contromisure e framework

esempi di contromisure

	Prevenzione	Rilevazione	Contrasto	Ripristino
Confidenzialità	controllo d'accesso, confinamento crittografia	logging, IDS, auditing	logging, IDS, auditing	-
Integrità	controllo d'accesso, confinamento, backup (ripristino), crittografia (rilevazione)	logging, IDS, auditing, crittografia	logging, IDS, auditing	ripristino backup
Disponibilità	ridondanza, high availability, fail over, auditing, backup (ripristino)	logging, auditing	attivazione fail-over	fix hardware, ripristino backup

difficoltà e framework

- fare una accurata analisi del rischio è difficile e costoso
- scegliere le migliori contromisure è difficile e costoso
- molte esigenze di sicurezza sono comuni

- esistono degli standard che guidano nell'analisi del rischio e nella scelta delle contromisure
  - tipicamente chiamati «framework»

Sistema di Gestione della Sicurezza delle Informazioni

- policy, procedure, linee guida e risorse
- per stabilire, realizzare, condurre, monitorare, rivedere, mantenere e migliorare la sicurezza
- scopo finale: proteggere gli asset informativi

- la terminologia è introdotta ISO27001

Framework di riferimento

(per gentile concessione di Fabio Vernacotola – Avanade)

- Insieme di «controlli», variamente organizzati, che definiscono cosa una organizzazione deve fare per poter gestire la propria sicurezza informatica.
- I framework rappresentano la formalizzazione di una «best practice» ma possono essere anche di derivazione normativa.
- I framework:
  - consentono una valutazione del proprio livello di sicurezza;
  - semplificano le attività di conduzione del proprio Sistema di Gestione della Sicurezza delle Informazioni;
  - forniscono una base per le attività di audit interno.

ISO 27001: esempi di controlli

Dominio

Obiettivo di controllo

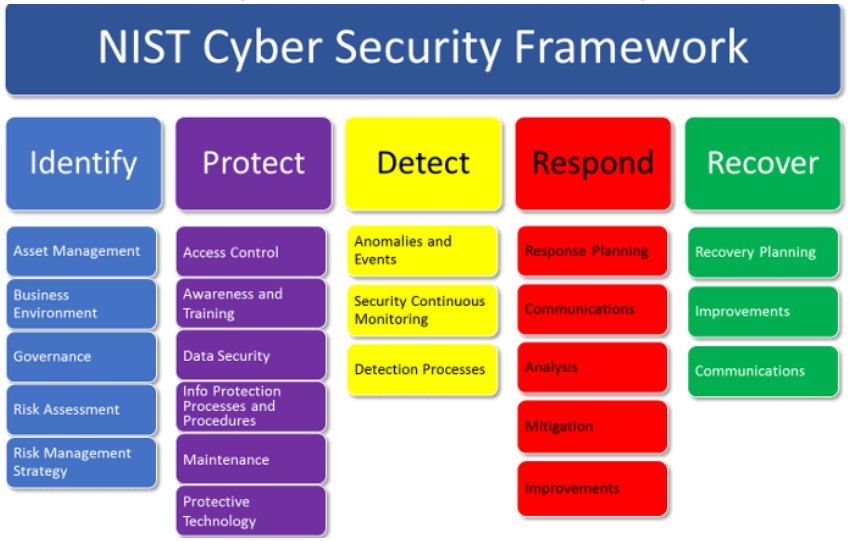
Controlli

A.5 Politiche per la sicurezza delle informazioni		
A.5.1 Indirizzi della direzione per la sicurezza delle informazioni		
Obiettivo: Fornire gli indirizzi ed il supporto della direzione per la sicurezza delle informazioni in accordo con i requisiti di business, con le leggi e con i regolamenti pertinenti.		
A.5.1.1	Politiche per la sicurezza delle informazioni	*Controllo* Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti.
A.5.1.2	Riesame delle politiche per la sicurezza delle informazioni	*Controllo* Le politiche per la sicurezza delle informazioni devono essere riesaminate ad intervalli pianificati o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.

A.13 Sicurezza delle comunicazioni		
A.13.1 Gestione della sicurezza della rete		
Obiettivo: Assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto.		
A.13.1.1	Controlli di rete	*Controllo* Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni.
A.13.1.2	Sicurezza dei servizi di rete	*Controllo* I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete devono essere identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall'interno o siano affidati all'esterno.
A.13.1.3	Segregazione nelle reti	*Controllo* Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi.

altri esempi

- NIST Cyber Security Framework



- CIS Security Controls