Glosario - Módulo 6: Seguridad digital y protección de datos

Ciberseguridad: Conjunto de medidas para proteger sistemas informáticos y redes frente a ataques o accesos no autorizados.

Malware: Software malicioso diseñado para dañar o acceder sin permiso a un sistema.

Phishing: Técnica de engaño para obtener información confidencial haciéndose pasar por una entidad legítima.

Auditoría de seguridad: Proceso de revisión y análisis de los sistemas informáticos para detectar vulnerabilidades.

RGPD: Reglamento General de Protección de Datos, normativa europea que regula el tratamiento de datos personales.

Protección de datos: Conjunto de prácticas para garantizar la privacidad y seguridad de la información personal.

Copia de seguridad: Duplicado de los datos almacenados para poder recuperarlos en caso de pérdida o daño.

Firewall: Sistema que controla el tráfico de red y bloquea accesos no autorizados.

Antivirus: Programa que detecta y elimina software malicioso en un dispositivo.

Vulnerabilidad: Debilidad en un sistema que puede ser explotada por un atacante.

Ciberataque: Acción deliberada para dañar, robar o interrumpir sistemas informáticos.

Plan de contingencia: Conjunto de medidas preparadas para actuar en caso de un incidente de seguridad.

Encriptación: Proceso de codificar información para que solo pueda ser leída por quien tenga la clave.

Autenticación de dos factores (2FA): Método de verificación que requiere dos pruebas de identidad para acceder a un sistema.

Respuesta a incidentes: Conjunto de acciones para gestionar y solucionar un ataque o fallo de seguridad.