Framework di sicurezza e compliance normativa

IDEATO DA KEVIN PIZZINATO

Cosa tratterà questo argomento?

- Faremo una analisi comparativa tra i due standard di sicurezza(ISO 27001, NIST CSF).
- Quanti e come possiamo implementare tecniche di sicurezza.
- Gap analysis e risk assessment metodologie.
- Audit e certificazione di sicurezza.

- L'evoluzione della normativa della sicurezza informatica.
- Le/a Responsabilità legali delle organizzazioni.
- Bilanciamento tra compliance e innovazione.
- Trasparenza e accountability nelle politiche di sicurezza.

Prima di tutto... Cosa sono questi due standard?

- **L'ISO 27001➤** è una norma che specifica i requisiti per stabilire, implementare, mantenere e migliorare un sitema di gestione della sicurezza delle informazioni, con obiettivo di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni presenti nel sistema.

- **NIST CSF➤** Il **NIST Cybersecurity Framework** è un framework basato su standard e linee guida, che aiuta le organizzazioni a identificare, proteggere, rilevare, rispondere e recuperare da eventi (perlopiù attacchi) di sicurezza informatica.

COMPARAZIONE TRA I DUE

NOME	ISO 27001	NIST CSF
ORIGINE	ISO (internazionale)	USA
Certificabile	tramite audit	No
Obiettivo	Gestione formale della sicurezza.	Gestione del rischio cyber
Struttura	Requisiti + Controlli (Allegato A)	Identifica, Preoteggi, Individua, Rispondi, Recupera
Approccio	Normativo, sistemico	Pratico, modulare
Flessibilità	Più rigido, formale	Adattabile, scalabile
Target	Qualsiasi organizzazione	Organizzazioni (pubbliche e private), Soprattutto negli USA
Riconoscimento	Mondiale	Molto Conosciuto, ma soprattutto negli Stati Uniti

L'implementazione tecnica dei controlli di sicurezza

L'implementazione tecnica dei controlli di sicurezza include l'uso di soluzioni firewall, crittografia, backup e controllo dei log in come citati anche in classe usati per proteggere i dati e prevenire incidenti di sicurezza.

Nel Dettaglio

- **Firewall ➤** Filtrano il traffico e rilevano/prevenzione intrusioni
- **Crittografia ➤** Protegge dati in transito e a riposo (es. HTTPS, VPN)
- **Gestione accessi ➤** Autenticazione forte, controllo dei privilegi
- **Backup e ripristino ➤** Protezione dei dati con copie sicure e piani di recovery
- **Monitoraggio dei logging ➤** Registrazione eventi e avvisi su comportamenti anomali

Gap analysis e risk assessment metodologie

Che cosa sono?

-Gap Analysis ➤ Serve per individuare le differenze tra la situazione attuale della sicurezza informatica dell'organizzazione e i requisiti di uno standard. Quindi cerca di essere conforme lo standard ISO 27001.

-Risk Assessment ➤ È il processo di identificare, analizzare e valutare i rischi per la sicurezza delle informazioni.Quindi si concenrtra soprattutto nelle minacce, vulnerabilità, impatti e probabilità della sicurezza.

Audit e certificazione di sicurezza

Cosa sono?

-Audit ➤ È una **verifica sistematica** e **indipendente** per valutare se l'organizzazione rispetta i requisiti di uno standard.
con l'obiettivo di verificare la **conformità** e l'**efficacia** del sistema di gestione

-Certificazione ➤ È riconoscimento ufficiale da un ente terzo che attesta la conformità a uno standard di sicurezza.
Ha come obiettivo di certificare il Sistema di Gestione per la Sicurezza delle Informazioni.

L' Evoluzione normativa della sicurezza informatica

Anno del rilascio	Nome Normativa	Descrizione
1995	Direttiva UE 95/46/CE	Prima legge europea sulla protezione dei dati personali
2005	ISO 27001:2005	Prima versione dello standard internazionale per la gestione della sicurezza.
2013	NIST Cybersecurity Framework	Guida volontaria per la gestione del rischio informatico, USA
2016	Regolamento UE 2016/679 (GDPR)	Nuova normativa europea per la protezione dei dati personali.
2022	ISO 27001:2022	Ultimo aggiornamento della norma ISO 27001, con 93 controlli rivisti.
2023	Direttiva NIS2	Rafforza la cybersecurity nei settori critici in tutta l'UE.

Responsabilità legale delle organizzazioni

Le organizzazioni hanno l'**obbligo legale** di **proteggere i dati personali e i sistemi informativi** da accessi non autorizzati, perdite e violazioni.
Se non adottano **misure di sicurezza adeguate**, possono essere **civilmente, penalmente o amministrativamente responsabili**.

Responsabilità da rispettare

-Privacy[GDPR]

-Cybersecurity

-Codice Penale (In Italia)

-Responsabilità amministrativa (D.Lgs. 231/2001): se un crimine informatico è commesso nell'interesse dell'ente.

Che cos'è il Bilanciamento tra Compliance e Innovazione?

Il Bilanciamento tra Compliance e Innovazione è quando e organizzazioni devono rispettare norme e standard di sicurezza senza ostacolare la velocità e creatività dell'innovazione tecnologica.

-Compilance➤ garantisce **sicurezza, fiducia** e **continuità** ma può rallentare i processi se troppo rigida.

-Innovazione➤ spinge verso nuove **soluzioni** e **competitività**, ma può introdurre nuovi **rischi** se non governata.

La Trasparenza e Accountability nelle Politiche di Sicurezza

La Transparenza e Accountability nelle politiche di sicurezza è suddivisa in due parti che sono:

-Transparenza➤ Significa rendere **chiare, accessibili e comprensibili** le politiche di sicurezza a tutte le parti coinvolte (dipendenti, clienti, partner).

-Accountability➤ L'organizzazione deve **dimostrare concretamente** di adottare misure efficaci per proteggere i dati e gestire i rischi.

Glossario

CSF ➤ CyberSecurity Framework.
GDPR ➤ General Data Protection Regulation.
ISO ➤ International Organization for Standardization.
NIST ➤ National Institute of Standards and Technology.
VPN ➤ Virtual Private Network.
HTTPS ➤ HyperText Transfer Protocol Secure.
D.Lgs. 231/2001 ➤ Decreto Legislativo sulla responsabilità amministrativa degli enti.
NIS2➤ Network and Information Security Directive 2.
CE➤ Comunità Europea.

The End