Glosario de Ciberseguridad

- **Ciberataque**: Intento malicioso de vulnerar un sistema, dispositivo o red para robar información o causar daño.

- **Ciberdelincuentes**: Personas u organizaciones que realizan ataques digitales con fines de fraude, robo o espionaje.

- **Sospecha digital**: Hábito de desconfiar de correos, links o mensajes sospechosos como primera barrera de defensa.

- **Ingeniería social**: Estrategia de manipulación en la que el atacante se aprovecha de la información pública de una persona para engañarla.

- **Phishing**: Estafa en la que se envían correos o mensajes falsos que imitan entidades legítimas para robar datos.

- **Malware**: Software malicioso que se instala en un dispositivo sin permiso para espiar, robar o dañar información.

- **Ransomware**: Tipo de malware que “secuestra” archivos o sistemas y pide un pago (rescate) para liberarlos.

- **VPN (Red Privada Virtual)**: Herramienta que cifra la conexión a internet y protege la privacidad al usar redes públicas.

- **Doble autenticación (2FA)**: Método de seguridad que requiere un segundo paso además de la contraseña (código SMS, huella, app).

- **Gestor de contraseñas**: Aplicación que guarda y organiza claves seguras, evitando repetirlas o olvidarlas.

- **Actualizaciones de seguridad**: Cambios en software o sistemas que corrigen vulnerabilidades y reducen riesgos.

- **Antivirus**: Programa diseñado para detectar y bloquear virus, malware y otras amenazas digitales.

- **Checklist de seguridad personal**: Lista de pasos básicos para asegurar cuentas, dispositivos y hábitos digitales.