POL01

Politica per la sicurezza delle informazioni

INDICE

1 Scopo ed obiettivi 3
2 Campo di applicazione 3
3 Contestualizzazione 4
3.1 Sensibilizzazione 5
3.2 Uso delle strumentazioni informatiche 5
3.3 Segnalazione delle violazioni 6
3.4 Controlli di sicurezza 6
3.4.1 Controllo degli accessi fisici 6
3.4.2 Controllo degli accessi logici 6
3.4.3 Gestione degli asset 7
3.4.4 Risposta agli incidenti di sicurezza 7
3.5 Il Community cloud regionale 7
4 Ruoli e responsabilità 7

1 Scopo ed obiettivi

La Giunta Regionale e l'Assemblea Legislativa della Regione Emilia-Romagna (di seguito Ente) considerano le informazioni gestite nell'ambito della loro attività istituzionale parte integrante del proprio patrimonio istituzionale.

La tutela del patrimonio delle informazioni riveste importanza strategica per l'Ente, oltre che essere soggetta a precisi vincoli normativi.

La sicurezza delle informazioni è definita come la salvaguardia di riservatezza, integrità e disponibilità delle stesse.

In particolare:

1. tutelare la *riservatezza* significa assicurare che le informazioni siano accessibili solo a coloro che sono autorizzati ad avervi accesso;

2. tutelare l'*integrità* significa salvaguardare l'accuratezza e la completezza delle informazioni e del loro trattamento;

3. tutelare la *disponibilità* significa assicurare che gli utenti autorizzati abbiano accesso, quando richiesto, alle informazioni e agli strumenti ad esse associati.

Per questi motivi:

- la Giunta Regionale adotta un Sistema di Gestione per la Sicurezza Informatica (SGSI) secondo gli standard internazionali ISO/IEC 27001:2013, ISO/IEC 27017:2015 e ISO/IEC 27018:2019;
- l'Assemblea Legislativa ha certificato i suoi processi inerenti la tutela della privacy e la sicurezza informatica secondo gli standard internazionali ISO 9001:2015 e ha definito criteri per la sicurezza in modo congiunto e coordinato con la Giunta regionale in quanto facenti parte dello stesso sistema informativo.

2 Campo di applicazione

La politica di sicurezza delle informazioni si applica all'Ente nell'ambito di tutte le sue funzioni

istituzionali. In particolare, si applica alla gestione della sicurezza dei dati e delle informazioni nelle attività svolte dal Servizio ICT Regionale della Giunta e dal Servizio Funzionamento e Gestione dell'Assemblea Legislativa.

La politica si applica a tutte le informazioni trattate nell'ambito sopra definito, qualsiasi natura e forma esse abbiano o prendano, e a tutti i sistemi di gestione e supporti di memorizzazione utilizzati per il loro trattamento e conservazione.

I destinatari della politica sono tutti i collaboratori dell'Ente, dipendenti o non dipendenti. Sono tenuti al rispetto della politica tutti i soggetti che a vario titolo fruiscono dei servizi informativi dell'Ente, nonché i visitatori e gli ospiti. In particolare, sono tenuti al rispetto della politica di sicurezza, i fornitori di servizi informatici che operano direttamente sui sistemi di gestione delle informazioni.

3 Contestualizzazione

L'applicazione ed il mantenimento della sicurezza si attuano attraverso misure tecniche e misure organizzative che devono essere recepite dai processi di lavoro per diventarne parte integrante.

Prerequisito della politica di sicurezza delle informazioni è il rispetto delle misure di sicurezza minime ed idonee definite dalla normativa applicabile all'ambito della Giunta Regionale e dell'Assemblea Legislativa

La costruzione di un adeguato processo di gestione della sicurezza comprende le seguenti fasi distinte:

1. *pianificazione della sicurezza*: definizione degli obiettivi di sicurezza, analisi dei rischi, individuazione delle misure di sicurezza;

2. *implementazione delle misure di sicurezza*: messa in opera delle misure di sicurezza individuate;

3. *controlli*: verifica dell'efficienza e della corretta applicazione delle misure di sicurezza adottate;

4. *revisioni*: attuazione di correzioni ed adeguamenti al sistema di protezione delle informazioni sulla base dei risultati ottenuti dai controlli applicati e dagli aggiornamenti normativi e tecnologici.

La scelta delle misure da rendere esecutive è quindi effettuata a seguito di un'analisi costi/benefici (analisi dei rischi) e tale analisi è costantemente ripetuta nel tempo alla luce dei progressi tecnologici, dei mutamenti normativi e del riscontro ottenuto dai controlli sulle misure già adottate.

3.1 Sensibilizzazione

La sicurezza di un sistema è costituita da tecnologie, procedure e comportamenti di tutti gli utenti del sistema stesso. Ciò rende fondamentale la sensibilizzazione di tutti coloro che effettuano trattamenti di dati personali e di informazioni ritenute riservate circa i rischi incombenti sui dati e circa il corretto utilizzo dei relativi strumenti di protezione disponibili.

I sistemi e le reti d'informazione sono sottoposti a rischi interni ed esterni, è quindi necessario porre in essere azioni di sensibilizzazione finalizzate a creare nei destinatari della presente politica la consapevolezza che, a causa dell'interconnessione e dell'interdipendenza tra sistemi, le falle in materia di sicurezza su un componente del sistema possono propagare i loro effetti fino ad incidere gravemente sull'integrità dei sistemi, delle reti, delle banche dati, degli archivi e arrecare danni ad altri.

Comportamenti non partecipi, disinformati o indifferenti, possono ostacolare gravemente la tutela del patrimonio informativo e ledere il rapporto di fiducia che deve necessariamente intercorrere tra l'Amministrazione regionale e la società civile.

3.2 Uso delle strumentazioni informatiche

Le strumentazioni informatiche che l'Ente mette a disposizione devono essere utilizzate in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.

Con specifico riferimento agli strumenti informatici e telematici, alla posta elettronica e a Internet, i destinatari della presente politica sono tenuti in particolare a:

1. utilizzare tali beni per motivi non attinenti all'attività lavorativa soltanto in casi di urgenza e

comunque non in modo ripetuto o per periodi di tempo prolungati e mai in violazione delle politiche di sicurezza stabilite dall'Ente;

2. utilizzare la posta elettronica e Internet nel rispetto del principio di riservatezza, per le specifiche finalità della propria attività istituzionale e rispettando le esigenze di funzionalità della rete e quelle di semplificazione dei processi lavorativi.

3.3 Segnalazione delle violazioni

Le violazioni di sicurezza interna o gli eventi che possono portare a credere che vi sia stata un'elusione delle misure di sicurezza previste, devono essere tempestivamente segnalate secondo le modalità e le regole tecniche definite da uno o più documenti specifici.

3.4 Controlli di sicurezza

L'Ente effettua i controlli ritenuti opportuni per la verifica della corretta applicazione e dell'efficienza delle misure di sicurezza adottate per la protezione dei dati personali.

Tali controlli, di seguito indicati a titolo esemplificativo, sono effettuati esclusivamente da personale debitamente autorizzato.

3.4.1 Controllo degli accessi fisici

L'accesso e la permanenza all'interno delle sedi dell'Ente sono consentiti esclusivamente alle persone autorizzate.

Le aree dove sono situati i sistemi e le apparecchiature di elaborazione dei dati sono dotate di un ulteriore meccanismo di controllo accessi basato su badge e di sistemi di videosorveglianza.

3.4.2 Controllo degli accessi logici

L'accesso ai dati e alle informazioni trattati con strumentazioni informatiche avviene esclusivamente previa autenticazione, ossia tramite una procedura che verifica anche indirettamente l'identità di chi vi accede.

Ogni utente deve custodire le proprie credenziali di accesso ai sistemi, adottando le necessarie cautele per assicurare la segretezza della componente riservata e la diligente custodia dei dispositivi in proprio possesso ed uso esclusivo.

Ogni utente deve poter accedere solo all'insieme minimo di risorse necessarie allo svolgimento del proprio lavoro.

3.4.3 Gestione degli asset

Deve esistere un catalogo costantemente aggiornato degli asset rilevanti ai fini della gestione della sicurezza delle informazioni e per ciascuno deve essere individuato un responsabile.

3.4.4 Risposta agli incidenti di sicurezza

Gli utenti del sistema informativo dell'Ente devono operare tempestivamente e in uno spirito di collaborazione per prevenire, rilevare e rispondere efficacemente agli incidenti di sicurezza nel minor tempo possibile anche al fine di ridurre gli impatti conseguenti alla rapidità della diffusione conseguente all'interconnessione dei sistemi e delle reti d'informazione.

3.5 Il Community cloud regionale

La Giunta ha dato attuazione al Community Cloud Regionale e definisce con specifici atti il modello di cloud afferente al contesto regionale, la tipologia e la modalità di erogazione dei servizi da parte della Giunta per mezzo del Servizio ICT Regionale.

4 Ruoli e responsabilità

Con specifico provvedimento (DGR. n. 1123/2018 per la Giunta, DUP n. 107/2018) sono state definite le competenze e le responsabilità in materia di protezione dei dati personali, ripartendo compiti e funzioni tra i soggetti competenti tenuto conto della specifica organizzazione dell'Amministrazione.

Al Servizio ICT Regionale per la Giunta e al Servizio Funzionamento e Gestione per l'Assemblea sono assegnate le funzioni di gestione della sicurezza delle informazioni, ivi compresa l'individuazione delle misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente. Tutte le azioni e le iniziative adottate da questi che contemplino dati personali devono essere coordinate con il Responsabile della protezione dei dati in aderenza al modello organizzativo adottato dall'Ente per l'attuazione degli oneri derivanti dalla normativa in

materia di protezione dei dati personali.

Le strutture che gestiscono, sviluppano, progettano e forniscono prodotti e servizi nell'ambito dei sistemi informativi, devono agire in modo da garantire la sicurezza dei sistemi e delle reti, tutelare la riservatezza dei dati personali e diffondere informazioni utili per assicurare l'adozione di idonee pratiche di sicurezza.

Tutti gli utenti devono adoperarsi per elaborare e adottare pratiche esemplari e incoraggiare comportamenti che tengano conto degli imperativi di sicurezza e di tutela dei diritti altrui.

La violazione delle policy discendenti dai principi definiti nella presente politica, ferme restando eventuali responsabilità penali, civili o amministrativo-contabili, è rilevante sotto il profilo disciplinare e di responsabilità dirigenziale.