUNE DI
REGGIO EMILIA

Manuale di gestione documentale del Comune di Reggio Emilia

Allegato 6

PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI

COMUNE DI
REGGIO EMILIA

Indice generale

Introduzione

Le Pubbliche Amministrazioni, ai sensi del paragrafo § 3.9 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia per l'Italia Digitale – AgID, nell'ottica di ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017 predispongono il "Piano della sicurezza del sistema di gestione informatica dei documenti", prevedendo opportune misure tecniche e organizzative per 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 (GDPR), anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso".
Il suddetto Piano deve essere predisposto dal Responsabile della gestione documentale, d'intesa con il Responsabile della conservazione, il Responsabile per la transizione digitale e il Responsabile per la protezione 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 che la compongono sono:

- 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 sono le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia per l'Italia Digitale – AgID, che al paragrafo 3.4 definiscono nel seguente modo i compiti del Responsabile della gestione documentale e i contenuti del piano di sicurezza per i documenti informatici:

"3.4. Compiti del responsabile della gestione documentale

"Il responsabile della gestione documentale è preposto al servizio di cui all'articolo 61 del TUDA e, d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale di cui all'art.17 del CAD e acquisito il parere del responsabile della protezione dei dati personali, di cui agli artt. 37 "Designazione del responsabile della protezione dei dati" e 39 "Compiti del responsabile della protezione dei dati" del Regolamento UE 679/2016, predispone:

- il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione.

Tale manuale conterrà inoltre, come parte integrante dello stesso, il piano per la sicurezza informatica, per la quota parte di competenza, nel rispetto delle:

- misure di sicurezza predisposte dall'AgID e dagli altri organismi preposti;
- delle disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio fatta;
- indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AgID.”

Architettura delle Infrastrutture e gestione della Sicurezza

Descrizione generale

Il Servizio Gestione e sviluppo delle tecnologie e dei 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 WI-FI 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.

L'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 "MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA"

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 e 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 "MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA", che descrive le modalità con cui vengono attuate all'interno dell'Ente. Si rimanda quindi a tale documento per alcune parti del presente Piano.

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 è connessa tramite doppio percorso e ogni anello può connettere una o più sedi.
I server fisici sono nei Datacenter di Lepida SCPA, società in house della regione Emilia Romagna deputata all'infrastrutturazione tecnologica del territorio. Tali datacenter rientrano nell'elenco dei "Poli Strategici Nazionali" definiti di AGID in base a requisiti di sicurezza molto stringenti. La configurazione adottata è pertanto pienamente conforme nelle direttive a cui gli enti della PA si devono attenere per garantire un adeguato livello di sicurezza dei propri dati
L'accesso al Datacenter di Lepida è totalmente ridondato (doppio apparato attivo, doppio percorso) ed erogato tramite link 10 Gb aggregati.
Dal punto di vista logico i server sono su un ramo di rete dedicato e separato tramite il *firewall* dai *client o da altri*

oggetti più critici dal punto di vista delle possibili intrusioni.
La separazione del traffico e quindi la sicurezza dei sistemi è garantita anche dall'uso di VLAN distinte, con diversi livelli di sicurezza, per i vari servizi erogati dall'ente

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 ruotate staticamente dal Black Diamond.

Eventuali accessi dall'esterno a sistemi non visibili da internet è consentito tramite VPN SSL gestite direttamente dal firewall e abilitate dopo un processo autoritativo normato e gestito direttamente dal Personale del "Servizio Gestione es viluppo delle tecnologie e dei sistemi informativi"
Anche lo smartworking è stato attivato tramite VPN nominative

La sala macchine e la protezione dei dispositivi

Tutti i collegamenti della periferia confluiscono presso un locale tecnico (sala macchine) che è situata presso la sede del Servizio Sviluppo delle tecnologie e dei sistemi informativi di Piazza Scapinelli.
Nello stesso locale sono installati anche gli apparati che permettono il collegamento con i Datacenter di Lepida. È quindi un punto importante per garantire l'accesso ai dati.
Per questa ragione l'accesso al Palazzo, ma anche ai locali della sala, è protetto da un controllo di accessi con badge; in particolare, l'ingresso della sala è abilitato solo agli operatori del Servizio autorizzati ad operare all'interno di essa.
Sono attivati sistemi di prevenzione come antintrusione, videosorveglianza, antincendio per garantire la sicurezza dei locali

Gli amministratori di sistema e la gestione utenti

Il rilascio delle credenziali è gestito dal Servizio Sviluppo delle tecnologie e dei sistemi informativi e subordinato alla comunicazione al 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) sia durante gli interventi formativi, viene ribadito che esse 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.
Per alcuni servizi accessibili da web è stato attivato accesso a due livelli tramite OTP via sms / email. Per altri è in corso di attivazione.

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. Tali 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 il recupero dei dati in caso di danno grave ai sistemi presenti nei locali del Servizio gestione e sviluppo delle tecnologie.
Conformemente a quanto previsto della politiche di continuità dei servizi di AgID, è stato attivato un sistema di *disaster recovery* su un sito remoto rispetto a quello in cui si trova il back-up principale : dati e back-up principale sono sul sito di Ferrara, back-up per disaster recover sul sito di Modena. Tutti i back-up (cosi' come i sistemi attivi sia si test che di produzione) si trovano nei Datacenter di lepida SCPA e vengono effettuati, tramite software dedicato, su dispositivi con dischi dedicati che prevedono archiviazione con meccanismi di deduplica e compresisone. Il formato con cui sono memorizzati i back-up è accessibile solo tramite software specifico.

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 attivi diversi moduli per prevenire attacchi (*Intrusion prevention systemp IPS*, *antivirus*, *application control*, *antibot*) 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. È inoltre attivo un sistema di Thread Emulation per controllare e bloccare malware presenti in allegati di mail o scaricati da internet.
Un sistema di URL filter controlla la navigazione degli utenti per evitare l'accesso a siti pericolosi.
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 dall'altro.

Tutti gli endpoint sono protetti da antivirus Kaspersky che applica filtri non solo reputazionali ma anche comportamentali e che viene tenuto aggiornato e monitorato centralmente

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

È attivo un servizio di sicurezza denominato CERTEGO. Tale servizio tramite una sonda installata presso l'ente consente di analizzare il traffico da/per internet e di evidenziare eventi anomali. Tramite il supporto di specialisti della sicurezza consente di eliminare alert causati da falsi positivi, fornisce indicazioni sulle azioni da svolgere per chiudere la vulnerabilità, permette di attivare accorgimenti per prevenire attacchi a fronti di nuovi bug appena viene resa nota una vulnerabilità

I sistemi per la gestione dei documenti

Le disposizioni dettate dal Codice dell'amministrazione digitale – CAD 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 si è dotato già da alcuni anni un sistema di gestione “Protocollo e Atti” che permette una corretta gestione di documenti informatici, la cooperazione applicativa con i vari software verticali e la trasmissione verso il servizio di conservazione regionale (ParER).

L'architettura della sistema di gestione “Protocollo e Atti”

La suite jEnte, utilizzata come sistema per la gestione documentale, possiede alcune applicazioni, tra le quali:

- “jEnte Atti” (per la gestione delle determinazioni dirigenziali, delibere di Giunta e di Consiglio)
- “jEnte Protocollo” (per la gestione del protocollo generale)
- “Albo Pretorio”.

jEnte è installato su due server virtuali in bilanciamento che operano su un'infrastruttura VMWARE presso il datacenter di LEPIDA.
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 (ad 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 (ad 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 vengono memorizzati (dall'applicazione stessa) in cartelle apposite sul *file system* non accessibili agli utenti (ma solo alle applicazioni e agli amministratori di sistema) e/o sul documentale Alfresco (per invio in conservazione) accessibile solo alle procedure stesse o agli utenti autorizzati.

Tutti i server su cui sono memorizzati dati e/o le applicazioni stesse sono collegati a 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 è 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.

L'applicativo di gestione del protocollo informatico sopradescritto è realizzato nel rispetto delle indicazioni fornite dalla normativa vigente, ed in particolare tenendo a riferimento quanto previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

Regole di accesso

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 della procedura "jEnte – Atti" e "jEnte – Protocollo" da parte del singolo dipendente/collaboratore deve essere esplicitamente richiesto dal Dirigente del Servizio cui il dipendente/collaboratore appartiene e sono previsti diversi ruoli utente a seconda delle competenze e funzionalità a cui l'operatore deve essere abilitato. Tale profilazione arriva al dettaglio di ogni singola operazione.
Le suddette regole 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 verificare il tipo di operazioni effettuate da un utente pur senza entrare nello specifico dei dati inseriti (ad es., vedere che in una certa data/ora è stata creato un atto, ma senza conoscere il contenuto o le informazioni dell'atto stesso).

Applicazioni che colloquiano sul sistema di gestione "Protocollo e Atti"

Le principali applicazioni verticali utilizzate per l'informatizzazione dei procedimenti amministrativi, che gestiscono o producono documenti informatici, sono state configurate per permettere la protocollazione in entrata ed in uscita dialogando con il sistema di protocollo utilizzando i relativi servizi web (JProtocolloServices).

Conservazione dei documenti informatici

Le applicazioni "jEnte Atti" e "jEnte Protocollo" gestiscono l'invio in conservazione dei documenti informatici a PareER, (Polo archivistico regionale) in modalità "diretta" (connettore di jEnteProtocollo) o "indiretta" (tramite @Retain per jEnteAtti su documentale Alfresco).
Tale architettura è in fase di ottimizzazione e miglioramento alla luce delle recenti *Linee Guida per la formazione, gestione e conservazione dei documenti informatici* emanate dall'Agenzia per l'Italia Digitale – AgID.
Per ulteriori approfondimenti si rimanda al Manuale di conservazione del Comune di Reggio Emilia.