Politica per la Sicurezza delle Informazioni

La Direzione di ***01Sistemi***, riconoscendo l'importanza strategica degli asset organizzativi, siano essi di natura materiale (risorse umane, dispositivi informatici e infrastrutture) o immateriale (patrimonio delle informazioni), ha deciso di tutelare la salvaguardia delle informazioni trattate in tutte le fasi dei processi aziendali considerando l'*Information Security* uno strumento che permette la condivisione sicura delle informazioni, il miglioramento delle prestazioni rese ai Clienti e della propria immagine.

OBIETTIVI PERSEGUITI

01Sistemi persegue il Miglioramento continuo della Tutela dei dati personali mediante:

- L'adozione di un adeguato sistema documentale integrato nel sistema dell'organizzazione (linee guida, procedure, istruzioni operative, modelli documentali standard);
- La definizione di specifici indicatori per la misura di obiettivi e traguardi raggiungibili;
- L'identificazione degli aspetti connessi ai rischi derivanti dal trattamento di sicurezza delle informazioni già in fase di definizione/progettazione/revisione dei processi aziendali;
- L'identificazione di delegati dotati di adeguati requisiti e poteri per garantire il corretto funzionamento del sistema di gestione per la sicurezza delle informazioni;
- La definizione di un modello organizzativo adeguato al presidio del trattamento di sicurezza delle informazioni inerenti ad ogni processo aziendale;
- L'adozione di pareri di conformità normativa nell'integrazione, modifica e/o revisione di processi aziendali che prevedano un trattamento di sicurezza delle informazioni;
- L'adozione di misure di sicurezza idonee a prevenire e ridurre al minimo i rischi inerenti il trattamento di sicurezza delle informazioni;
- L'adozione delle migliori tecniche disponibili ed economicamente sostenibili per limitare i danni in caso di incidenti o eventi negativi in materia di trattamento di sicurezza delle informazioni;
- L'adozione di opportuni criteri e modalità di ripristino delle informazioni in caso di danneggiamento e perdita accidentale;
- Coinvolgimento degli stakeholder e protezione delle informazioni con azioni mirate a:

- Sensibilizzare dipendenti, fornitori, clienti, azionisti e cittadini su obiettivi, traguardi e impegni assunti in materia di protezione delle informazioni;
- Motivare e coinvolgere il personale dipendente affinché vengano raggiunti gli obiettivi prefissati e sviluppato, ad ogni livello, il senso di responsabilità verso la tutela della la sicurezza delle informazioni;
- Formare e informare ad un lecito e corretto trattamento della sicurezza delle informazioni;
- Promuovere il dialogo e il confronto con tutti i portatori d'interesse (P.A., Garante, Autorità, Cittadini, Associazioni, clienti, lavoratori, ecc.), tenendo conto delle loro istanze, in materia di trattamento di sicurezza delle informazioni, in coerenza con gli strumenti di partecipazione e comunicazione adottati dal gruppo.

Il Consiglio di Amministrazione riconosce come scelta strategica lo sviluppo di un sistema di gestione per la sicurezza delle informazioni integrato e condiviso.

La Direzione, per il tramite di suoi delegati, è coinvolta nel rispetto e nell'attuazione di questi impegni assicurando e verificando periodicamente che la Politica sia documentata, resa operante, mantenuta attiva, periodicamente riesaminata, diffusa a tutto il personale e resa disponibile al pubblico.

La Direzione, inoltre, in considerazione del fatto che il proprio personale si trova anche a svolgere attività lavorativa presso la sede dei Clienti e che offre i propri servizi ai Clienti, ha deciso di estendere tale tutela anche alle informazioni affidate, durante il rapporto contrattuale, dalle terze parti a ***01Sistemi***, o ai suoi rappresentanti, mediante il monitoraggio sistematico del rispetto delle regole di protezione delle informazioni vigenti in ***01Sistemi*** o definite in sede contrattuale.

La Direzione individua nel servizio cloud la principale risorsa attraverso cui fornire il servizio ai propri clienti. L'Organizzazione si impegna a gestire interamente l'infrastruttura cloud su cui risiedono i servizi da essa sviluppati ed erogati in modalità SaaS, garantendone anche le copie di sicurezza e tutte le attività di *disaster recovery* e *business continuity*. Per questa ragione, si è data particolare attenzione alle misure di sicurezza per limitare e contrastare i rischi alle informazioni contenute, mediante tecnologie, metodologie organizzative e risorse economiche, al fine di mantenere i dati isolati e controllati anche nei confronti di personale autorizzato ad accedervi.

Nell'individuare i CSP qualificati, la Direzione deve limitare la scelta al provider che garantisca almeno i livelli di sicurezza delle informazioni concordate negli SLA con il cliente del servizio cloud.

Sistema di Autenticazione per FirmoSemplice

Nei sistemi di identità digitale e firma elettronica basati su servizi cloud, la scelta tecnologica sul sistema di autenticazione per utenti è ricaduta (anche per conformità alle leggi e alle norme italiane) su SPID, che garantisce - allo stato - la migliore combinazione tra fruibilità e sicurezza. La scelta di SPID, oltre che essere, come si è detto, un obbligo normativo, garantisce anche una semplice gestione del ciclo di vita degli account utente, dal momento che essa viene governata dai singoli *Identity*

Provider. Tutte le scelte tecniche devono garantire il rispetto della *privacy* dell'utente, ma anche la possibilità per gli operatori dei software di firma digitale di operare rapidamente ed efficacemente.

Sistema di Autenticazione per SiSemplice

Nel prodotto SiSemplice la scelta di autenticazione è ricaduta su una coppia di credenziali, dove username è rappresentato dall'indirizzo email univoca, e la password è decisa dall'operatore. Le credenziali e il processo di autenticazione sono gestiti da una piattaforma IAM (Keycloak) che offre un'ampia possibilità di configurazione ed di integrazione, sia in termini di sicurezza sia di metodologie di autenticazione. Questo ci permetterebbe attivare l'autenticazione a più fattori MFA, sia di adottare sistemi di identità digitale fra i più diffusi (SPID, CIE, Gmail…).

La gestione del ciclo di vita degli account utente viene gestita direttamente attraverso funzioni della piattaforma, che sono abilitate solo per le utenze amministrative del cliente.

Attualmente i clienti noti hanno preferito adottare solo la coppia di credenziali, username e password, che stiamo valutando di rafforzare con delle funzionalità che scattano al post Login, in modo che il titolare delle credenziali sia avvisto ogni qualvolta queste vengono utilizzate.

Sistema di Autenticazione per SempliceAI

Nei sistemi di intelligenza Artificiale, orientati alla comprensione, classificazione ed elaborazione del linguaggio naturale il software è fornito in licenza d'uso al cliente che utilizza API-KEY, generate successivamente al momento dell'avvio del progetto, per l'accesso alle funzionalità degli applicativi che ricadono in questa categoria.

La gestione del ciclo di vita delle API-KEY avviene nel corso della durata del contratto e termina con la conclusione dello stesso.

Particolare attenzione deve essere posta sulla sicurezza del sistema di virtualizzazione, grazie anche all'ausilio di sistemi di monitoraggio, di alerting e di supporto tecnico per gli utenti.

Il rispetto della normativa sulla protezione dei dati personali impone anche di comunicare tempestivamente eventuali data-breach. L'Organizzazione si impegna a fornire tutto il supporto tecnico per condividere informazioni in caso di investigazioni informatiche, secondo le più attuali modalità informatiche forensi.

Le procedure di change management che includono modifiche importanti o che aggiungono funzionalità significative devono prevedere la comunicazione preventiva al cliente dei servizi cloud secondo le modalità concordate.

Per garantire la continuità operativa delle attività di ***01Sistemi***, è necessario che le opportune forme di protezione siano applicate in modo sistematico in tutte le aree che risultino critiche sulla base di una valutazione dei rischi associata a quella del valore delle informazioni trattate.

In tale ambito, il percorso definito dalla Direzione prevede le seguenti fasi:

- Sviluppo di un Sistema di Gestione per la Sicurezza delle informazioni integrato e condiviso;
- Rilevazione di specifici indicatori di sicurezza delle informazioni per l'adozione di idonee azioni atte a mantenere il livello di rischio a livelli accettabili;
- Attuazione, ove necessario, di idonee azioni correttive per ridurre a livelli ritenuti accettabili l'incidenza di condizioni anomale sul funzionamento complessivo del sistema;
- Definizione di reazioni idonee al manifestarsi di violazioni della sicurezza delle informazioni ("Data Breach") per garantire la continuità dell'operatività in sicurezza (business continuity);
- Definizione di opportune modalità di comunicazione nei confronti degli interessati e del Garante della Privacy;
- Stabilizzazione e progressivo miglioramento del livello di sicurezza, anche attraverso l'attuazione di idonee azioni preventive, rispetto agli indicatori misurati negli anni precedenti.

Al fine di perseguire gli obiettivi prefissati dalla Direzione di ***01Sistemi***, saranno messe in atto iniziative finalizzate a:

- istituire un gruppo tecnico da coinvolgere ogniqualvolta si debbano gestire cambiamenti architetturali in ogni progetto. La sicurezza delle informazioni deve essere sempre tenuta in considerazione come default di ogni nuova iniziativa o in caso di modifiche di progetti esistenti.
- Definire, implementare e mantenere aggiornato ed operativo il Sistema di Gestione della Sicurezza delle Informazioni, conforme al nuovo Regolamento dell'Unione Europea n.2016/679, allo standard internazionale ISO/IEC 27001:2017, alla legislazione vigente e alla tutela dei copyright;
- Sensibilizzare e formare lo staff sul detto Sistema di Gestione della Sicurezza delle Informazioni (SGSI), sui relativi sistemi di riferimento e sulle sanzioni previste in caso di violazione delle regole di protezione delle Informazioni;
- Migliorare continuamente il livello di Sicurezza, sia "logica" (ad es. attraverso l'analisi per identificare potenziali minacce, garantendo in qualsiasi situazione la disponibilità e la capacità di almeno una copia dei dati per finalità di recovery, riducendo al minimo gli incidenti di sicurezza, aggiornando le patch di sicurezza, ecc.) che "organizzativa" (ad es. attraverso incontri di awareness periodica, training delle nuove risorse, training su nuove policy e procedure, NDA, ecc.), rispettando le strategie di business, in conformità ai requisiti legali, normativi e contrattuali, tenendo presente i requisiti delle terze parti interessate.
- Ridurre le vulnerabilità dei propri asset aziendali da minacce quali virus, software nocivo ecc. tramite interventi di monitoraggio e protezione ad ampio spettro che interessano:
    - sistemi hardware e software (personal computer, workstation, server, supporti di memorizzazione, apparecchiature di rete, sistemi di comunicazione elettronica);
    - informazioni (banche dati, documenti digitali e dati in transito su sistemi di comunicazione);

    - servizi (posta elettronica e accessi al portale).
- Caratterizzazione della propria offerta di servizi ai Clienti con la garanzia della salvaguardia delle informazioni condivise mediante il monitoraggio sistematico del rispetto delle regole di protezione delle informazioni vigenti in ***01Sistemi*** o definite in sede contrattuale
- Assegnare e monitorare opportuni ruoli e responsabilità per la gestione della sicurezza delle informazioni;
- Valutare periodicamente i rischi di sicurezza delle informazioni, di tutte le parti interessate, al fine di ridurli a livelli accettabili;
- Aumentare il livello di consapevolezza e competenza aziendale relativamente agli aspetti della sicurezza delle informazioni;
- Proteggere il proprio patrimonio informativo e quello delle parti interessate in termini di Riservatezza, Integrità e Disponibilità;
- L'Azienda si impegna a verificare periodicamente l'efficacia e l'efficienza del sistema di gestione per la sicurezza delle informazioni, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie, al fine di consentire l'attivazione di un processo continuo che tenga sotto controllo il variare delle condizioni a contorno o degli obiettivi di business aziendali al fine di garantirne il suo corretto adeguamento;
- Preservare al meglio l'immagine aziendale;
- Evitare ritardi nell'erogazione dei servizi (rispetto degli SLA);
- Assicurare e monitorare i requisiti di sicurezza all'interno degli accordi con le parti interessate;
- Ridurre il numero di incidenti di sicurezza delle informazioni;
- Soddisfare tutti i requisiti normativi relativi alla Sicurezza delle Informazioni vigenti e cogenti;

Il Sistema di Gestione per la Sicurezza delle Informazioni identifica e tiene conto dei requisiti derivanti dall'evoluzione del contesto interno e del contesto esterno, in particolare dei requisiti delle terze parti interessate, e identifica gli obiettivi di sicurezza da perseguire. La Direzione si impegna ad allocare le risorse necessarie alla realizzazione del predetto sistema e mantiene un "commitment" adeguato sulle tematiche della sicurezza, assicurando che gli obiettivi di sicurezza siano integrati nei processi aziendali e conseguiti.

Sono state inoltre individuate e messe a disposizione le opportune risorse e definite specifiche responsabilità assegnate al Responsabile del Sistema di Gestione della Sicurezza delle Informazioni, che avrà il compito di predisporre e aggiornare il Sistema di Gestione della Sicurezza delle Informazioni, verificarne l'efficacia e relazionare la Direzione sul relativo stato di attuazione.

Lo stato del Sistema di Gestione della Sicurezza delle Informazioni e la valutazione della sua efficacia sono discussi in appositi Riesami della Direzione, che sono riunioni periodiche (almeno una volta l'anno) cui partecipa la Direzione e Responsabile del Sistema di Gestione della Sicurezza delle Informazioni con il compito di analizzare, discutere e fornire indicazioni relativamente a:

- Eventuali variazioni subite dai fattori che determinano l'esito dell'analisi dei rischi: incremento, variazione delle minacce, modifiche valutazione degli impatti, ecc.;
- Risultanze di Rapporti di Incidenti di sicurezza;
- Rapporti di Audit interni.

In considerazione dell'importanza degli obiettivi da raggiungere e dell'impegno necessario per il loro ottenimento, si invita tutto lo Staff a prestare la propria disponibilità e collaborazione nell'attuazione ed aggiornamento del Sistema e ad attenersi scrupolosamente alle prescrizioni contenute nelle procedure operative, nelle politiche e nelle altre disposizioni in merito eventualmente fornite dal management.

11/01/2024 La Direzione