



Fastweb Digital Academy

# **CIBERSICUREZZA: DIFESA PERSONALE**

Docente  
**Guglielmo Bondioni**

# DEFINIZIONE DI MINACCIA INFORMATICA

**Ciò che può causare un danno a un sistema informatico**

Può essere:

- a) Dolosa, da parte di persone / organizzazioni
- b) Accidentale o conseguenza di eventi indipendenti

# MISURE MINIME DI SICUREZZA ICT PER LE PA

Articolate in **8 gruppi di controlli**.

I controlli sono mutuati dai "critical security controls" (CSC) del Center for Internet Security (CIS).

Le misure sono **obbligatorie** per le pubbliche amministrazioni.

I controlli sono suddivisi in **3 livelli**:

- Minimo: controlli obbligatori per tutte le P.A.
- Standard: il livello che tutte le P.A. dovrebbero ottenere
- Alto: l'obiettivo a cui le P.A. devono tendere

# MISURE AGID: NON SOLO PER LE PA

Le "misure minime" AgID sono valide per qualsiasi organizzazione

Sono necessarie per avere il governo:

- dei sistemi informatici
- dei dati
- dell'operato delle persone su sistemi e dati

Sono **misure organizzative** prima che tecniche.

# MISURE TECNICHE "PERSONALI"

**Ciascuno di noi, sui propri dispositivi, ha la responsabilità di:**

- Controllo accessi
- Cifratura dei dati (encryption)
- Aggiornamento del software (patching)
- Installazione da fonti note / autorizzate

# MINACCE NON TECNOLOGICHE

## Minacce che sfruttano le persone

- Messaggi con mittente contraffatto
- Creano pressione e urgenza
- Fanno leva sulla paura
- Inducono la vittima ad agire precipitosamente per **aggirare le misure di sicurezza**

# MINACCE NON TECNOLOGICHE: DIFENDERSI

## Verificare il messaggio

- Se è personale: **contattare** il mittente dichiarato, usando un **canale diverso** rispetto a quello da cui arriva il messaggio
- Se è inoltrato, riferito, o se appare in un sito o app: **verificare** l'attendibilità **su fonti autorevoli**

