Fastweb Digital Academy

COME PROTEGGERE I DATI PERSONALI NEGLI AMBIENTI DIGITALI

Docente
Raoul Brenna

PROTEGGERE IL DATO PERSONALE DIGITALE

Valutare i rischi

01 Sapere dov'è il dato

Attraverso un continuo processo di inventory e meccanismi tecnologici e organizzativi di prevenzione della proliferazione incontrollata.

02 Regolare chi accede

Sia ai locali fisici, che mediante accessi logici ai sistemi su cui i dati sono ospitati o processati. Identificazione, autenticazione, autorizzazione.

03 Memorizzazione e trasporto

Protezione del dato dall'alterazione delle sue proprietà RID, sia quando esso è memorizzato (o elaborato) sui sistemi che quando è in transito tra essi.

04 Copie di sicurezza protette

Meccanismi di backup del dato che siano quanto più possibile ridondati, protetti e a prova di attacco da parte di "ransomware" o altre violazioni.

Monitorare gli eventi

F D A
Fastweb Digital Academy

CENSIMENTO

Sapere dov'è il dato

- Trattamenti vs. dati.
- Dati master vs. repliche vs. copie temporanee.
- Server, database, cloud, ecc.
- Copie di lavoro e comunicazioni (allegati, estrazioni, ecc.).
- Analisi, correlazioni, dati derivati, ecc.

F D A
Fastweb Digital Academy

CONTROLLO ACCESSI

Regolare chi accede

- Ownership del dato.
- Gestione degli utenti e delle identità.
- Credenziali robuste su sistemi e applicazioni.
- Autenticazione a più fattori.
- Accessi controllati ai locali.
- Autorizzazione e privilegio minimo.

Fastweb Digital Academy

CIFRATURA / MASKING

Memorizzazione e trasporto

- Cifratura del dato in transito (TLS, IPSec, ...).
- Cifratura del dato "at rest" (memorizzato su server o dispositivi utente).
- Cifratura del file system, del database o a livello applicativo.
- Anonimizzazione (vs.) pseudonimizzazione.
- Mascheramento e oscuramento (a livello di dato salvato o di interfaccia).

F D A
Fastweb Digital Academy

BACKUP

Copie di sicurezza protette

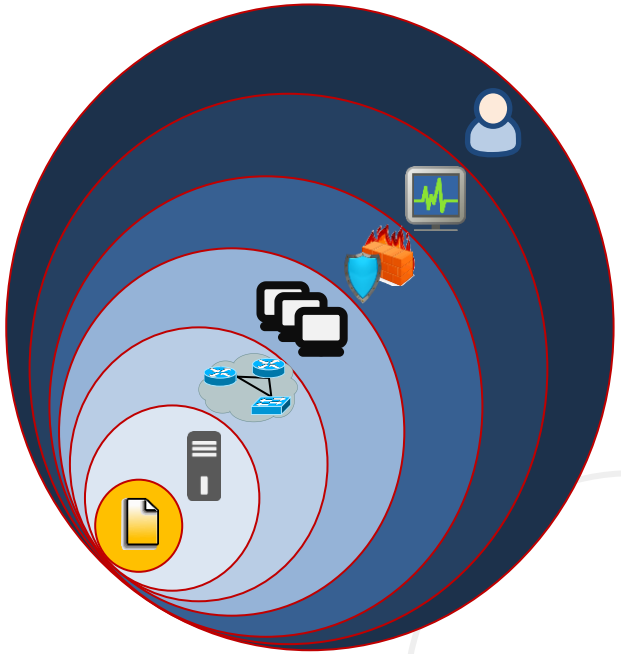
- Disconnessi dalla rete (offline) salvo quando necessario.
- Cifrati, con adeguata gestione delle chiavi.
- Aggiornati e ridondati su più copie e tecnologie.
- Con rigoroso controllo degli accessi.
- Effettuati tramite utenze appropriate.

F D A
Fastweb Digital Academy

LA SICUREZZA DELL'ANELLO DEBOLE E LA NECESSITÀ DI UNA DIFESA A STRATI

+

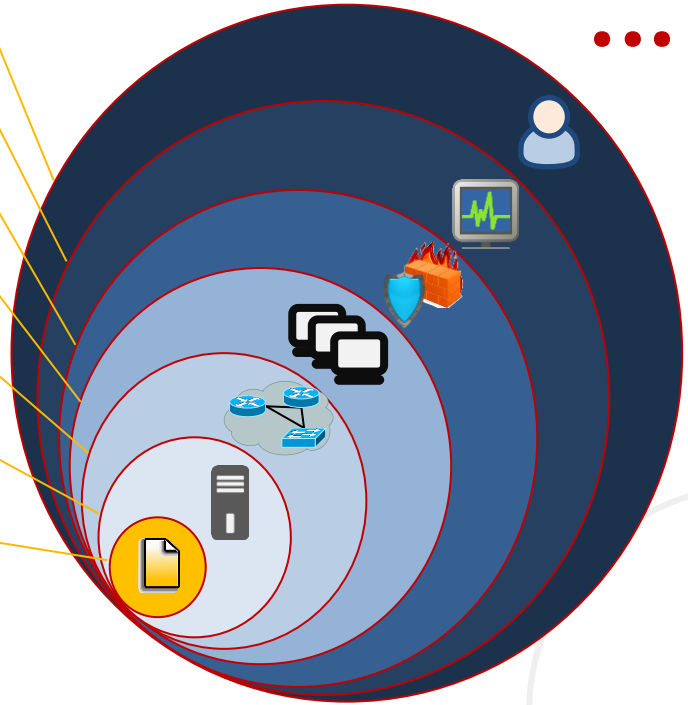
=



F D A
Fastweb Digital Academy

LA SICUREZZA DELL'ANELLO DEBOLE E LA NECESSITÀ DI UNA DIFESA A STRATI

- Awareness e "cyber-hygiene" verso le persone. Alert tempestivi. Gestione delle identità.
- Raccolta, correlazione e monitoraggio degli eventi sui sistemi. Presidio della "security posture".
- Filtraggio dei contenuti a tutti i livelli.
- Protezione dei terminali, della navigazione e delle applicazioni. Gestione delle utenze e controllo accessi.
- Reti protette a livello fisico, topologico e logico. Cifratura e rilevazione delle minacce.
- Datacenter protetti e sicurezza di sistemi e architetture (inclusi evoluzione, aggiornamento, fix di sicurezza, ecc.)
- Garantire le proprietà di sicurezza (RID e altre) del dato, e classificarlo opportunamente.

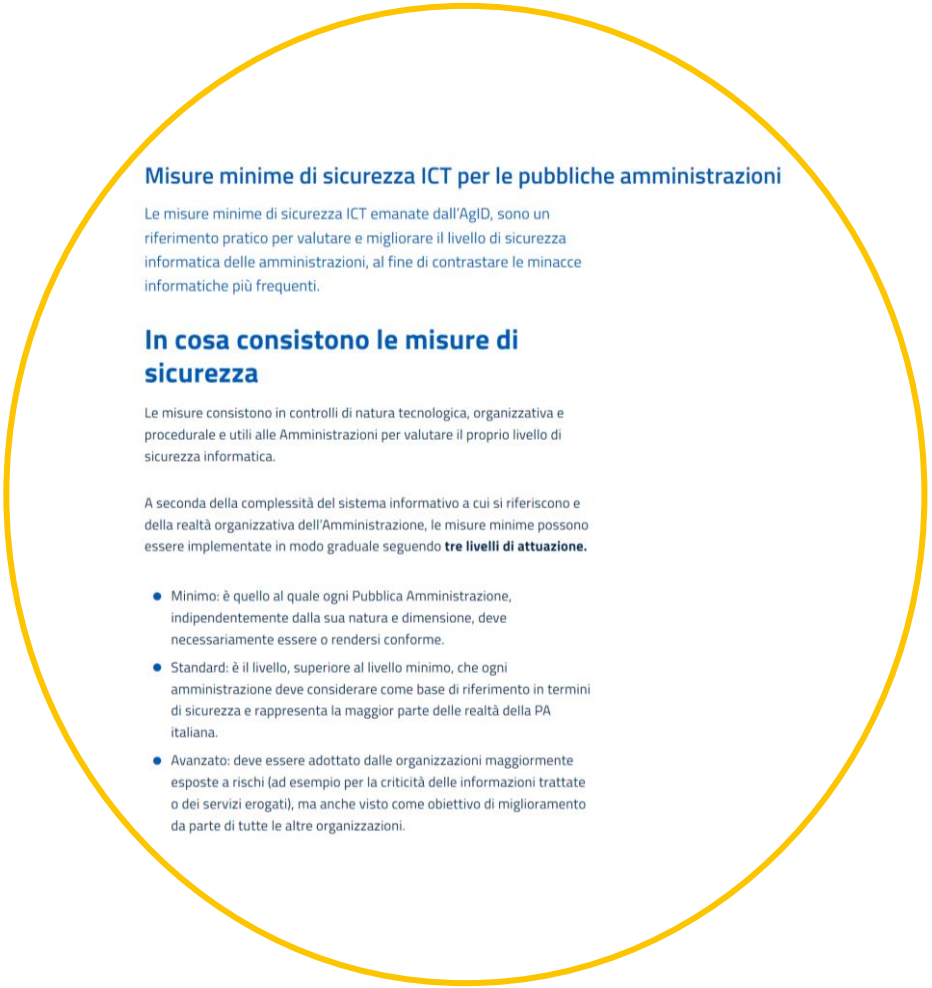


Fastweb Digital Academy

UN AIUTO DA AGID

Misure minime di sicurezza ICT per le pubbliche amministrazioni

- Un riferimento operativo direttamente utilizzabile (checklist).
- Una base comune di misure tecniche ed organizzative irrinunciabili.
- Utili per aumentare la protezione contro le minacce informatiche.
- Responsabilizzano le Amministrazioni sul mantenimento di un'adeguata cybersecurity posture.



Misure minime di sicurezza ICT per le pubbliche amministrazioni

Le misure minime di sicurezza ICT emanate dall'AgID, sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti.

In cosa consistono le misure di sicurezza

Le misure consistono in controlli di natura tecnologica, organizzativa e procedurale e utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica.

A seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, le misure minime possono essere implementate in modo graduale seguendo **tre livelli di attuazione.**

- Minimo: è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.
- Standard: è il livello, superiore al livello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della PA italiana.
- Avanzato: deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

F D A
Fastweb Digital Academy