Politiche per la sicurezza delle informazioni

In PagoPA consideriamo una priorità assoluta la sicurezza dei nostri progetti e delle informazioni che trattiamo, in particolare i dati dei cittadini.

L'approccio che adottiamo per garantire livelli di sicurezza e protezione sempre crescenti si fonda sull'adozione di best practices riconosciute e certificabili.
PagoPA, infatti, **ha definito il proprio Sistema di Gestione della Sicurezza delle Informazioni** (di seguito anche "SGSI") **basandosi sul framework internazionale della ISO/IEC 27001**, ottenendo alla fine del 2020 la certificazione dello stesso.
Il nostro SGSI implementa prassi e regole di sicurezza come di seguito sintetizzato.

POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI

Nell'ambito della governance del proprio Sistema di Gestione della Sicurezza delle Informazioni **PagoPA ha definito una Information Security Policy**, diffusa a tutto il personale, **al fine di proteggere dalle minacce le informazioni che costituiscono il patrimonio informativo** di PagoPA, nonché i dati dei cittadini che sono gestiti nel ciclo di vita dei prodotti e servizi forniti.

Lo scopo della Information Security Policy è quello di definire:

- gli obiettivi generali di sicurezza, in linea con le strategie di business;
- i principi di azione per una adeguata postura di sicurezza.

In linea con la Information Security Policy, PagoPA si è dotata di norme e procedure mirate a mantenere nel tempo un costante ed elevato livello di sicurezza del proprio sistema informativo.

ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

La gestione della sicurezza delle informazioni comprende processi e misure volti a:

- preservare la sicurezza delle informazioni e dei beni aziendali;
- garantire che le risorse aziendali siano protette in termini di riservatezza, integrità e disponibilità in maniera appropriata e coerente lungo il loro intero ciclo di vita.

Inoltre, l'organizzazione della sicurezza di PagoPA prevede la figura di **Responsabile della sicurezza delle informazioni** (o "CISO") che, in coordinamento con la Direzione Aziendale, definisce la strategia della sicurezza, la cui attuazione è assegnata ai manager di area.

Il CISO è supportato da un team con competenze relative a:

- Architecture & Product Security;

- Security Governance;
- Security Operations.

In ottemperanza agli obblighi normativi relativi al trattamento dei dati personali, **inoltre**, **PagoPA si è avvalsa altresì della figura del Data Protection Officer** (o "DPO").

SICUREZZA DELLE RISORSE UMANE

Al fine di assicurare che il personale e i collaboratori comprendano le proprie responsabilità e seguano i principi di sicurezza richiesti per i ruoli assegnati, è prevista la definizione e condivisione di policy, procedure istruzioni e linee guida, organizzative e tecniche, per diffondere la cultura e la consapevolezza sulle tematiche di Information security e compliance.

GESTIONE DEGLI ASSET

Nell'ambito dell'identificazione degli asset dell'organizzazione e della definizione di adeguate responsabilità per la loro protezione, ricadono non solo gli elementi fisici, ma anche i dati e le informazioni che fanno anch'essi parte a pieno titolo del patrimonio aziendale.

Tutte le categorie di asset sono inventariate, **identificabili ed aggiornate nel tempo**.
Il responsabile di ciascun asset assicura che lo stesso sia inventariato, appropriatamente classificato e protetto, definisce e riesamina periodicamente i privilegi di accesso e la classificazione, in particolare per gli asset più critici e, coerentemente con le linee guida stabilite per regolare le modalità di gestione e uso sicuro degli asset, assicura un corretto trattamento, la dismissione, la segnalazione e gestione nel caso di compromissione degli stessi.

CONTROLLO DEGLI ACCESSI

All'interno delle linee guida di security sono delineati i requisiti per la gestione e il controllo degli accessi, secondo i principi di:

- necessità (need to know/need to do);
- limitazione dei privilegi (least privilege)
- separazione dei ruoli (SoD, Segregation of Duties).

Le linee guida di sicurezza prevedono che siano definiti e verificati (almeno una volta l'anno da parte del referente dei singoli sistemi) i ruoli sui sistemi, i privilegi associati ai ruoli e le regole per l'assegnazione dei ruoli ai singoli utenti (cosa è autorizzato di default e quali sono / come si gestiscono eventuali eccezioni) in maniera tale che sia sempre possibile risalire a "chi può fare cosa, dove".
I singoli team hanno la responsabilità di applicare, in funzione dei rischi connessi, le regole di utilizzo e i sotto-processi per l'attribuzione, revisione e revoca dei diritti di accesso ai sistemi e alle applicazioni, nel rispetto dei suddetti principi.

L’accesso a sistemi e applicazioni avviene tramite credenziali che consentano di identificare e autenticare in maniera univoca gli specifici utenti.

Per tutti i sistemi critici è implementata l’autenticazione a 2 fattori.

CRITTOGRAFIA

Sono implementate misure per la protezione dei dati:

- ‘**in transito**’ (cifratura del canale, nel momento in cui si stabilisce la connessione, o del dato);
- ‘**a riposo**’ (cifratura di tutte le componenti per la conservazione / archiviazione dei dati).

L’approccio adottato tiene in considerazione la criticità dei dati, le minacce a cui sono esposti, gli obblighi normativi, la presenza di elementi a mitigazione dei rischi e gli impatti su performances e disponibilità dei servizi.

I servizi web Internet, al fine di garantire la riservatezza delle informazioni scambiate e permettere la verifica dell’attendibilità del sito (ad esempio in caso di phishing), **sono esposti utilizzando un certificato SSL** rilasciato da una Autorità di certificazione ufficialmente riconosciuta.

Anche **la sicurezza dei sistemi di posta elettronica è garantita tramite l’uso di protocolli per tutelare l’azienda** da utilizzo improprio (limitando tentativi di impersonificazione/spoofing del dominio, spam, phishing) e garantendo il corretto recapito dei messaggi.

SICUREZZA FISICA E AMBIENTALE

Sono definite:

- **istruzioni per il personale sulle misure** fisiche presenti e su comportamenti/pratiche da adottare per non diminuirne l'efficacia;
- **regole e vincoli per l'utilizzo di attrezzature all'interno e all'esterno delle aree di lavoro**, indicazione delle misure previste a protezione delle informazioni contenute e trattate tramite le stesse, dei comportamenti da adottare in pubblico, dei canali di comunicazione da utilizzare e delle pratiche da seguire in caso di furto o sospetta compromissione dell'apparecchiatura.

In linea con la Information Security Policy e con le relative linee guida di sicurezza è previsto che:

- ai dipendenti sia assegnato un badge con livelli di autorizzazione sufficienti a garantire accesso alle aree previste per il ruolo assegnato;
- l'accesso alle aree più critiche sia limitato e controllato;

- il personale esterno a cui sia concesso l'accesso venga registrato all'entrata e all'uscita, accompagnato da personale dipendente durante la permanenza nei locali, istruito sulle regole di sicurezza presenti e sulle sanzioni in caso di mancato rispetto delle stesse.

Altre misure per la protezione fisica e ambientale prevedono:

- sistemi di allarme antintrusione;
- prevenzione incendi;
- videosorveglianza.

SICUREZZA DELLE ATTIVITÀ OPERATIVE

Sono definite ed implementate linee guida e misure di sicurezza a supporto delle attività e dei processi operativi (corretto e sicuro funzionamento dei sistemi, gestione dei dati; mitigazione dei rischi legati ad errori umani, furto, frode o uso improprio di dati e sistemi). Tra le misure di protezione e mitigazione, inoltre, vi sono:

- **log management**: registrazione degli eventi di sicurezza, delle attività degli utenti in file di log che consentano di risalire ad attività anomale, root cause di eventuali problemi, ecc.;
- **separazione degli ambienti**: gli ambienti di sviluppo e collaudo sono logicamente separati da quello di produzione;
- **controlli di rete**: monitoraggio delle intrusioni e verifica degli eventi registrati dai sistemi di sicurezza a protezione della rete;
- **patch management**: acquisizione, test ed installazione di modifiche al codice (patches) per mantenere a livelli congrui la resilienza del sistema informatico, in particolar modo riguardo alla sicurezza;
- **backup e restore**: definite, testate ed adottate procedure per il salvataggio dei dati e delle configurazioni e per il relativo ripristino in caso di necessità;
- **penetration test e vulnerability assessment**: attività effettuata almeno annualmente tramite società esterne su infrastruttura e sw;
- **monitoraggio sistemi**: controllo su disponibilità, raggiungibilità, health check di sistemi e applicazioni prevedendo gli opportuni processi di escalation a fronte di anomalie per garantire interventi rapidi e qualità del servizio;
- **capacity planning**: garantito tramite opportune valutazioni che derivano dalla costante analisi (monitoraggio di capacità, volumi, utilizzo, performance, ecc; rilevazione di eventuali failure, colli di bottiglia e altre possibili anomalie) delle risorse impiegate (rete, sistemi, ecc.) rispetto ai vari obiettivi, inclusi quelli per la sicurezza;

- **antivirus**: ogni personal computer assegnato ai dipendenti è dotato di un software antivirus, attivo, costantemente aggiornato e monitorabile centralmente, a protezione della navigazione internet e della posta elettronica.

SICUREZZA DELLE COMUNICAZIONI

Le reti di trasmissione dati sono configurate prevedendo opportuna separazione in base ai servizi offerti. L'accesso ai sistemi all'interno della rete richiede un account di rete unico e univocamente associato all'utente. Non è consentito l'accesso anonimo alla rete.

- **Sono previste misure tecnico/organizzative volte a impedire l'interconnessione di reti esterne non autorizzate** alla rete aziendale e controlli per impedire l'accesso non autorizzato in entrata/uscita.
- **Sono adottate misure per la protezione contro gli attacchi basati sulla rete** (denial of service, intercettazioni, impersonificazione) e ulteriori controlli di network based intrusion detection / prevention.
- **Anche i tentativi** (riusciti/non riusciti) **di stabilire una connessione di rete sono loggati e tenuti sotto monitoraggio**.

ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI

Sono definite **linee guida e relativi approcci** per migliorare l'efficacia della sicurezza **lungo il ciclo di vita di sviluppo del software** (Software Development Life Cycle - SDLC) e, più in generale, nel più ampio processo di Gestione del Cambiamento:

- identificazione e gestione dei requisiti di sicurezza e di conformità alla normativa (in particolare per la **protezione della privacy dei cittadini**) già nelle fasi iniziali di sviluppo;
- definizione, in fase di progettazione, di opportuni threat model (identificazione, enumerazione e prioritizzazione delle potenziali minacce), per individuare adeguate **misure per il rispetto dei requisiti** e la mitigazione dei rischi, soprattutto per i cambiamenti più critici;
- **analisi statica del codice e soluzione delle vulnerabilità**, pianificata sulla base dei livelli di criticità rilevati.
- **Qualsiasi modifica**, prima di essere promossa in produzione, **deve essere opportunamente testata ed approvata**.
- Quando l'intero sviluppo, o singole fasi di sviluppo di sistemi/servizi sono assegnate a terze parti o in caso di acquisizione di strumenti / sistemi OTS, **la sicurezza delle informazioni e l'adozione dei relativi requisiti è regolata tramite opportune clausole contrattuali di sicurezza**; i fornitori sono quindi valutati nel

tempo rispetto alla capacità di rispondenza ai requisiti ed al rispetto delle regole definite.

Per i trattamenti più critici, in ottemperanza con gli obblighi relativi alla protezione dei dati personali, sono condotte attività preliminari di valutazione dei possibili impatti sui cittadini interessati a cui si riferiscono i dati trattati (DPIA).

GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI

Sono definite linee guida e viene dato supporto per **assicurare un approccio coerente ed efficace** per la gestione degli incidenti relativi alla sicurezza delle informazioni, incluse le indicazioni per efficaci comunicazioni interne e verso l'esterno (ad esempio in caso di Notifica alle Autorità di eventuali violazioni dei dati personali in ottemperanza agli obblighi previsti in tal senso dal **GDPR**), la registrazione di ogni incidente e il reporting. L'esperienza ricavata da ogni accadimento viene acquisita e documentata ai fini del miglioramento del processo stesso.

ASPETTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI NELLA GESTIONE DELLA CONTINUITÀ OPERATIVA

Sono identificate ed indirizzate, nei confronti delle terze parti eventualmente impiegate in una o più fasi della catena di erogazione dei servizi, i livelli minimi di funzionamento e i normali regimi di operatività, fissando gli obiettivi di recupero della stessa (recovery time objectives (RTO) e recovery point objectives (RPO)).

È richiesto che per i sistemi, i database, le infrastrutture e ogni altra iniziativa a copertura della continuità aziendale, sia nel day-by-day che durante un evento avverso, il livello di sicurezza sia mantenuto allineato con la produzione e i processi nella cosiddetta "normal operation".

La continuità della sicurezza delle informazioni è garantita anche attraverso le attività necessarie sulle 'basi dati' per assicurare la continuità del servizio.