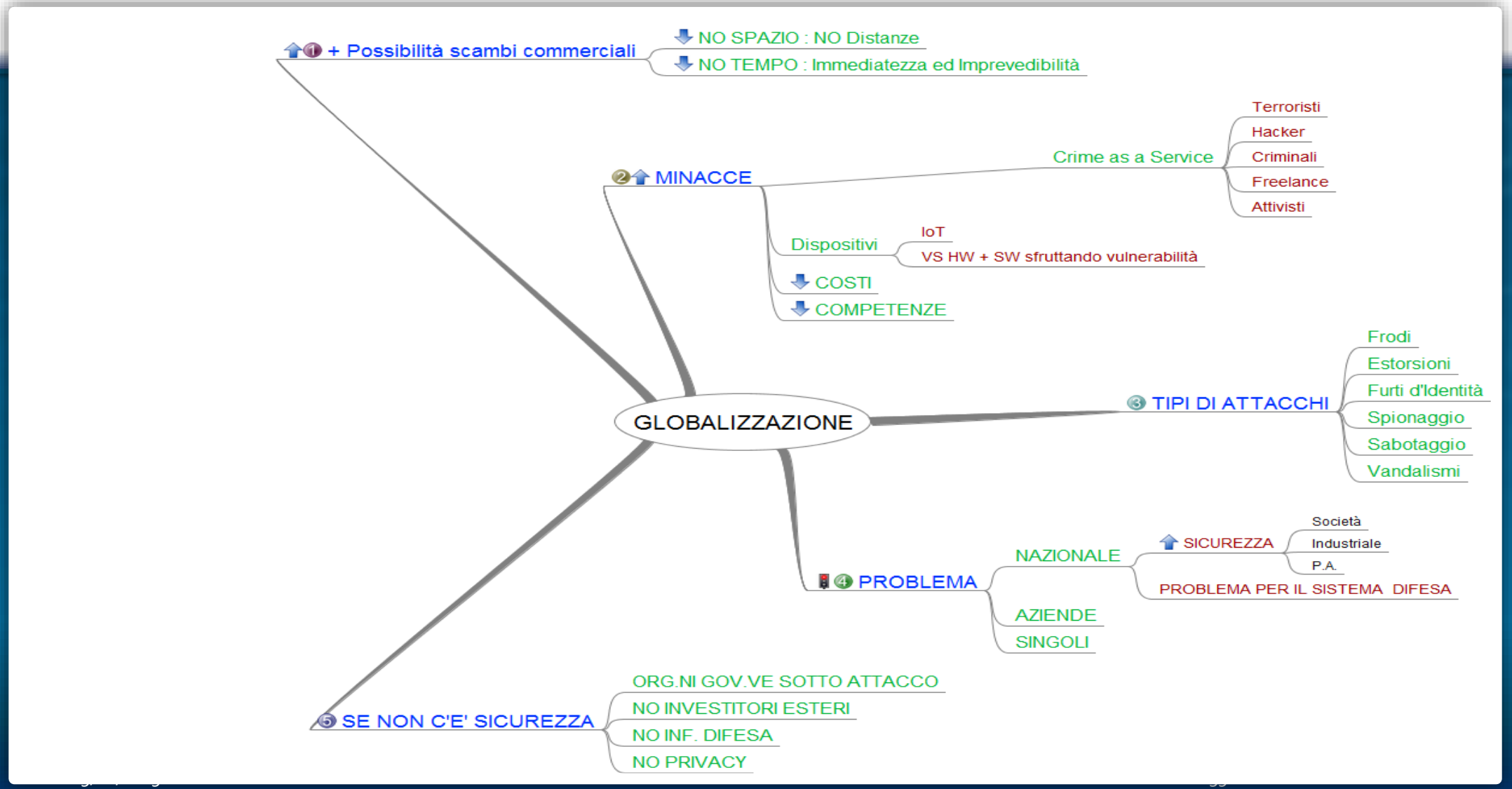
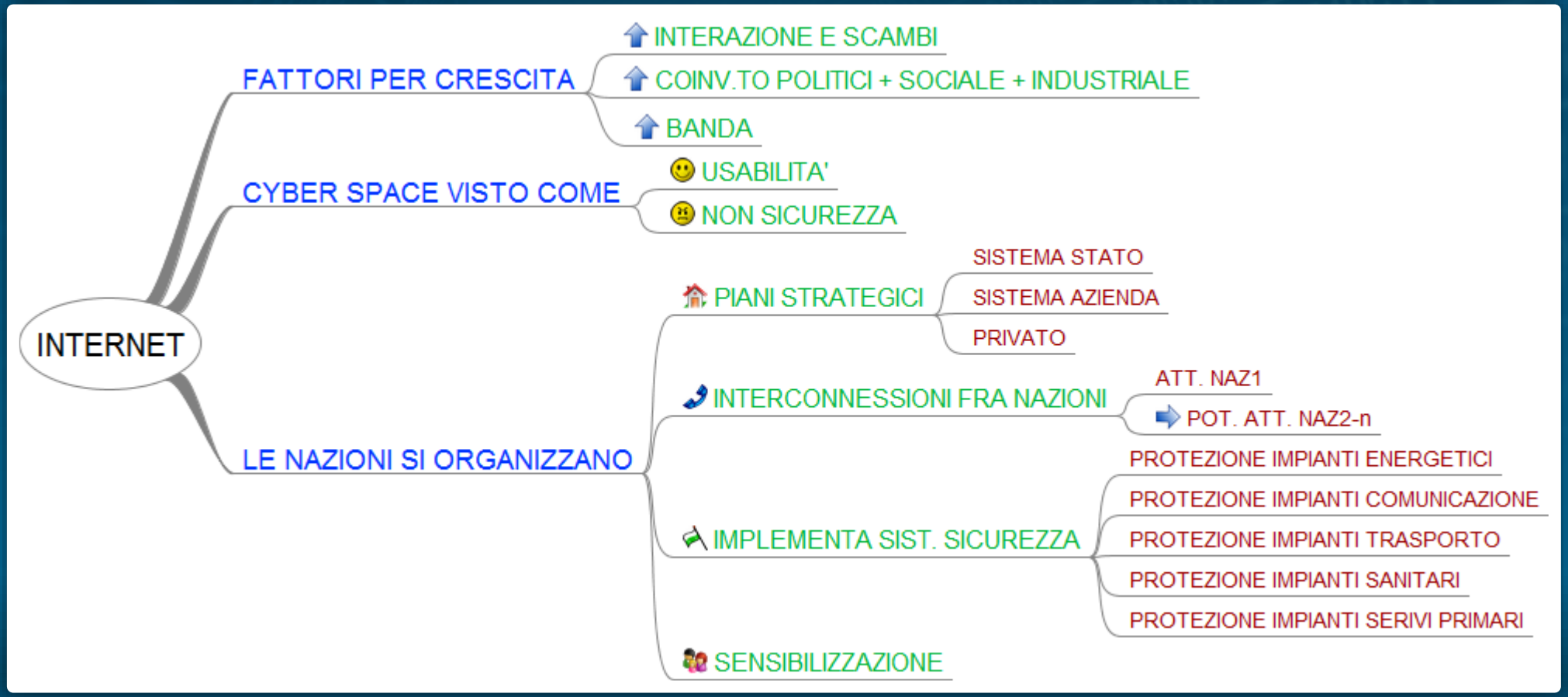
CYBER SECURITY

Lezione 01 – Concetti di base

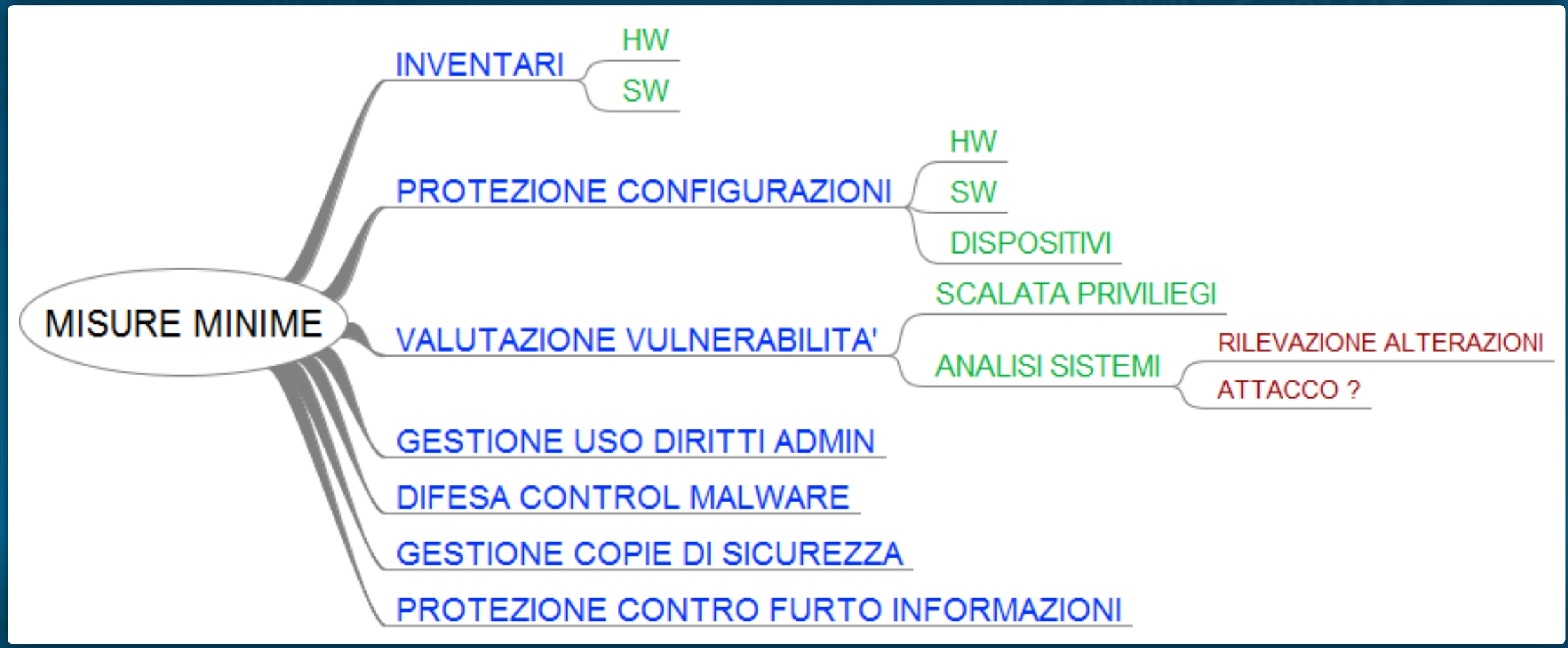
LA GLOBALIZZAZIONE



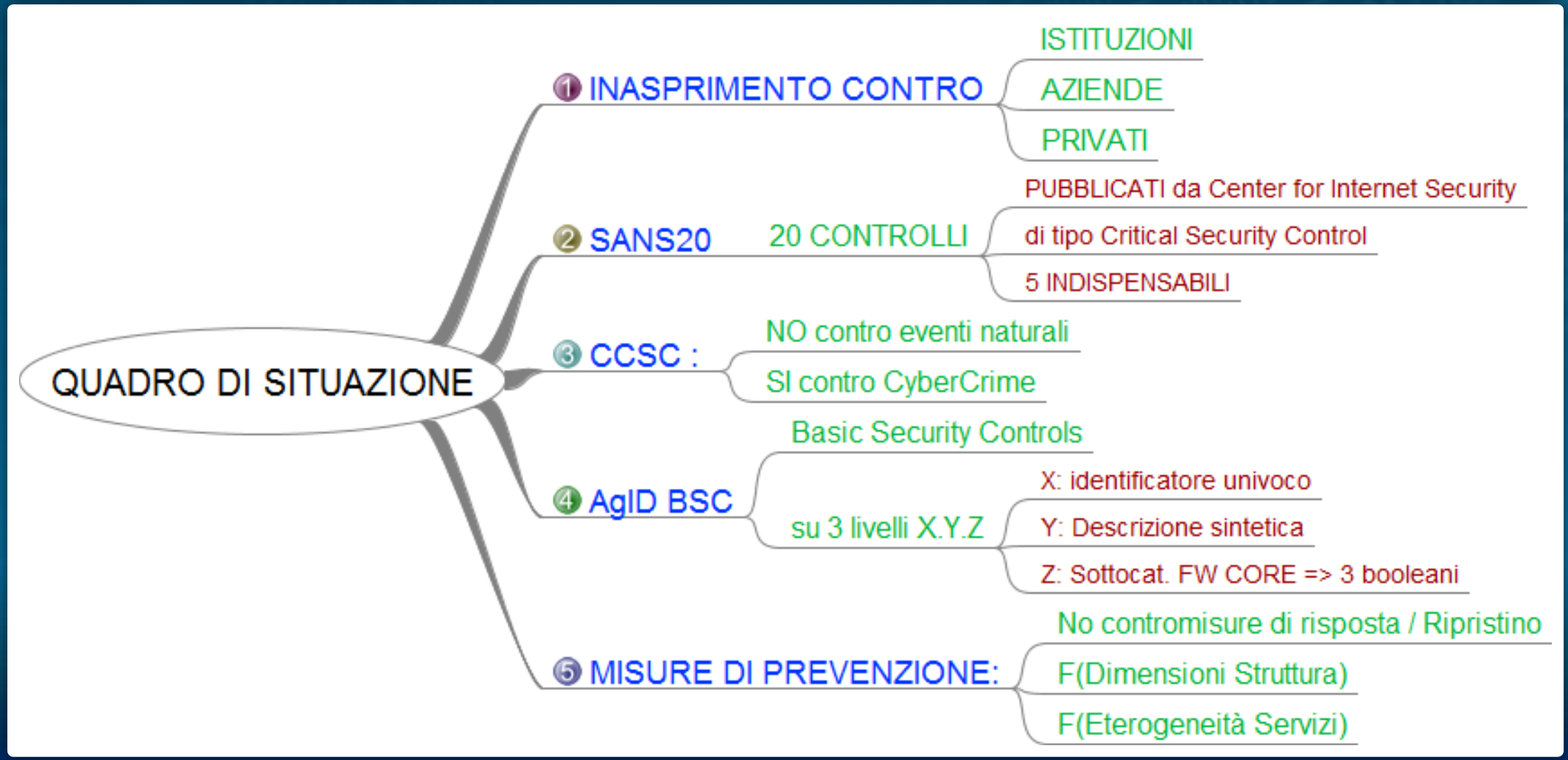
INTERNET


INTERNET
FATTORI PER CRESCITA
INTERAZIONE E SCAMBI
COINV.TO POLITICI + SOCIALE + INDUSTRIALE
BANDA
CYBER SPACE VISTO COME
USABILITA'
NON SICUREZZA
LE NAZIONI SI ORGANIZZANO
PIANI STRATEGICI
SISTEMA STATO
SISTEMA AZIENDA
PRIVATO
INTERCONNESSIONI FRA NAZIONI
ATT. NAZ1
POT. ATT. NAZ2-n
IMPLEMENTA SIST. SICUREZZA
PROTEZIONE IMPIANTI ENERGETICI
PROTEZIONE IMPIANTI COMUNICAZIONE
PROTEZIONE IMPIANTI TRASPORTO
PROTEZIONE IMPIANTI SANITARI
PROTEZIONE IMPIANTI SERIVI PRIMARI
SENSIBILIZZAZIONE

MISURE MINIME



QUADRI DI SITUAZIONE



Il Framework

- 5 FUNZIONI
- 21 CATEGORIE
- 98 SOTTOCATEGORIE

- LIVELLI DI PRIORITA'
- LIVELLI DI MATURITA'

Dal National Institute for Standards and Technology (NIST) statunitense eredita:

- Framework Core,
- Profile
- Implementation Tier.

Il Framework Core

- Framework Core.
- Il core rappresenta la struttura del ciclo di vita del processo di gestione della cyber security, sia dal punto di vista tecnico sia organizzativo. Il core è strutturato gerarchicamente in Function, Category e Subcategory.
- Le Function, concorrenti e continue, sono: **Identify, Protect, Detect, Respond, Recover** e costituiscono le principali tematiche da affrontare per operare una adeguata gestione del rischio cyber in modo strategico.

Il Framework

- 5 FUNZIONI
- 21 CATEGORIE
- 98 SOTTOCATEGORIE

- LIVELLI DI PRIORITA'
- LIVELLI DI MATURITA'

Dal National Institute for Standards and Technology (NIST) statunitense eredita:

- **Framework Core,**
- Profile
- Implementation Tier.

Le Functions

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Le Functions: Identify

- La Function Identify è legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati.
- Le Categories all'interno di questa Function sono:
  - Asset Management;
  - Ambiente di business;
  - Governance;
  - Valutazione del rischio;
  - Strategia di gestione del rischio.

Le Functions: Protect

- La Function Protect è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica.
- Le Categories all'interno di questa Function sono:
  - Access Control;
  - Awareness and Training;
  - Data Security;
  - Information Protection Processes and Procedures;
  - Maintenance;
  - Protective Technology.

Le Functions: Detect

- La Function Detect è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica.
- Le Categories all'interno di questa Function sono:
  - Anomalies and Events;
  - Security Continuous Monitoring;
  - Detection Processes

Le Functions: Respond

- La Function Respond è legata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato.
- Le Categories all'interno di questa Function sono:
  - Planning;
  - Communications;
  - Analysis;
  - Mitigation;
  - Improvements.

Le Functions: Recover

- La Function Recover è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente.
- Le Categories all'interno di questa Function sono:
  - Recovery Planning;
  - Improvements;
  - Communications.

Il Framework

- 5 FUNZIONI
- 21 CATEGORIE
- 98 SOTTOCATEGORIE

- LIVELLI DI PRIORITA'
- LIVELLI DI MATURITA'

Dal National Institute for Standards and Technology (NIST) statunitense eredita:

- Framework Core,
- **Profile**
- Implementation Tier.

Il Profile

- I Profile rappresentano il risultato della selezione, da parte di un'organizzazione, di specifiche Subcategory del Framework.
- I profili possono essere utilizzati per migliorare lo stato di sicurezza mettendo a confronto un profilo attuale (anche detto corrente), con un profilo desiderato (anche detto target).
- I profili possono essere utilizzati per:
  - Effettuare un'autovalutazione o per comunicare il proprio livello di gestione del rischio all'interno o all'esterno dell'organizzazione.
  - Definire profili minimi richiesti da un'organizzazione per poter usufruire di servizi offerti da terzi.

Il Framework

- 5 FUNZIONI
- 21 CATEGORIE
- 98 SOTTOCATEGORIE

- LIVELLI DI PRIORITA'
- LIVELLI DI MATURITA'

Dal National Institute for Standards and Technology (NIST) statunitense eredita:

- Framework Core,
- Profile
- **Implementation Tier.**

Implementation Tier.

- Gli Implementation Tier forniscono contesto su come l'azienda, nel suo complesso, veda il rischio cyber e i processi posti in essere per gestirlo.
- Sono previsti quattro livelli di valutazione, dal più debole al più forte:
  - (1) Parziale,
  - (2) Informato,
  - (3) Ripetibile,
  - (4) Adattivo.

Implementation Tier.

- **(1) Parziale,**
- (2) Informato,
- (3) Ripetibile,
- (4) Adattivo.

Parziale. Un modello di gestione del rischio di cyber security di una organizzazione è parziale se questo non tiene conto in modo sistematico del rischio cyber o delle minacce ambientali.

Implementation Tier.

- (1) Parziale,
- **(2) Informato,**
- (3) Ripetibile,
- (4) Adattivo.

Informato. Un modello di gestione del rischio cyber di una organizzazione è informato se l'organizzazione ha dei processi interni che tengono conto del rischio cyber, ma questi non sono estesi a tutta l'organizzazione.

Implementation Tier.

- (1) Parziale,
- (2) Informato,
- **(3) Ripetibile,**
- (4) Adattivo.

Ripetibile. Un modello di gestione del rischio cyber di una organizzazione è ripetibile se l'organizzazione aggiorna regolarmente le proprie pratiche di cyber security basandosi sull'output del processo di risk management.

Implementation Tier.

- (1) Parziale,
- (2) Informato,
- (3) Ripetibile,
- **(4) Adattivo.**

Adattivo. Un modello di gestione del rischio cyber di una organizzazione è adattivo se l'organizzazione adatta le sue procedure di cyber security frequentemente attraverso l'utilizzo delle esperienze passate e degli indicatori di rischio.

Livelli di Priorità

Determinazione sulla base di :

- capacità di ridurre il rischio cyber, agendo su uno o più dei fattori chiave per la determinazione, ovvero:
  - esposizione alle minacce, intesa come l'insieme dei fattori che aumentano o diminuiscono la facilità con cui la minaccia stessa può manifestarsi;
  - probabilità di loro accadimento, ovvero la frequenza con cui una specifica minaccia può verificarsi nel tempo;
  - impatto conseguente sulle Business Operations o sugli Asset aziendali, intesa come l'entità del danno conseguente al verificarsi di una minaccia;
- semplicità di implementazione delle Subcategory, anche considerando il livello di maturità tecnica e organizzativa tipicamente richiesto per realizzare la specifica azione.

I LIVELLI DI MATURITÀ

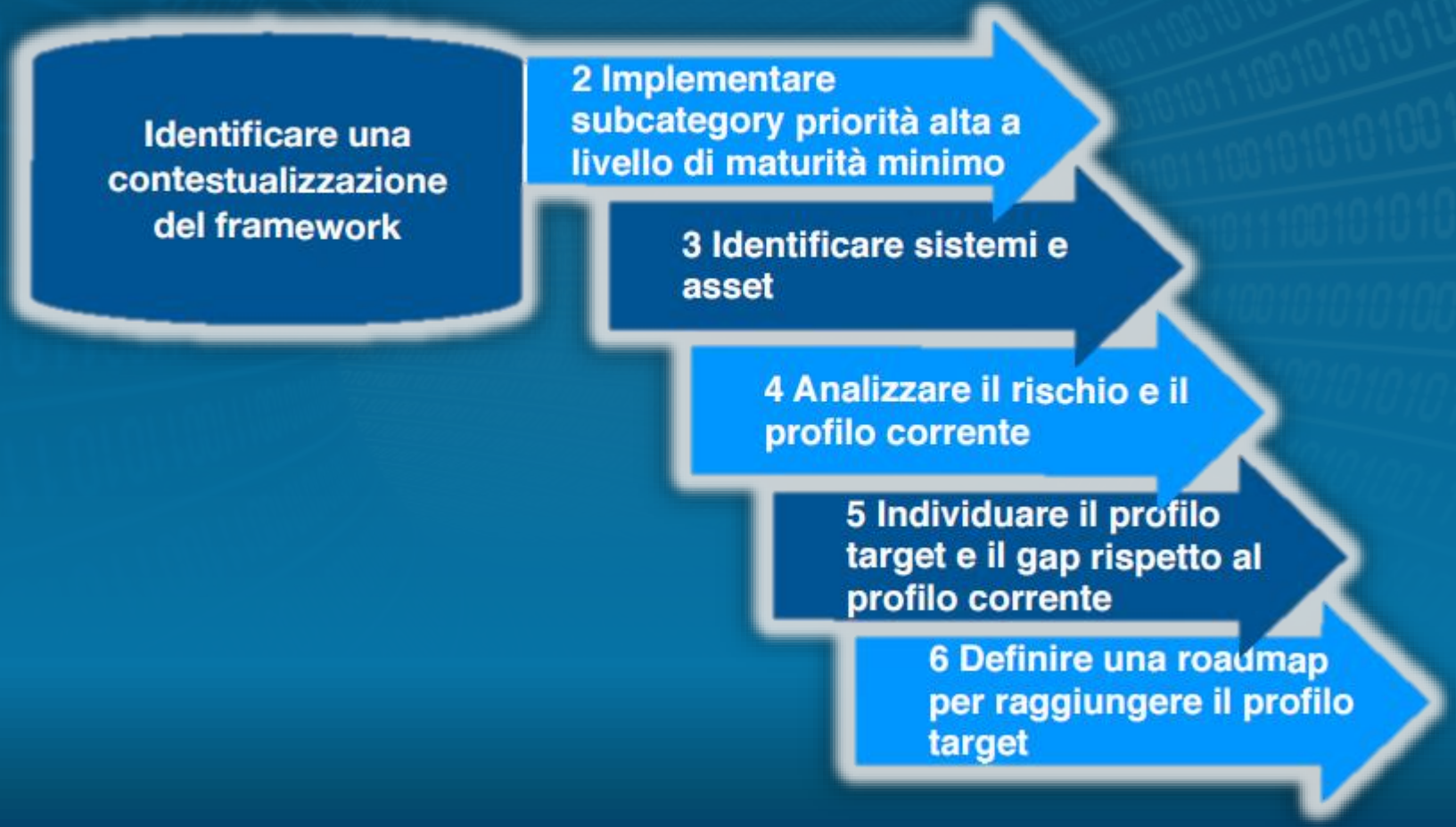
- I livelli di maturità forniscono un punto di riferimento in base al quale ogni organizzazione può valutare la propria implementazione delle Subcategory e fissare obiettivi e priorità per il loro miglioramento.
- I livelli devono essere in progressione, dal minore al maggiore

I LIVELLI DI MATURITÀ

- Esempio di livelli di maturità per Subcategory "PR.AC-1: PR.AC-1:Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate".

Livello	Descrizione
M1	Le identità e le credenziali sono amministrate localmente su ciascun dispositivo o sistema IT.
M2	Le identità e le credenziali sono amministrate attraverso una directory aziendale che consente l'applicazione omogenea di regole e livelli minimi di sicurezza.
M3	Specifiche soluzioni tecnologiche sono adottate per gestire in maniera specifica e appropriata le utenze privilegiate (es. Amministratori di Sistema).

Step per le PMI



Step per le Grandi Aziende