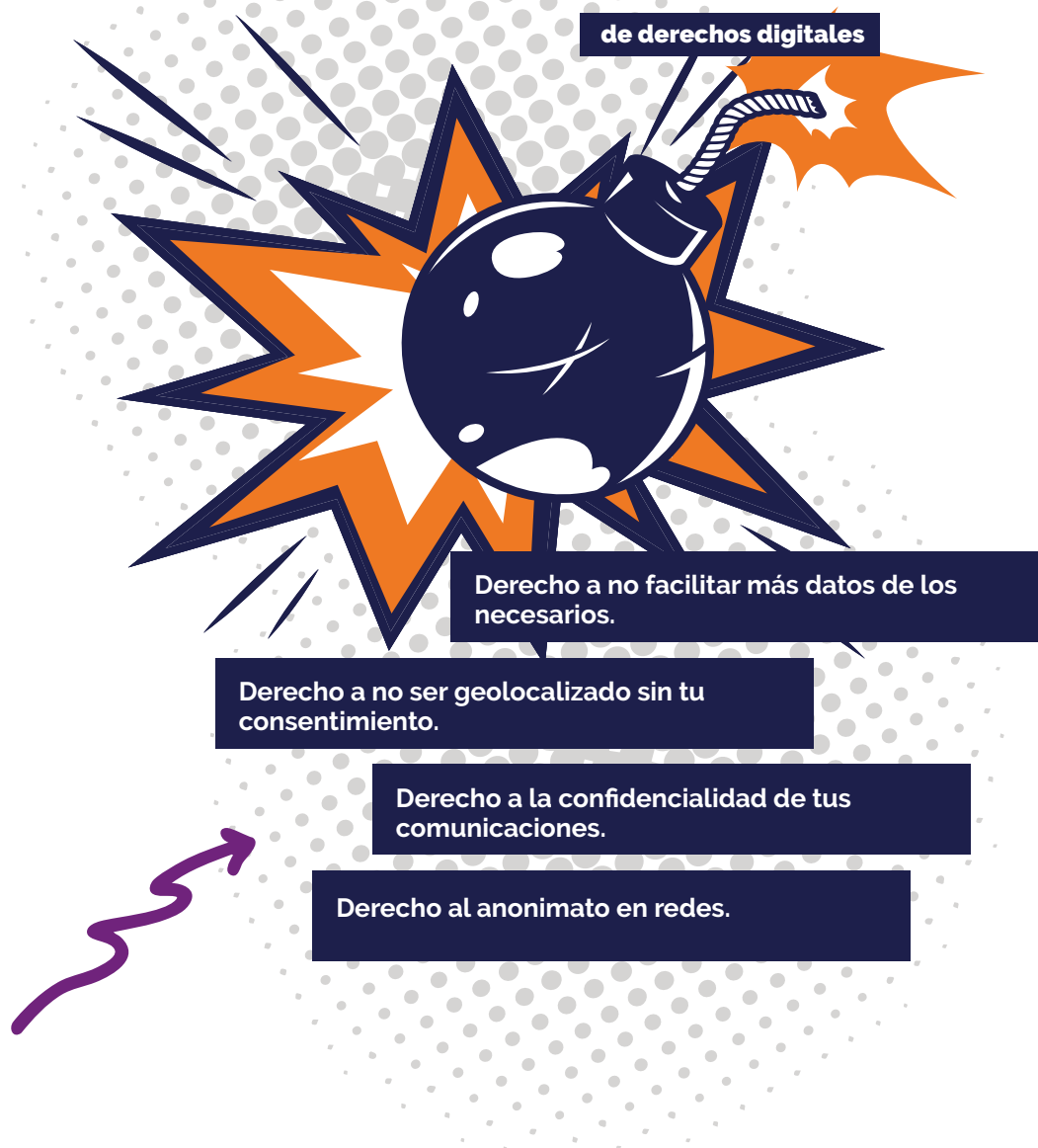


TUS DERECHOS
SEGÚN LA

CARTA

de derechos digitales



Ciberseguridad cotidiana

Hoy vivimos conectados todo el tiempo: compartimos fotos, ubicaciones, gustos y hasta rutinas sin pensarlo demasiado. Pero ¿sabías que cada clic, cada app y cada permiso que aceptas dice mucho sobre ti? En internet, tus datos personales son una especie de "moneda" muy valiosa, y protegerlos no solo es una cuestión técnica, sino una forma de cuidar tu identidad y tu privacidad.

La buena noticia es que mantenerte seguro en el mundo digital no es tan complicado. Revisar los permisos de tus aplicaciones, crear contraseñas fuertes, evitar el Wi-Fi público y mantener tus dispositivos actualizados puede marcar la diferencia. Ser consciente de lo que compartes no significa desconectarte del mundo, sino usar la tecnología con inteligencia. En definitiva, se trata de disfrutar de lo digital sin perder de vista tu seguridad.

Ciberseguridad cotidiana

El 70 % de los usuarios de redes sociales acepta permisos sin leer las condiciones (Comisión Europea, 2021).

EXCESO DE PERMISOS

- **Aplicaciones que piden acceso a cámara, micrófono o ubicación sin justificación real.**

SIEMPRE ES MEJOR SI...

- Revisas y limitas los permisos de las aplicaciones que usas.

9 de cada 10 internautas en Europa reconocen que han compartido más datos personales de los necesarios al usar aplicaciones o servicios digitales (Eurobarómetro, 2022).

FALTA DE CONTROL EN LA IDENTIDAD DIGITAL

- **Compartir datos en exceso facilita la suplantación o el fraude.**

RIESGO EN REDES PÚBLICAS

- **El uso de Wi-Fi abiertas facilita el robo de datos.**

SIEMPRE ES MEJOR SI...

- Mantienes el sistema operativo y las aplicaciones siempre actualizadas.
- Verificas que los sitios web empiecen con "https://" antes de introducir datos personales. Debe llevar la "s" de https.
- No compartes tus contraseñas y las cambias con regularidad.

En 2024, más de 65.000 ciudadanas y ciudadanos fueron víctima de ciberataques (Incibe, 2024).

CIBERATAQUES Y VULNERABILIDADES

- **Sistemas desactualizados se convierten en puertas de entrada.**
- **Contraseñas fáciles de adivinar o reutilizadas en varios servicios.**

SIEMPRE ES MEJOR SI...

- Priorizas actualizaciones críticas de seguridad.
- Deshabilitas cuentas y servicios innecesarios.
- Mantienes copias de seguridad desconectadas.
- Creas contraseñas fuertes y diferentes para cada servicio (puedes apoyarte en un gestor de contraseñas).
- Evitas conectarte a redes Wi-Fi públicas para transacciones sensibles.

PALABRAS CLAVE PARA ENTENDER Y AMPLIAR

Antivirus y antispyware

Programas diseñados para detectar, bloquear y eliminar virus y software espía de los sistemas.

Autenticación de doble factor (2FA)

Método de seguridad que requiere dos formas de verificación para acceder a una cuenta o sistema.

Ciberseguridad

Conjunto de medidas, técnicas y políticas destinadas a proteger sistemas, datos y redes frente a ataques digitales.

Datos biométricos

Información única de tu cuerpo (huella, rostro, voz) usada para identificarte.

Geolocalización

Determinación de la ubicación física de un dispositivo o usuario mediante tecnologías digitales.

Gestor de contraseñas

Herramienta que almacena y genera contraseñas seguras.

Higiene digital

Conjunto de hábitos y prácticas que garantizan un uso seguro, responsable y saludable de la tecnología.

Huella digital activa y pasiva

Registro de información que una persona deja en línea: activa (lo que publica) y pasiva (lo que generan otros sobre ella o sistemas).

Identidad digital

Conjunto de información, perfiles y acciones que representan a una persona en entornos digitales.

HTTPS

Protocolo que cifra la comunicación entre el navegador y la web, proporcionando una navegación segura.

Malware

Software malicioso diseñado para dañar, infiltrarse o robar información de sistemas y dispositivos.

Phishing

Técnica de engaño para robar datos personales haciéndose pasar por una fuente confiable.

Privacidad digital

Derecho y capacidad de controlar qué información personal se comparte y quién puede acceder a ella en línea.

Vulnerabilidad

Debilidad en un sistema digital que puede ser explotada por atacantes para acceder, dañar o robar información.