CITTÀ DI GRANAROLO DELL'EMILIA

Allegato G

PIANO DELLA SICUREZZA INFORMATICA

Indice generale

1. Premessa

Nel descrivere l'obiettivo di questo documento e guidare alla comprensione del suo contenuto, è doverosa una sintesi sul contesto normativo in materia di privacy e di sicurezza, perché ci troviamo di fronte ad un imminente cambiamento di rotta a livello europeo, che era atteso da diversi anni.

1.1 Contesto normativo presente e futuro

È vigente ora in Italia il Decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali". Con la sua entrata in vigore, il legislatore ha sancito che il diritto alla riservatezza, all'identità personale e alla protezione dei dati riferiti a persone fisiche o giuridiche sono da annoverarsi tra i diritti fondamentali. Di conseguenza qualsiasi trattamento di dati personali deve svolgersi nel rispetto della dignità del soggetto interessato sottoposto al trattamento.

Il contesto europeo da cui tale decreto prende vita, è la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995.
Nel gennaio 2012 la Commissione europea ha presentato le proposte relative al nuovo quadro giuridico europeo in materia di protezione dei dati. Un nuovo Regolamento che andrà a sostituire la Direttiva in vigore, che è stato approvato a dicembre 2015, pubblicato in Gazzetta Ufficiale dell'Unione Europea n. 119 del 4 maggio 2016 ed ufficialmente entrato in vigore il 25 maggio 2016.
Il Regolamento 2016/679/UE sulla protezione dei dati personali, noto con l'acronimo GDPR (General Data Protection Regulation), dispiegherà la propria completa efficacia a partire dal prossimo 25 maggio 2018 (due anni dopo la sua entrata in vigore) quando dovrà essere garantito l'allineamento fra la normativa nazionale in materia di protezione dati e le disposizioni del Regolamento.
Nel prossimo futuro si dovranno pertanto prevedere nuovi adeguamenti, che andranno ad integrare quello che è attualmente in essere.

Ad oggi gli adempimenti in vigore sono dettati dal Decreto legislativo 30 giugno 2003, n. 196, che impone degli obblighi di sicurezza (art. 31) e delle misure minime (art. 33 e segg.), mentre il "Decreto Sviluppo" (decreto legge n. 5 del 2012 "Disposizioni urgenti in materia di semplificazione e di sviluppo"), in materia di trattamento dei dati, ha stabilito che non è più obbligatorio, entro il 31 marzo di ogni anno, per il titolare redigere il Documento Programmatico sulla Sicurezza (DPS) contenente idonee informazioni riguardo l'elenco dei trattamenti di dati personali.

È da aggiungere poi che la Direttiva 1/8/2015 del Presidente del Consiglio dei Ministri assegna all'Agid il compito di sviluppare gli standard di riferimento per le PA e che, in attuazione di questo, la Circolare n. 2/2017, pubblicata in Gazzetta Ufficiale n. 103 del 5/5/2017 contiene le linee guida per consentire alle PA di valutare e migliorare il proprio livello di sicurezza informatica.
Tale documento, dal titolo 'Misure minime per la sicurezza ICT per le Pubbliche Amministrazioni', si articola sull'attuazione di controlli di natura tecnologica, organizzativa e procedurale.

1.2 Contenuti del piano

Gli attacchi ai sistemi informatici rappresentano sempre di più un elemento di grande criticità non solo per le aziende private, ma anche per le Pubbliche Amministrazioni.

Il raggiungimento di elevati livelli di sicurezza, quando è molto elevata la complessità della struttura e l'eterogeneità dei servizi erogati, può essere eccessivamente oneroso se applicato in modo generalizzato. Pertanto ogni Amministrazione dovrà avere cura di individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, caratterizzati da omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure adatte al valore del bene intangibile da proteggere (informazione) ed al rischio sostenibile, senza ridurre la possibilità di fruizione dello stesso.
Nei fatti le misure preventive, destinate ad impedire il successo di eventuali attacchi, devono essere affiancate da efficaci strumenti di rilevazione in grado di abbreviare i tempi, oggi pericolosamente lunghi, che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte.

Il presente documento "Piano della sicurezza" prevede l'indicazione delle misure di sicurezza adottate sull'infrastruttura gestita dal Settore Informatico Associato (SIA) dell'Unione Terre di Pianura, a cui tutti i Comuni afferiscono, tramite apposita convenzione sulla gestione delle funzioni informatiche.
Sarà nel seguito effettuata una analisi del rischio, con l'obiettivo di identificare le minacce alle risorse critiche del sistema, trovare misure per contrastarle, e allo stesso tempo valutare le perdite derivanti dal verificarsi di tali minacce e potere eventualmente giustificare i costi da sostenere per la gestione della sicurezza.

Il controllo dei rischi deve operare attraverso misure:

- organizzative (regole per l'accesso, contenuti abilitazioni/incarichi, linee guida per la sicurezza, formazione, monitoraggio dei dati);
- logiche (identificazione/autenticazione utente, controllo degli accessi e politiche antivirus, firma digitale, monitoraggio sessioni di lavoro)
- fisiche (vigilanza sedi e locali, dispositivi di allarme, continuità elettrica, verifiche leggibilità supporti).

2. L'infrastruttura centralizzata

2.1 La componente server

Fino al 2012 il Datacenter dell'Unione era fisicamente contenuto in locali appositamente adibiti all'interno di uno degli Enti che ne facevano parte.
Dal 2012 al giugno 2015, consci dei rischi e delle misure da mettere in atto per la sicurezza dei suddetti locali, le macchine fisiche di proprietà dell'ente, sono state spostate in housing presso l'infrastruttura Datacenter di Telecom.
Nel giugno 2015 quelle macchine vengono dismesse, e si stipula un contratto con Lepida S.p.A. a favore di un servizio di hosting completo, su infrastruttura condivisa, completamente gestita dalla società in house.
A gennaio 2017 si modifica il contratto con Lepida S.p.A., favorendo una soluzione dedicata, tramite l'acquisizione di lame blade, fisicamente collocate nel Datacenter Lepida di Ravenna, su cui è possibile gestire in autonomia tutte le macchine virtuali.
Sui singoli Comuni è presente un solo server fisico cosiddetto "dipartimentale", che ha il solo scopo di distribuire, tramite servizio DHCP, gli indirizzi IP dei sigoli client, nonché fungere da proxy per il controllo della navigazione internet.

2.2 L'accesso ai sistemi

Il sistema di autenticazione utilizzato in tutti gli Enti afferenti all'Unione per accedere alla rete, è Microsoft Windows Active Directory, in cui ciascun utente è definito una volta sola (esiste un solo Domain controller).
Tale sistema viene utilizzato per autenticare gli utenti attribuendo loro delle risorse condivise sulla rete: cartelle di file system, applicativi software, stampanti.
Anche per l'accesso ai Personal Computer ci si avvale esclusivamente della stessa credenziale di Active Directory.
I criteri per l'accesso al sistema di gestione informatica del protocollo, come a quello di ogni altro software applicativo, insieme alle indicazioni sulla corretta gestione delle credenziali, sono indicati nel documento "Disciplinare di utilizzo degli strumenti informatici" (D.G. Unione n. 35/2017).

Il fornitore della procedura applicativa del protocollo informatico è ADS per tutti gli enti afferenti all'Unione e l'Unione stessa, tranne per il Comune di Malalbergo, in cui è presente il fornitore Datagraph.
La procedura applicativa ADS è attualmente integrata con Active Directory di Windows e quindi le credenziali di accesso sono le stesse dell'accesso alla rete e al PC. Quella di Malalbergo è predisposta per tale integrazione, ma ad oggi non attivata.
Per entrambi le procedure applicative, è necessaria la profilazione di ogni utente con l'indicazione dei suoi diritti.

2.3 La componente applicativa

Tutti i software applicativi, incluso il protocollo informatico, sono centralizzati e distribuiti via Citrix a tutti gli utenti.

Il processo di omogeneizzazione dei software verticali è in corso.
Si tratta di una attività iniziata nel 2002, in occasione di bandi che consentivano di ottenere finanziamenti Regionali, in caso di avvio del processo. Da allora sono state fatte diverse operazioni in tal senso, ma si è assistito anche a diversi mutamenti della geometria del territorio dell'Unione.
La maggior parte delle applicazioni di back office degli Enti sono ad oggi omogenee tra i 4 Comuni "storici", ovvero tutti utilizzano i medesimi applicativi: questa operazione ha consentito di avere maggior forza contrattuale con i fornitori, nonché di avere un migliore controllo su installazioni e aggiornamenti.
Nella maggioranza dei casi, sono comunque presenti istanze diverse per ogni Ente, non sono ancora presenti installazioni multi-ente.

3. Analisi dei rischi

In linea con l'art. 35, Capo I, Titolo V del d.lgs. n. 196/2003 che "*impone di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta"* si procede analizzando i rischi a cui sono soggetti i dati informatici ed i dati cartacei trattati dagli incaricati dell'ente.

I rischi ai quali possono essere soggetti i dati residenti sui sistemi presenti nell'ente, sono i seguenti:

A) **Accesso indebito alle risorse** (in ottemperanza al d.lgs. n. 196/2003, dati, programmi e strumenti di comunicazione devono essere protetti da accessi non autorizzati, quindi da azioni particolari come modifica o copia di informazioni, messaggi, file,

programmi, uso non autorizzato dei privilegi di sistema, dirottamento o duplicazione di informazioni o programmi da parte di persone non autorizzate).

B) **Comportamenti non corretti degli operatori** (possono essere comportamenti dolosi, ma anche mancanza di consapevolezza e formazione sull'uso dei sistemi).

C) **Eventi relativi agli strumenti** (cosiddetto "fault" del servizio, ovvero situazioni in cui un servizio più o meno critico, più o meno importante, smette di funzionare in seguito ad un guasto o ad altro evento, piuttosto che attacchi di virus e malware, spamming, malfunzionamenti vari).

D) **Eventi relativi al contesto** (guasti ai sistemi infrastrutturali di base (es. impianti elettrici, impianti condizionamento, …)).

E) **Rischi connessi alla trasmissione dei dati** (il rischio è il furto dei dati al momento della trasmissione da e per gli enti dell'Unione, i tentativi di intrusione nella rete sono sempre più frequenti da parte di pirati esterni).

F) **Perdita dell'integrità fisica dei dati** (il rischio è l'eliminazione del dato per errore).

G) **Perdita dell'integrità logica dei dati** (i rischi sono legati ad errori operativi, che generano incongruenze nei dati, che le applicazioni non sono in grado di gestire; le operazioni critiche devono essere attivabili solo da personale autorizzato e devono essere previsti strumenti per ripristinare lo stato corretto del sistema nel caso vengano rilevati errori operativi).

H) **Manomissioni o furti** (il rischio è legato alle postazioni client: furti di dati al loro interno e furto dello stesso hardware).

I) **Eventi dannosi o disastrosi** (il sistema informativo deve prevedere contromisure per tutela da eventi dannosi o disastrosi, come incendi, terremoti, …).

In considerazione di quanto elencato, si ricorda che il sistema deve dare garanzia di:

- autenticità dei dati, ovvero deve essere disponibile un meccanismo per associare ad una unità di registrazione l'identificativo dell'utente che l'ha generata nella forma in cui essa è memorizzata, con una prova incontestabile;
- integrità del dato, che si esplicita in integrità logica (*coerenza e consistenza*) e fisica (*esistenza di copie o di salvataggi*).

4. Misure di sicurezza

Si riprendono nel seguito i rischi elencati sopra, esplicitati nel dettaglio, con le relative misure adottate.

RISCHIO	DETTAGLIO	MISURA
A) Accesso indebito alle risorse	• Accesso alle banche dati non autorizzato	• Ogni utente ha un codice identificativo ed una password che lo abilitano ad entrare nel sistema di rete, limitatamente ai dati e agli applicativi necessari per lo svolgimento delle proprie mansioni.
B) Comporta-menti non corretti degli operatori	• Mancanza di consapevolezza sull'uso dei sistemi	• Realizzazione del documento "Disciplinare di utilizzo degli strumenti informatici" (D.G. Unione n. 35/2017), divulgato presso gli utenti di tutti gli enti afferenti all'Unione.
	• Comportamenti dolosi	• Controlli periodici sull'operato, controllo degli accessi (sia a campione, sia su richiesta di responsabili). • Content filtering tramite server proxy.

RISCHIO	DETTAGLIO	MISURA
C) Eventi relativi agli strumenti	• "Fault" del servizio	• Essendo il Datacenter interamente presso Lepida SpA, gli eventi a cui è necessario fare fronte sono la sostituzione degli apparati di rete (switch e router), in caso di rottura o obsolescenza.
	• Attacchi di virus e malware	• Aggiornamento periodico dei sistemi antivirus sui server e sui PC client.
D) Eventi relativi al contesto	• Guasti ai sistemi infrastrutturali di base	• Essendo l'intera infrastruttura su Datacenter presso Lepida SpA, le attenzioni sono poste sul corretto funzionamento degli armadi di rete e del PAL, nonché dei server dipartimentali.
E) Rischi connessi alla trasmissione dei dati	• Accesso degli utenti interni alla rete pubblica	• L'accesso dall'interno alla rete esterna è regolato da un proxy con conservazione delle attività fatte (log).
	• Accessi indebiti alla rete interna dall'esterno	• Il sistema firewall si preoccupa di proteggere la rete locale da "attacchi" esterni.
	• Necessità di attivare collegamenti via VPN	• Nonostante la tendenza è di minimizzare questo tipo di accessi, con alcuni fornitori è necessario procedere in questo modo per semplificare le attività di intervento.
F) Perdita dell'integrità fisica dei dati	• Eliminazione per errore di un dato presente su sistemi gestiti internamente	• Esiste un sistema di back-up dei server separato per ciascun server e differenziato a seconda della tipologia dei server stessi. I server applicativi sono soggetti a back-up settimanale full e conservati per i 15 giorni precedenti. I dati contenuti sui server dei file system sono soggetti a back-up quotidiano incrementale e conservati per i 30 giorni precedenti. I dati cancellati sono ripristinabili fino ai sei mesi precedenti. Periodicamente viene eseguita la prova di restore parziale dei dati. Il backup viene effettuato presso il Datacenter Lepida Spa.
	• Eliminazione per errore di un dato presente su sistemi non gestiti internamente	• Attualmente i sistemi gestiti in cloud da fornitori esterni sono: la posta elettronica "Zimbra" per tutti gli Enti afferenti all'Unione e l'Unione stessa, il sistema di segnalazione "Comunichiamo" per i tutti i Comuni, il sistema gestionale dei servizi scolastici per i Comuni di Budrio (fornitore PADigitale) e Baricella-Minerbio (fornitore Project). Per questi, i rispettivi contratti assicurano il mantenimento del dato nel rispetto della Privacy.
	• Eliminazione dati	• Sono presenti sistemi antivirus sui server e sui

RISCHIO	DETTAGLIO	MISURA
	causati da virus	PC client.
G) Perdita dell'integrità logica dei dati	• Errori operativi, che generano incongruenze nei dati	• La presenza di applicazioni verticali ad hoc sui singoli settori, preclude tale rischio.
H) Manomissioni o furti	• Furti di dati contenuti nei PC client e furto dello stesso hardware	• Essendo l'intera infrastruttura su Datacenter presso Lepida SpA, le attenzioni sono poste sui client, in particolare sul furto dell'hardware; per questo si rimanda alla sicurezza di accesso ai locali comunali. • Come da "Disciplinare di uso degli strumenti informatici" (D.G. Unione n.35/2017), la raccomandazione è che non venga memorizzato nulla sui PC locali; se tale disposizione è rispettata, non vi è alcun rischio di furto di dati.
I) Eventi dannosi o disastrosi	• Rischio di perdita dati	• Non è presente un sistema di disaster recovery.