POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

VERSIONE PUBBLICA - 25/05/2024

NAMEX
ROMA IXP

La Security Governance rappresenta un punto fondamentale per la crescita del business di NaMeX, e il suo posizionamento sul mercato come IXP, considerando la sua influenza su:

- preservare gli asset aziendali;
- supportare il rafforzamento del ruolo di NaMeX nell'ambito del mercato di riferimento;
- far crescere i risultati di business aumentando i livelli di efficacia e di efficienza ottimizzando le risorse;
- aumentare la fiducia dei clienti.

Pertanto, la definizione di una Politica di Gestione della Sicurezza delle Informazioni è un punto strategico per supportare e garantire gli obiettivi che possono essere raggiunti.

NaMeX si impegna a implementare la strategia per la Sicurezza delle Informazioni, basata sulla protezione della riservatezza, integrità e disponibilità di tutte le risorse informative fisiche e logiche dell'azienda, al fine di garantire il rispetto dei requisiti normativi, operativi e contrattuali.

In particolare, gli obiettivi principali della Sicurezza delle Informazioni da affrontare sono:

- **Riservatezza:** garantire che le informazioni siano accessibili solo a coloro che sono autorizzati ad accedervi;
- **Integrità:** salvaguardia dell'accuratezza e della completezza delle informazioni e dei metodi di elaborazione;
- **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni quando necessario.

Gli obiettivi generali della Sicurezza delle Informazioni includono quanto segue:

- Garantire la conformità con le attuali leggi nazionali, i regolamenti e le relative linee guida,
- Assicurare un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente, tenendo conto, tra gli altri, dei seguenti elementi:
    a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
    b) la sicurezza dei sistemi e degli impianti;
    c) la gestione degli incidenti;
    d) gestione della continuità operativa;
    e) sicurezza della catena di approvvigionamento;
    f) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete;
    g) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;
    h) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;
    i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi.
- Essere allineati con le politiche interne del Consorzio NaMeX in materia di protezione organizzative e tecnica della propria infrastruttura tecnologica
- Stabilire controlli per proteggere i sistemi informativi e le informazioni di NaMeX da furti, abusi e altre forme di danno e perdita;
- Motivare tutti i dipendenti a migliorare la loro consapevolezza della sicurezza al fine di proteggere e salvaguardare i dati di NaMeX;

- Assicurarsi che NaMeX sia in grado di dare continuità ai propri servizi, anche se si verificano incidenti di sicurezza importanti
- Garantire la disponibilità e l'affidabilità dell'infrastruttura di rete e la continuità dei servizi essenziali forniti e gestiti da NaMeX in relazione al proprio ruolo di IXP
- Rispettare le metodologie degli standard internazionali per la Sicurezza delle Informazioni, in particolare quelle della norma ISO/IEC 27001;
- Garantire flessibilità e un adeguato livello di sicurezza per l'accesso ai sistemi di informazione.
- Garantire un processo di miglioramento continuo volto a valutare le opportunità per incrementare il proprio livello di gestione della sicurezza delle informazioni

La visione della sicurezza di NaMeX si basa sulla protezione delle risorse informative, sulla gestione dei rischi per la sicurezza, sull'attuazione delle strategie di business in modo efficace ed efficiente, supportata da una leadership operativa e sostenuta da tutti i dipendenti NaMeX.

I principali driver coinvolti in una definizione del piano strategico di sicurezza sono:

- **Aspettative di sicurezza di NaMeX:** l'aspettativa e l'ambizione dell'organizzazione che sono l'input principale per definire gli obiettivi, le relative attività di sicurezza e l'investimento in una visione a lungo termine;
- **Gestione del rischio:** i risultati dal punto di vista della gestione del rischio per quanto riguarda i principali rischi per la sicurezza di NaMeX in termini di Sicurezza delle Informazioni;
- **Regolamentazione e conformità:** influenza esterna attraverso esigenze normative e di conformità;
- **Esigenze e aspettative delle altre parti interessate:** aspettative specificate all'interno della definizione del contesto definito da NaMeX
- **Posizionamento rispetto alla sicurezza:** la posizione di sicurezza risultante da una valutazione tecnica interna/esterna (ad esempio vulnerability assessment) e da considerazioni esterne che possono influenzare le priorità sulle attività aziendali; tra queste ultime sono da considerare quelle derivanti dai requisiti relativi all'adozione di misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che NaMeX utilizza nelle proprie operazioni.
- **Campagne di sensibilizzazione:** i risultati delle campagne di sensibilizzazione che sono un indicatore della prontezza dei dipendenti in materia di sicurezza.

Questi driver e i relativi obiettivi devono essere stabiliti e rivisti ogni anno, al fine di considerarli come la base per una strategia a livello organizzativo e per impostare un livello corretto per la Sicurezza delle Informazioni.

Devono essere noti sia il livello di classificazione delle informazioni che l'organizzazione memorizza e processa, che il potenziale danno che potrebbe essere causato da incidenti di sicurezza che interessano tali informazioni; così come la violazione dei dati personali ai sensi del GDPR.

Ciò significa che la questione della sicurezza sarà considerata un'alta priorità nel prendere qualsiasi decisione di tipo aziendale. Ciò consentirà a NaMeX di allocare risorse umane, tecniche e finanziarie sufficienti alla gestione della Sicurezza delle Informazioni e di intraprendere azioni appropriate in risposta a tutte le possibili violazioni alla Sicurezza.

Gli impegni e gli sforzi aziendali per la sicurezza saranno:

- **Coordinati:** saranno prese misure di sicurezza basate su un quadro comune e tutto il personale sarà coinvolto nel mantenimento della conformità con esso;

- **Proattivi:** le minacce e le lacune di sicurezza saranno rilevate, identificate e gestite al fine di prevenire incidenti di sicurezza;
- **Supportati al massimo livello:** la sicurezza delle informazioni sarà supportata pienamente dal management per implementare i controlli di sicurezza identificati attraverso un processo di valutazione del rischio continuo.

La Politica per la Sicurezza delle Informazioni, elaborata dalla Direzione viene revisionata ed eventualmente aggiornata ogni anno durante il Riesame della Direzione.

La Direzione