Check list per la sicurezza informatica

1. È stato affidato a persona o società specializzata l'incarico di occuparsi di sicurezza informatica?

   Sì ☐ No ☐

   Note: _____

2. È stato effettuato e aggiornato un inventario dei componenti *server*, *client* e degli altri apparati condivisi (stampanti, macchinari di produzione in rete, etc.)[1]?

   Sì ☐ No ☐

   Note: _____

3. La protezione perimetrale è stata attuata?

   Sì ☐ No ☐

   Note: _____

4. I sistemi operativi e i programmi installati e/o utilizzati su *server* e *client* sono aggiornati e protetti?

   Sì ☐ No ☐

   Note: _____

5. I profili utente sono differenziati per l'accesso alle risorse di rete?

   Sì ☐ No ☐

   Note: _____

6. Sono state messe a disposizione dei lavoratori in *smart working* e di coloro che si debbono collegare alla rete aziendale collegamenti VPN affidabili e ben configurati?

   Sì ☐ No ☐

   Note: _____

[1] Ad esempio: Quali asset ITC sono presenti in azienda? Dove sono dislocati? Chi sono gli utilizzatori e in che modo sono utilizzati? Quanto sono costati, quanto valgono ora e quanto costerebbe sostituirli? Quando sono da sostituire o eventualmente da aggiornare?

7. La posta elettronica è protetta da *antivirus*, *antispam*, etc.?

   Sì ☐ No ☐

   Note: _____

8. La rete aziendale è convenientemente segmentata (è opportuno che i macchinari *IOT*, con proprio sistema operativo, non siano in linea con *server* e *client*)?

   Sì ☐ No ☐

   Note: _____

9. Fotocopiatrici e stampanti sono protette? Sono dietro al firewall? I firmware sono aggiornati?

   Sì ☐ No ☐

   Note: _____

10. I *backup* sono effettuati con regolarità?

    Sì ☐ No ☐

    Note: _____

11. Vi è ridondanza di copie?

    Sì ☐ No ☐

    Note: _____

12. È tenuto in debita considerazione il fatto che la nuova generazione di *ransomware* è programmata per criptare innanzitutto le copie di *backup*?

    Sì ☐ No ☐

    Note: _____

13. Viene effettuata congrua verifica sulla affidabilità delle copie di *backup*?

    Sì ☐ No ☐

    Note: _____

14. Nel caso di perdita di dati conseguente ad attacco o incidente è ragionevolmente sicura la possibilità di ripristinare la disponibilità dei dati nella loro integrità?

    Sì ☐ No ☐

    Note: _____

15. Sono installati *Firewall, Antivirus, IDS/IPS* tecnologicamente avanzati e ben configurati?

    Sì ☐ No ☐

    Note: _____

16. Vi sono altri strumenti di protezione?

    Sì ☐ No ☐

    Note: _____

17. I profili utente sono differenziati per l'accesso alle risorse di rete?

    Sì ☐ No ☐

    Note: _____

18. Vi è una *policy* aziendale in materia di trattamento dei dati? È prevista una *password policy*?

    Sì ☐ No ☐

    Note: _____

19. I servizi web (ad es. sito web, social network, servizi cloud, posta elettronica, spazio web) sono gestiti da terze parti affidabili?

    Sì ☐ No ☐

    Note: _____

20. Il personale è stato opportunamente informato e formato in materia di sicurezza informatica?

    Sì ☐ No ☐

    Note: _____

21. È stato istituito un piano di Disaster Recovery e di continuità del business?

    Sì ☐ No ☐

    Note: _____