



Asignatura- Área: Tecnología informática y emprendimiento Grado: 6

Tema: Peligros en la web

#### 1. Competencia:

Identifica los riesgos y amenazas que se tienen con el uso de los sistemas informáticos y crea su propio protocolo de seguridad.

Conceptualización y ampliación: Lee atentamente haz un resumen en tu cuaderno y Resuelve las actividades y cuestionamientos propuestos.

### PELIGROS EN LA WEB, RASTREO DIGITAL

La transformación digital es inevitable, día a día nos enfrentamos a un mundo más tecnificado desde procesos del hogar, industrias agrícolas hasta ciudades enteras que buscan apropiarse de las tecnologías y mejorar los procesos, es por ello que debemos estar preparados para ser parte de ésta y qué mejor forma de buscar soluciones tecnológicas que puedan aportar al crecimiento económico de la sociedad.

#### ACCIONES QUE PERMITIRÁN DISMINUIR EL RIESGO DE UN ATAQUE

- **Seguridad informática:** Herramientas o mecanismos de defensa que se implementan en los sitios de almacenamiento o gestión de información digital para obstaculizar o minimizar el riesgo de pérdida, daño o robo de los datos, para esto se definen un grupo de personas, procesos y políticas de acceso.
- **Firewall:** Dispositivo tecnológico de seguridad que define unas políticas o reglas de acceso que impiden el acceso a la red de fuentes no autorizadas, con el único fin de proteger la información, otra de sus funciones es monitorear todas las conexiones entrantes y salientes en la red.
- **Antivirus:** Software que tiene como función principal detectar y eliminar componentes dentro de un sistema informático que pueda generar daños en el sistema operativo y que afecte el correcto funcionamiento del sistema.
- **Clave de seguridad:** Se define como una combinación de letras, números y caracteres

especiales (\$, %, & entre otros) que permiten acceder a un usuario a una plataforma web y resguardar sus datos de terceros.

- **Ataques informáticos:** generan pérdida o daño de datos sensibles para los proyectos que ejecutemos.
- Utilizar herramientas como Firewall para que de forma externa o interna no puedan acceder a nuestra red local persona no autorizadas.

#### RECOMENDACIONES PARA ESTAR SEGUROS EN UN AMBIENTE INFORMÁTICO

1. Cuando acceda a información, correos o plataformas propias en equipos de terceros, asegúrese de ingresar como modo incógnito para no dejar registro de los sitios visitados.
2. Realizar el cambio de contraseña de forma periódica, se recomienda que sean en un periodo de **30 a 60 días**, evitando repetir claves utilizadas con anterioridad y asignando números, letras y caracteres especiales para mayor seguridad. Utilizar combinaciones de letras mayúsculas, minúsculas y caracteres especiales (@, %, &).
3. No guardar o recordar contraseñas en equipos de terceros, esto evitará fraudes o acceso no autorizados, asegurarse de cerrar sesión posterior al ingreso a cualquier plataforma web.
4. Importante generar copias de seguridad de la información que se maneja en la web, realizando los debidos procesos de protección mencionados en este documento, esto evitará disminuir el riesgo de pérdida de la información por robo o daño.



## LAS AMENAZAS MÁS COMUNES QUE SE PRESENTAN LA WEB

Bullying	Grooming	Sexting	Phishing	hoax/Bulo
Intimidación, burla, o acoso de una persona a otra.	Intimidaciones virtuales a través de medios de comunicación como redes sociales, chat privados	Acción de compartir fotos, videos o contenido sexual a través de los dispositivos móviles. mediante las redes sociales, chats privados, correos o medios de comunicación	Utilizado por los hackers con el objetivo de engañar a un usuario y poder obtener la información relevante como datos de acceso, claves bancarias o información de tarjetas de crédito	Realiza una persona o entidad para generar cadenas de mensajes falsos con el fin de expandirlo en las redes sociales
Genera malestar emocional generando	Invasión a la privacidad		Mediante el envío de correos que llevan a la autenticación en sitios falsos	
Problemas psicológicos, aceptación y rechazo.	Robo de datos personales o acceso a las cámaras de los dispositivos con objetivos de espionaje			Atentan contra la moral y el buen nombre de una marca o una persona.

### Hoy puedes aprender más protegiéndote de:

- **QUÉ ES EL VISHING?**

En esta modalidad, por medio de llamadas telefónicas esperan conseguir tus datos personales y/o bancarios a través de engaños, amenazas y suplantaciones.

Esta modalidad de **fraude electrónico** se presenta a través de **una llamada**.

#### ¿Cómo funciona?

Recibes una llamada de un número desconocido.

Los delincuentes **se hacen pasar por colaboradores del Banco**, dándote información parcial de tus productos financieros o datos personales.

Una vez entregas tus datos, **pueden adueñarse de tus productos financieros**.

### ¿CÓMO PUEDES EVITARLO?

**No compartas tus datos financieros con nadie.** El Banco nunca te llama solicitando información confidencial.

- **SMISHING**

El smishing es una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima -red social, banco, institución pública, etc.

Por eso:

- Si recibes un mensaje de texto sospechoso, **NO** respondas ni abras links. Comunícate de inmediato con nuestra línea de atención



**1** **No accedas a links que te inviten a desbloquear** tus cuentas o productos, los canales para desbloquear tus productos son la línea telefónica o las oficinas.



**2** **Nunca entregues tu tarjeta** a la hora de pagar.



**3** **Cambia las claves de acceso**

**POR LO MENOS 1 VEZ AL MES**



6. Resuelve la sopa de letra y escribe una oración con las palabras encontradas invitando a tener cuidado con las redes

A	Ñ	C	O	M	U	N	I	D	A	D	B	M
R	P	T	I	Q	R	S	Y	Q	U	E	U	G
T	A	P	P	P	A	A	N	B	C	Q	L	H
Y	Z	O	R	E	S	P	E	T	O	P	L	J
O	Ñ	N	O	T	O	Ñ	V	O	M	L	Y	K
L	P	M	T	E	C	N	O	L	O	G	I	A
K	O	Z	E	T	I	O	Z	E	T	Q	N	A
M	S	Q	C	R	A	L	X	R	B	E	G	Z
N	O	U	C	W	L	E	R	A	Y	U	D	A
G	C	T	I	R	G	M	F	N	I	A	S	Q
V	A	M	O	R	E	Q	J	C	K	V	P	Z
B	R	R	N	E	R	Z	V	I	D	A	S	R
H	W	F	A	M	I	L	I	A	M	I	L	Y

COMUNIDAD
BULLYING
RESPECTO
PROTECCION
SOCIAL
TOLERANCIA
FAMILIAR
VIDA
PAZ
AMOR
ACOSO
AYUDA