

Módulo 6: Protección de Datos Sensibles

El blog “ciberseguridad para principiantes” te invita a participar en este módulo. En este módulo, profundizaremos en la protección de datos sensibles, proporcionando recursos adicionales, enlaces a artículos relevantes, ejemplos prácticos y noticias recientes para ilustrar la importancia de este tema.

Guía Práctica para Mantener tus Datos Seguros en Internet

¿Por qué es tan importante la protección de datos?






Cada día se generan y transfieren millones de datos personales en internet: contraseñas, información financiera, documentos confidenciales, imágenes privadas, correos electrónicos, etc. Si estos datos caen en las manos equivocadas, pueden ser utilizados para **robo de identidad, fraude, extorsión o incluso espionaje digital**.

Como experto en ciberseguridad, mi misión es enseñarte cómo **proteger tu privacidad y seguridad online**, implementando **hábitos efectivos y herramientas confiables** para blindar tus datos contra ataques y filtraciones.

Identifica los datos sensibles que manejas

Antes de protegerte, necesitas **identificar qué datos personales y sensibles estás exponiendo** sin darte cuenta.


Ejemplo de datos que debes proteger:


-  Información personal: Nombre, dirección, teléfono, fecha de nacimiento.
-  Datos bancarios: Tarjetas de crédito, cuentas bancarias, historial de transacciones.
-  Credenciales: Contraseñas, respuestas de seguridad, PINs.
-  Datos médicos: Historias clínicas, diagnósticos, recetas electrónicas.
-  Archivos privados: Fotos, documentos legales, contratos laborales.

Ejemplo real:

En 2021, **Facebook sufrió una brecha de datos** donde se filtraron los teléfonos, nombres y correos electrónicos de 533 millones de personas. Estos datos fueron vendidos en foros de ciberdelincuentes y usados en ataques de **phishing y suplantación de identidad**.

Herramienta útil:

¿Tus datos han sido filtrados en internet?  Verifícalo en [Have I Been Pwned](https://haveibeenpwned.com/).



 **Tarea:** Ingresa tu correo en Have I Been Pwned y revisa si ha sido comprometido. Si es así, **cambia tus contraseñas inmediatamente** y activa la autenticación en dos pasos (2FA).

Minimiza la exposición de tus datos personales

Norma de oro en ciberseguridad:

 **“Si un dato no es necesario, NO lo compartas”.**

Cómo reducir tu exposición en internet:

-  No publiques información sensible en redes sociales (ubicación, viajes, teléfono).
-  Usa **correos electrónicos temporales** para registros en sitios desconocidos.

Módulo 6: Protección de Datos Sensibles

 Revisa y **limita permisos de aplicaciones y extensiones de navegador**.

 Borra cuentas antiguas que ya no usas.

 **Ejemplo de mal hábito digital:**

✗ Muchas personas publican en Facebook: “¡Me voy de vacaciones una semana! 🌴 ✈️”

✓ **Solución: Publica las fotos después del viaje.** Así evitarás alertar a delincuentes sobre tu ausencia.

 **Herramienta útil:**

 [JustDeleteMe](#) – Para eliminar cuentas en servicios online.

3 Fortalece la seguridad de tus contraseñas y accesos

Tu **contraseña es la primera barrera** contra ciberdelincuentes. Sin embargo, el **82% de los ataques exitosos** ocurren debido al uso de **contraseñas débiles** o repetidas.


✓ **Reglas para una contraseña segura:**

- ◆ Mínimo **12 caracteres** (mayúsculas, minúsculas, números y símbolos).
- ◆ Nunca uses datos personales como tu nombre, fecha de nacimiento o teléfono.
- ◆ No repitas contraseñas en varias cuentas.
- ◆ Usa un **gestor de contraseñas** para generar y almacenar claves seguras.

 **Herramientas recomendadas:**

 [Bitwarden](#) – Gestor de contraseñas gratuito y seguro.

 [LastPass](#) – Almacena y genera contraseñas automáticamente.

 **Tarea:** Descarga **Bitwarden** y almacena al menos **tres contraseñas críticas** (banco, correo y redes sociales).

4 Habilita la autenticación en dos pasos (2FA)

◆ **¿Qué es el 2FA?**

Es una capa adicional de seguridad que solicita un código extra para acceder a tu cuenta, además de la contraseña.

 **Ejemplo práctico:**

Si intentas iniciar sesión en Gmail desde otro dispositivo, Google te pedirá un código enviado a tu teléfono o generado por una app autenticadora.

 **Apps recomendadas para 2FA:**

✓ **Google Authenticator** (Android)

✓ [Authy](#) – Guarda códigos en la nube y permite recuperación fácil.

 **Tarea:** Activa 2FA en **Gmail, Facebook y tu banco**.

5 Cifra tu información confidencial

Módulo 6: Protección de Datos Sensibles

📌 ¿Por qué es importante cifrar tus archivos?

Si un hacker accede a tu disco duro o pendrive, puede robar documentos privados. **El cifrado hace que la información sea ilegible sin la clave correcta.**

◆ Herramientas recomendadas:

🔒 [VeraCrypt](#) – Cifra discos y carpetas fácilmente.

🔒 [BitLocker](#) – Disponible en Windows.

📖 **Tarea:** Descarga **VeraCrypt** y cifra una carpeta con documentos importantes.

🌐 Protege tu conexión a internet y navegación

Cada vez que navegas en internet, dejas un **rastro digital**. Es fundamental proteger tu actividad en línea.

◆ Usa una VPN para ocultar tu IP

Las VPNs **cifran tu conexión** y evitan que terceros rastreen tu actividad.

📌 Recomendaciones:

✅ [ProtonVPN](#) – VPN gratuita y segura.

✅ [NordVPN](#) – Una de las más rápidas y seguras.

📖 **Tarea:** Descarga **ProtonVPN** y conéctate a una red segura al usar Wi-Fi público.

🔒 Configura la privacidad en redes sociales

✓ Pasos básicos para mejorar la privacidad:

◆ **Facebook:** Ajusta quién puede ver tus publicaciones en *Configuración > Privacidad*.

◆ **Instagram:** Activa la opción de cuenta privada.

◆ **WhatsApp:** Limita quién puede ver tu última conexión.

📌 Ejemplo real:

En 2020, WhatsApp implementó la opción de ocultar el "Última vez visto" debido a **casos de acoso digital**.

📌 Guía completa:

🔗 [Centro de seguridad de Facebook](#)

📖 **Tarea:** Entra a la configuración de privacidad de Facebook e Instagram y **ajusta la visibilidad de tus datos**.

🚀 CONCLUSIÓN Y RETO FINAL

Si sigues estas prácticas, **serás mucho más difícil de atacar**. Sin embargo, **la seguridad digital es un proceso continuo**.

✓ RETO FINAL:

◆ **Cambia tus contraseñas débiles** y almacénalas en un gestor.

Módulo 6: Protección de Datos Sensibles

- ◆ **Activa 2FA** en tus cuentas más importantes.
- ◆ **Instala una VPN** y prueba navegar en modo seguro.
- ◆ **Configura la privacidad en tus redes sociales.**

● **Recuerda:** La **ciberseguridad no es un lujo, es una necesidad.** ¡Haz que sea parte de tu día a día! 🔥

✦ **Más información en:**

- [Guía completa de ciberseguridad](#)
- [Consejos para mejorar la seguridad online](#)