OPERAZIONI DI AUDIT DI SICUREZZA INFORMATICA

VERIFICARE PER LE SINGOLE POSTAZIONI:

1. ☐ Tipologia di apparato informatico
2. ☐ Sistema Operativo Versione e Build
3. ☐ CPU (gen) & RAM (gen)
4. ☐ Tipologia e versione di Office Application
5. ☐ Tipologia di Antivirus
6. ☐ Tipologia di Software Teleassistenza
7. ☐ Tipologia di Connettività

VERIFICARE PER L'INFRASTRUTTURA:

1. ☐ Tipologia di connessione
2. ☐ Tipologia di router
3. ☐ Tipologia di Telefonia
4. ☐ Tipologia e modello di apparati di backup e/o di NAS di rete
5. ☐ Tipologia di reti presenti (es. Lan, WiFi, altro)
6. ☐ Sistemi di continuità energetica
7. ☐ Tipologia e modelli di stampanti e scanner
8. ☐ Esistenza di Sistemi di Video Sorveglianza connessi alla Rete
9. ☐ Tipologia e modello di apparati Voip (compreso centralini Telefoni, altoparlanti, video citofoni o altro)
10. ☐ Tipologia e modello di server ove presenti
11. ☐ Tipologia e modello di Apparati di rete quali switch o affini ove presenti

VADEMECUM OPERAZIONI DI AUDIT DI SICUREZZA FISICA

VERIFICARE RISCHI FISICI:

1. ☐ Cavetteria delle postazioni
2. ☐ Elettrificazione delle postazioni
3. ☐ Qualità dell'impiantistica telematica (ove presente un impianto di rete diffuso)
4. ☐ Congruità dell'ubicazione degli apparati centralizzanti quali: server, switch, NAS, router e altro affine
5. ☐ Controllo delle caratteristiche di continuità elettrica a livello di macro struttura informatica per gli apparati centralizzanti
6. ☐ Verifica dell'esistenza di sicurezze d'accesso fisici ai luoghi di particolare delicatezza a livello di apparecchiature informatiche
7. ☐ Verificare se per gli apparati esistono rischi: da inondazione, incendio e/o terremoto. Nel caso siano state prese in considerazione tali eventualità verificare e documentare le soluzioni attuate.

Staff SYNAPSE