

Seguridad en Internet

Protege tu identidad, tus datos y

A Analizar la
audiencia

S State
objectives

S Seleccionar
materiales

U Usar
materiales

R Requerir
participacion

E Evaluar y
revisar

Objetivo de aprendizaje

Al finalizar esta guía, el estudiante identificará al menos 4 buenas prácticas de seguridad en internet, reconocerá señales de phishing con un 80% de precisión y comprenderá la importancia de proteger su identidad digital.

Vivimos conectados. Redes sociales, banca en línea, correo electrónico, compras digitales... Cada acción en internet deja una huella de datos. Saber proteger esa información no es opcional: es una habilidad esencial del siglo XXI.

01 | Que es la Seguridad en Internet

La **seguridad en internet** es el conjunto de medidas, tecnologías y hábitos que protegen nuestra información, identidad y dispositivos mientras navegamos en línea.

Áreas clave que cubre la seguridad en internet:

Área	Que protege
Privacidad de datos	Información personal, historial de navegación, ubicación
Seguridad de cuentas	Correos, redes sociales, banca, plataformas educativas
Seguridad de dispositivos	Computadoras, celulares, tabletas contra virus y malware
Seguridad en comunicaciones	Mensajes, videollamadas, correos electrónicos
Seguridad financiera	Datos bancarios, tarjetas, transacciones en línea

Dato importante

Según reportes globales de ciberseguridad, cada 39 segundos ocurre un ataque informático en algún lugar del mundo. La mayoría de las víctimas son usuarios que no tomaron precauciones básicas.

02 | Contraseñas Seguras

La contraseña es la primera barrera de protección de tus cuentas. Una contraseña débil es como dejar la puerta de tu casa abierta.

Comparativa: contraseñas débiles vs. fuertes

Ejemplos DÉBILES (NO usar)	Buenas prácticas (SI usar)
123456, qwerty, abc123	Mínimo 12 caracteres mixtos
Tu nombre o apellido	Sin datos personales obvios
Fecha de nacimiento	Combinación aleatoria o frase clave
La misma en todas las cuentas	Única por cada plataforma
Palabras del diccionario	Incluye símbolos: @, #, !, \$, %

Método de la frase clave (Passphrase)

En lugar de inventar una contraseña compleja que olvidarás, usa una frase que solo tú conozcas y modifícala:

Frase: "Mi gato tiene 3 colores favoritos"

Contraseña resultante: MiGato!Tiene3Colores#Fav

Por qué funciona: larga, fácil de recordar, combina mayúsculas, minúsculas, números y símbolos.

Gestores de contraseñas recomendados

Gestor	Plataforma	Costo
Bitwarden	Windows / Mac / iOS / Android	Gratuito / Premium
1Password	Multiplataforma	Pago
KeePass	Windows / Linux	Gratuito
Google Password Manager	Navegador Chrome / Android	Gratuito

03 | Phishing: El Engano Digital

El **phishing** es una técnica de ingeniería social en la que ciberdelincuentes se hacen pasar por entidades confiables (bancos, redes sociales, empresas de paquetería) para robar credenciales o datos financieros.

6 señales de alerta de un correo phishing

#	Senal de alerta	Por que es peligrosa
1	Remitente con dominio sospechoso	Los atacantes imitan nombres reales con dominios falsos
2	Urgencia o amenaza exagerada	Presionan para actuar sin pensar
3	Enlace acortado o extraño	Ocultan la URL maliciosa real
4	Errores ortograficos o gramaticales	Revelan origen no profesional o traducciones automaticas
5	Solicitan contrasena o tarjeta	Ninguna entidad real pide datos sensibles por email
6	Premio o herencia inesperada	Estrategia clasica de fraude por promesas falsas

Regla de oro

Ningun banco, red social ni empresa de confianza te pedira tu contrasena, numero de tarjeta o codigo de verificacion a traves de un correo electronico o mensaje de texto. Ante la duda: NO hagas clic, NO respondas, reporta el mensaje.

04 | Redes Wi-Fi y HTTPS

No todas las redes Wi-Fi son seguras. En redes publicas (cafeterias, aeropuertos, universidades) cualquier persona en la misma red puede interceptar tu trafico si la conexion no esta cifrada.

Wi-Fi PUBLICA (RIESGO)	Wi-Fi SEGURA (RECOMENDADO)
Red Wi-Fi publica sin VPN	Red Wi-Fi privada o con VPN
Trafico visible para terceros	Trafico cifrado de extremo a extremo
Riesgo de ataque Man-in-the-Middle	Proteccion contra interceptacion
No apta para operaciones bancarias	Segura para cualquier tipo de uso
Conexion automatica puede exponerte	Requiere autentificacion explicita

HTTPS vs HTTP

HTTPS (HyperText Transfer Protocol Secure) cifra la comunicacion entre tu navegador y el servidor web usando TLS/SSL. Busca siempre el candado en la barra del navegador antes de introducir datos personales.

Caracteristica	HTTP	HTTPS
Cifrado	NO	SI (TLS/SSL)
Indicador en navegador	Advertencia "No seguro"	Candado verde
Uso recomendado	Solo lectura de contenido publico	Toda transaccion con datos
Riesgo	Datos visibles en la red	Minimo (datos cifrados)

05 | Buenas Practicas Digitales

La seguridad en internet no es un evento unico, sino un conjunto de habitos diarios. Implementar estas practicas reduce drasticamente tu riesgo en linea.

Practica	Por que es importante	Como implementarla
Actualizar software	Los parches corrigen vulnerabilidades conocidas	Activa actualizaciones automaticas en tu dispositivo
Activar 2FA	Una segunda capa bloquea accesos no autorizados	Usa Google Authenticator o Microsoft Authenticator
Revisar permisos de apps	Las apps pueden acceder a camara, microfono y ubicacion	Revisa permisos de apps en ajustes de tu dispositivo
Copias de seguridad	Protege tus datos ante ransomware o fallos de hardware	Regla 3-2-1: 3 copias, 2 medios, 1 fuera de casa
Cerrar sesion en dispositivos ajenos	Sesiones abiertas pueden ser explotadas	Revisa "sesiones activas" en tu cuenta de correo y redes sociales

Actividad de Reflexion

Antes de continuar con el OVA interactivo, reflexiona sobre tus propios hábitos digitales respondiendo las siguientes preguntas en tu cuaderno o en la plataforma:

1. Escribe las 3 contraseñas que más usas (sin decírlas a nadie). ¿Cumplen los criterios de seguridad aprendidos? ¿Qué cambiarías?

2. Recuerda la última vez que recibiste un correo o mensaje sospechoso. ¿Cuántas señales de phishing identificas ahora que ya conoces el tema?

3. ¿Usas la misma contraseña en más de una cuenta? ¿Qué riesgos implica eso? ¿Qué harás al respecto?

4. Menciona dos situaciones cotidianas donde aplicarás a partir de hoy al menos una buena práctica de seguridad en internet.

Glosario Básico

Termino	Definicion
Phishing	Técnica de engaño que suplanta identidades para robar datos personales
Malware	Software malicioso: virus, ransomware, spyware, troyanos, etc.
VPN	Red Privada Virtual que cifra el tráfico de internet
2FA / MFA	Autenticación de dos o múltiples factores para verificar identidad
HTTPS	Protocolo web con cifrado TLS; garantiza comunicación segura
Firewall	Barrera de seguridad que filtra el tráfico de red
Ransomware	Malware que cifra tus archivos y exige rescate económico
Ingeniería social	Manipulación psicológica para obtener información confidencial
Gestor de contraseñas	Aplicación que almacena y genera contraseñas seguras de forma cifrada

Esta guía forma parte del OVA "Seguridad en Internet" diseñado con el Modelo ASSURE. Para la actividad interactiva y la evaluación, accede al módulo en la plataforma.

Recurso educativo de uso libre | Diseñado para integración en Liveworksheets via e-frame