Sicurezza informatica nel luogo di lavoro PA Parte II

prof. Monica Palmirani

Sicurezza

- Sicurezza dell'autenticazione dei soggetti attori
  - autenticazione
- Sicurezza degli applicativi
  - autorizzazione e sicurezza degli applicativi WEB
- Sicurezza dell'integrità del dato
  - es. virus
- Sicurezza del sistema di rete
  - firewall e proxy
- Sicurezza del canale di trasmissione
  - es. VPN
- Sicurezza del computer
  - es. policy di password
- Sicurezza dei dispositivi
  - dischi e mobile

Smart working

Le 11 raccomandazioni di AgID per uno Smart working sicuro

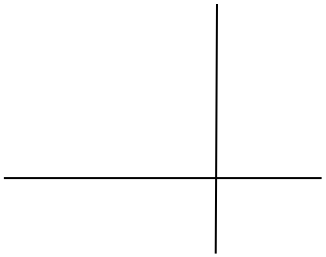
1. - Segui prioritariamente le policy e le raccomandazioni dettate dalla tua Amministrazione
2. - Utilizza i sistemi operativi per i quali attualmente è garantito il supporto
3. - Effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo
4. - Assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati
5. - Assicurati che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla tua Amministrazione

Le 11 raccomandazioni di AgID per uno Smart working sicuro

6. - Non installare software proveniente da fonti/repository non ufficiali
7. - Blocca l’accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro
8. - Non cliccare su link o allegati contenuti in email sospette
9. - Utilizza l’accesso a connessioni Wi-Fi adeguatamente protette
10. - Collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione)
11. - Effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.

Sicurezza nello smart working della PA

- Direttiva n. 1/2020 **Dipartimento della Funzione Pubblica** prevede la possibilità di utilizzare i propri devices (pc, tablet, smartphone) per il lavoro remoto e agile e definisce i livelli di sicurezza e protezione della rete



Mobile

- Bring your own device – proprietà del dipendente che lo usa anche per scopi di lavoro
- Choose-your-own-device – proprietà della PA e uso solo per scopi di lavoro
- Corporate-owned, personally-enabled - proprietà della PA ed è consentito un uso misto

Cosa serve?

- Disciplinare
- Separazione dati private e pubblici
- Garanzia di protezione dei dati dei cittadini e della PA
- Garanzia del segreto d’ufficio
- Protezione della proprietà intellettuale
- **ISO/IEC 27002:13**

Cosa fare?

- Antivirus
- Aggiornare sempre i sistemi operativi
- Aggiornare sempre gli applicativi
- Fare backup costanti
- Autenticarsi e chiudere le sessioni di lavoro
- Depositare il lavoro concluso in cloud
- Crittografia