Aplicar Buenas Prácticas en el Uso de TIC Garantizando Seguridad y Privacidad

En la era digital, la seguridad y privacidad en el uso de las Tecnologías de la Información y Comunicación (TIC) son más cruciales que nunca. Esta presentación explorará las amenazas, las medidas preventivas y las buenas prácticas esenciales para proteger nuestra información y nuestra identidad en el ciberespacio.

¿Qué es la Seguridad y Privacidad en las TIC?

Protección Integral

Se refiere a salvaguardar la información y a las personas de amenazas digitales, asegurando un entorno seguro para la interacción en línea.

Principios Fundamentales

Garantizar la confidencialidad, integridad y disponibilidad de los datos es crucial para evitar manipulaciones o pérdidas.

Prevención de Riesgos

Evita el robo de identidad, el acoso digital y la pérdida de información personal o sensible.

Amenazas Más Comunes en el Uso de TIC

Las amenazas digitales son diversas y están en constante evolución. Conocerlas es el primer paso para protegernos eficazmente.

- **Ciberacoso y Grooming:** *Riesgos específicos para menores, incluyendo el acoso en línea y el engaño para fines de explotación.*
- **Malware y Ataques:** *Virus, ransomware y otros programas maliciosos diseñados para robar, dañar o destruir datos.*
- **Usurpación de Identidad:** *Robo de datos personales para cometer fraudes o acceder a cuentas sin autorización.*
- **WiFi Públicas Inseguras:** *Riesgo de que terceros capturen datos (sniffers) en redes no protegidas.*

Puertas de Entrada de las Amenazas

Factores Externos

Desastres naturales como inundaciones o terremotos pueden afectar la infraestructura tecnológica y causar pérdida de datos.

Vulnerabilidades Técnicas

La falta de actualizaciones, sistemas obsoletos o configuraciones inadecuadas exponen a los datos y sistemas.

Factor Humano

Errores no intencionados, falta de concienciación o acciones malintencionadas de usuarios internos o externos.

Medidas Clave para Garantizar Seguridad y Privacidad

Implementar estas medidas es fundamental para una protección robusta.

1

Control de Acceso

Utiliza contraseñas fuertes y la autenticación de dos factores para proteger tus cuentas.

2

Actualizaciones y Antimalware

Mantén tus sistemas y software actualizados y usa herramientas antimalware fiables.

3

Concienciación

Capacita a los usuarios en buenas prácticas y riesgos para crear una cultura de seguridad.

4

Copias de Seguridad

Realiza copias de seguridad periódicas de tus datos y protege físicamente tus dispositivos.

Buenas Prácticas en Redes Sociales

- **Configuración de Privacidad:** *Revisa y ajusta las opciones de privacidad de tu perfil y publicaciones regularmente.*
- **Datos Personales:** *Evita compartir información sensible como tu dirección, número de teléfono o documentos de identidad.*

- **Contactos Desconocidos:** *No aceptes solicitudes de amistad de personas que no conoces y limpia contactos sospechosos periódicamente.*
- **Geolocalización:** *Desactiva la función de geolocalización en tus publicaciones para proteger tu ubicación.*

Uso Seguro de Dispositivos y Navegación

Tu comportamiento en línea y el uso de tus dispositivos son clave para tu seguridad.

Evita Redes WiFi Abiertas

Las redes públicas no seguras son un foco de espionaje. Usa VPN si es imprescindible conectarse a ellas.

Cuidado con Enlaces Sospechosos

No hagas clic en enlaces o descargues archivos de fuentes desconocidas para evitar malware.

Software Aprobado

Descarga solo software y aplicaciones de tiendas oficiales y fuentes de confianza.

Cubre tu Cámara

Tapa la cámara de tus dispositivos cuando no la uses para evitar posibles accesos no autorizados.

Políticas y Normativas para la Protección en TIC

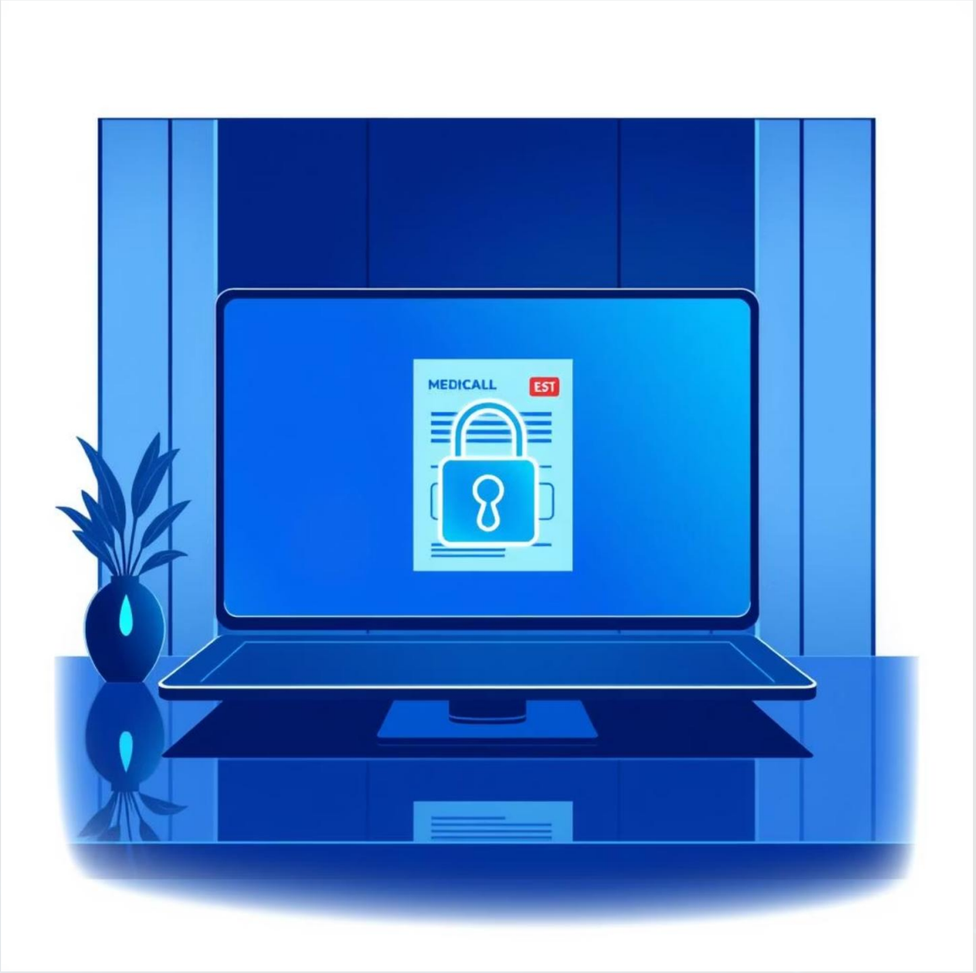
El marco legal y las políticas internas son esenciales para la protección de datos.

Conocimiento Legal	*Familiarízate con normativas como GDPR, FERPA o COPPA, según el contexto de tu organización.*
Políticas Internas	*Implementa políticas claras de uso aceptable y privacidad para todos los empleados o usuarios.*
Formación Continua	*Capacita a docentes, empleados y usuarios en el manejo responsable de datos y sistemas.*
Supervisión y Auditoría	*Realiza auditorías regulares para asegurar el cumplimiento de las políticas y detectar posibles brechas.*

Caso Real: Sector Salud y Ciberseguridad

Los datos médicos son extremadamente sensibles y representan un objetivo prioritario para los ciberatacantes. Un ataque exitoso en este sector puede tener consecuencias devastadoras, no solo en términos de robo de identidad o fraude, sino también afectando la vida y la seguridad de los pacientes.

> *La* **Confidencialidad**, **Integridad** *y* **Disponibilidad** *(CIA) de la información son pilares esenciales para la confianza y la seguridad en la atención médica. Es vital establecer protocolos estrictos y una formación continua para proteger estos datos críticos.*



Conclusión: Tu Papel en la Seguridad y Privacidad TIC

Primera Línea de Defensa

Eres el factor más importante. Tu concienciación y buenas prácticas son clave para protegerte.

Responsabilidad Digital

Protege tu información y la de los demás con un manejo responsable de los datos.

Cultura de Privacidad

Adopta hábitos seguros y promueve una cultura de privacidad y seguridad en tu entorno.

Juntos podemos crear un entorno digital más seguro para todos.