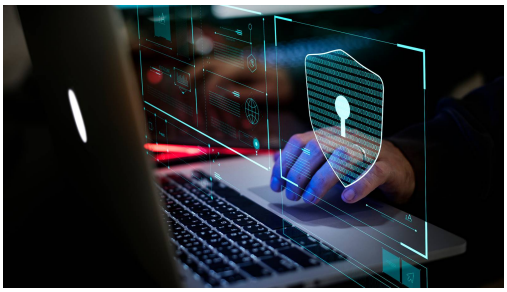

IFCT0024. Ciberseguridad para usuarios.

Sku: PS_IFCT0024

Horas: 10

Formato: HTML

OBJETIVOS

- Valorar la necesidad de la gestio?n de la seguridad en las organizaciones.
- Distinguir las principales amenazas a los sistemas de informacio?n e identificando las principales herramientas de seguridad y su aplicacio?n en cada caso.

CONTENIDOS

- **Conocimientos / Capacidades cognitivas y prácticas.**
  - Aproximacio?n a la seguridad en sistemas de informacio?n:
  - Asimilacio?n de conceptos de seguridad en los sistemas:
    - Clasificacio?n de las medidas de seguridad.
    - Conocimiento acerca de los requerimientos de seguridad en los sistemas de informacio?n.
    - Identificacio?n de principales caracteri?sticas.
    - Confidencialidad.
    - Gestio?n de la integridad.
    - Comprensio?n de la disponibilidad.
    - Identificacio?n de otras caracteri?sticas.
    - Identificacio?n de tipos de ataques.
  - Conocimiento del a?mbito de la Ciberseguridad para usuarios:
    - Comprensio?n del concepto de ciberseguridad.
    - Identificacio?n de amenazas ma?s frecuentes a los sistemas de informacio?n.
    - Utilizacio?n de tecnologi?as de seguridad ma?s habituales.
    - Gestio?n de la seguridad informa?tica.
  - Identificacio?n de softwares dan?inos:
    - Asimilacio?n de conceptos sobre software dan?ino.
    - Clasificacio?n del software dan?ino.

        - Identificacio?n de amenazas persistentes y avanzadas.
        - Prevencio?n sobre la ingenieri?a social y redes sociales.
    - Gestio?n de seguridad en redes inala?mbricas.
    - Aplicacio?n de herramientas de seguridad:
        - Aplicacio?n de medidas de proteccio?n.
        - Control de acceso de los usuarios al sistema operativo.
        - Gestio?n del permiso de los usuarios.
        - Gestio?n del registro de usuarios.
        - Autentificacio?n de usuarios.
        - Gestio?n segura de comunicaciones, carpetas y otros recursos compartidos.
        - Gestio?n de carpetas compartidas en la red.
        - Identificacio?n de tipos de accesos a carpetas compartidas.
        - Procedimiento para compartir impresoras.
        - Proteccio?n frente a co?digo malicioso.
        - Configuracio?n del antivirus.
        - Configuracio?n del cortafuegos (firewall).
        - Aplicacio?n del antimalware.

- **Habilidades de gestión, personales y sociales.**
    - Identificacio?n de las ciberamenazas y formas de fomentar la ciberseguridad en el comercio electro?nico.
    - Buenas pra?cticas para mejorar la confianza de los clientes.
    - Actuacio?n ante un incidente de seguridad.