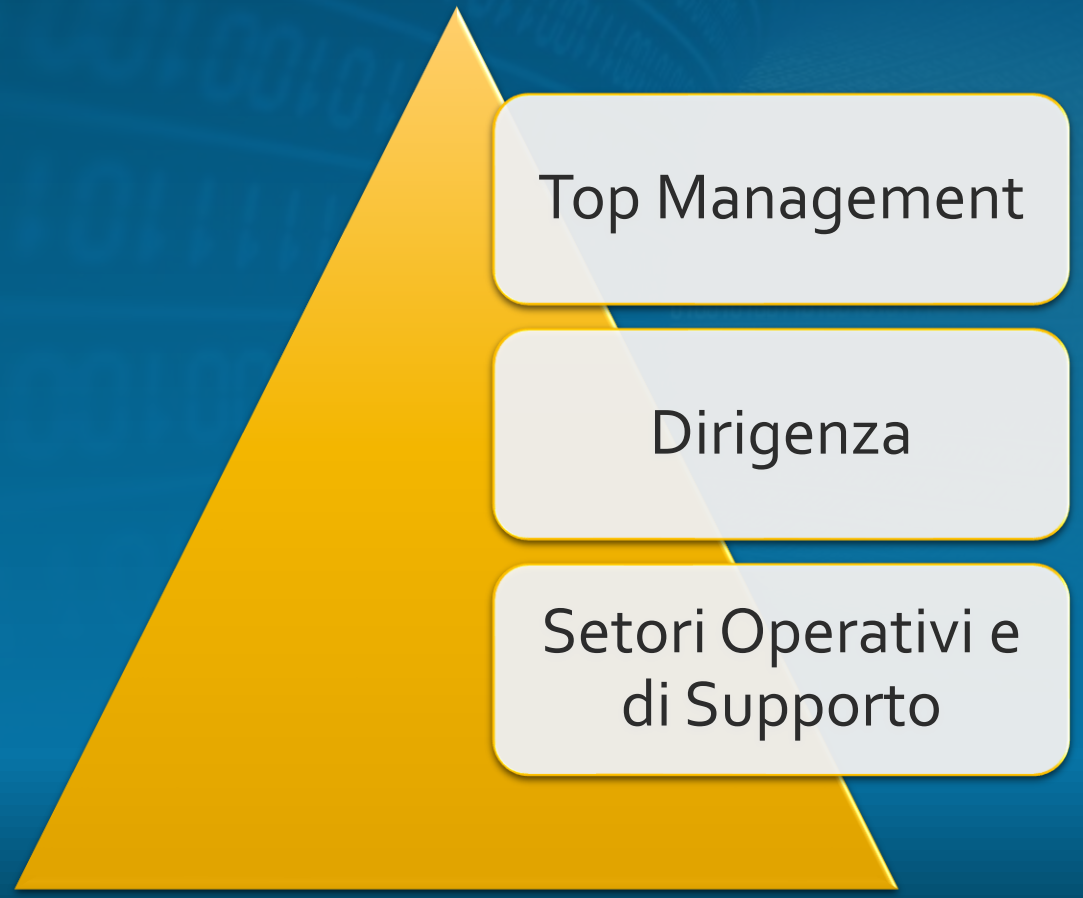
CYBER SECURITY

Lezione 06 - Organizzazione della sicurezza

Obiettivo

- Conoscere i principali **processi** da attivare in un'organizzazione che mira a conseguire la sicurezza delle informazioni.

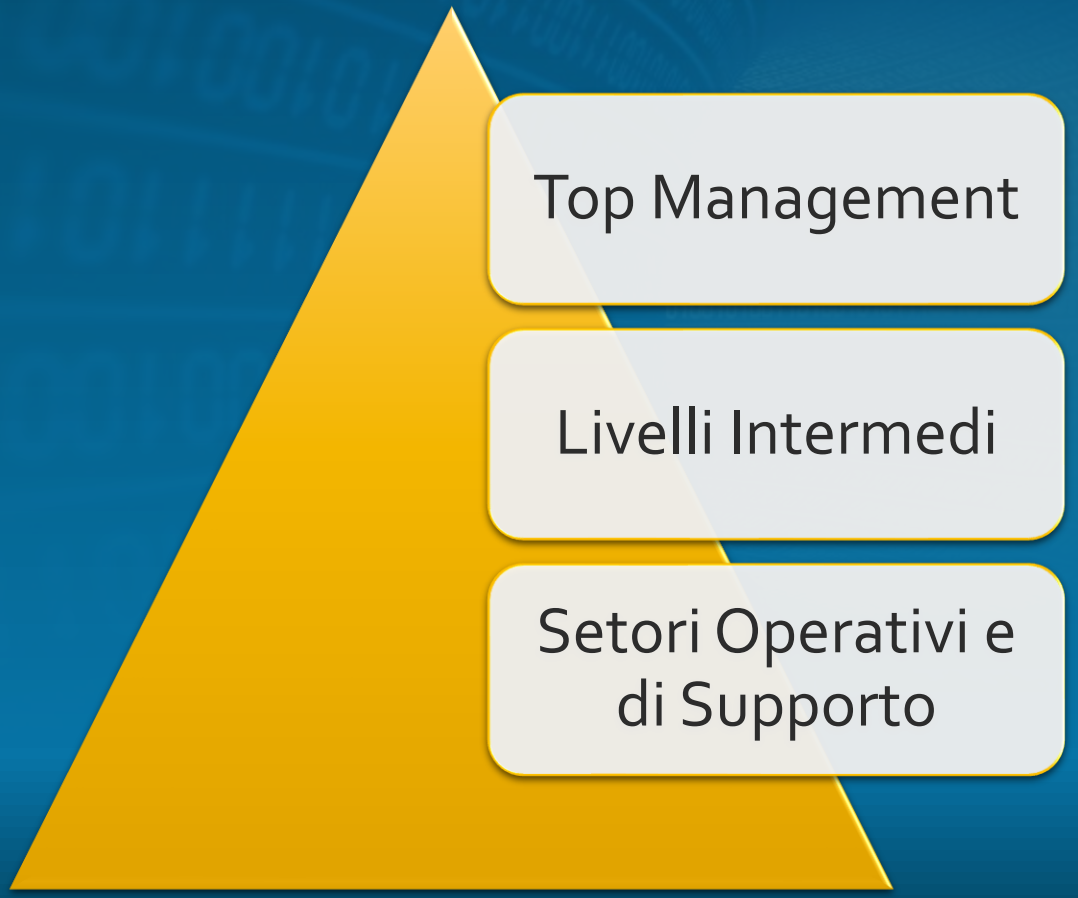
Organizzazione della Sicurezza



obiettivi di business strategici

- classificazione dei beni e del loro valore
- censimento di vulnerabilità e minacce
- analisi del rischio
- analisi costi/benefici delle contromisure
- valutazione del grado di protezione
- definizione delle politiche di sicurezza
- pianificazione, implementazione e gestione dei progetti di sicurezza
- monitoraggio della conformità tra le soluzioni adottate e le politiche di sicurezza

Organizzazione della Sicurezza



Vantaggi coinvolgimento Top-Btm

- *coinvolgere tutti i livelli aziendali interessati,*
- *assegnare precise responsabilità,*
- *definire politiche coerenti per l'intera struttura aziendale,*
- *sensibilizzare ed educare il personale,*
- *finanziare adeguatamente il progetto sicurezza*
- *rimuovere gli ostacoli*

Policy di Sicurezza

Generalmente sono necessarie ***diverse politiche di sicurezza a più livelli****, da quello superiore riguardante l'intera azienda, scendendo ad argomenti più specifici, come il sistema informatico e i singoli aspetti tecnici.*

- **politica di sicurezza aziendale**
- **politica di sicurezza del sistema informatico**
- **politica di sicurezza tecnica**

https://www.sans.org/security-resources/policies/

Policy di Sicurezza

*Generalmente sono necessarie **diverse politiche di sicurezza a più livelli**, da quello superiore riguardante l'intera azienda, scendendo ad argomenti più specifici, come il sistema informatico e i singoli aspetti tecnici.*

- **politica di sicurezza aziendale**
- **politica di sicurezza del sistema informatico**
- **politica di sicurezza tecnica**

indica tutto ciò che deve essere protetto (beni materiali e immateriali) in funzione del tipo di attività dell'azienda, del modello di business, dei vincoli esterni (mercato, competizione, leggi vigenti) e dei fattori di rischio.

Policy di Sicurezza

*Generalmente sono necessarie **diverse politiche di sicurezza a più livelli**, da quello superiore riguardante l'intera azienda, scendendo ad argomenti più specifici, come il sistema informatico e i singoli aspetti tecnici.*

- **politica di sicurezza aziendale**
- **politica di sicurezza del sistema informatico**
- **politica di sicurezza tecnica**

definisce, coerentemente con la politica di sicurezza aziendale, come l'azienda intende proteggere le informazioni e le risorse informatiche, senza entrare nel merito delle tecnologie che verranno adottate.

Policy di Sicurezza

*Generalmente sono necessarie **diverse politiche di sicurezza a più livelli**, da quello superiore riguardante l'intera azienda, scendendo ad argomenti più specifici, come il sistema informatico e i singoli aspetti tecnici.*

- **politica di sicurezza aziendale**
- **politica di sicurezza del sistema informatico**
- **politica di sicurezza tecnica**

traduce in requisiti tecnici funzionali gli obiettivi che si desidera raggiungere attraverso le contromisure di tipo tecnico informatico, nel contesto dell'architettura di sistema adottata o pianificata dall'azienda.

Disaster recovery e Business continuity

- *La* **Disaster Recovery**, *nel contesto informatico, è la capacità di un'infrastruttura di riprendere le operazioni dopo un disastro.*

Due caratteristiche per valutare l'efficacia di un sistema disaster recovery sono il:

- **Recovery Point Objective** (RPO, il momento nel tempo a cui il sistema è riportato), e il
- **Recovery Time Objective** (RTO, il lasso di tempo che intercorre prima di ripristinare l'infrastruttura).

Disaster recovery e Business continuity

La **business continuity** *descrive i processi e le procedure che un'organizzazione mette in atto per assicurare che le funzioni essenziali rimangano operative durante e dopo un disastro*

Il Business Continuity Planning cerca di prevenire l'interruzione dei servizi critici e di ripristinare la piena operatività nel modo più rapido e indolore possibile

Disaster recovery e Business continuity

- un piano di disaster recovery è *reattivo* e si focalizza di solito sul ripristino dell'infrastruttura informatica. Sebbene sia logico irrobustire l'infrastruttura informatica per prevenire un disastro, lo scopo principale del piano di disaster recovery è rimediare ai danni all'infrastruttura.
- un piano di business continuity non soltanto è *proattivo*, ma ha anche l'obiettivo di mantenere in funzione le attività dell'azienda durante qualsiasi evento, non limitandosi a ripristinare i computer dopo il fatto.