



Introducción a la seguridad de la información [Nivel 1]

Lección 1/Actividad 1

Manejo seguro de la información

IMPORTANTE

Para resolver tu actividad, **guárdala** en tu computadora e **imprímela**.

Si lo deseas, puedes conservarla para consultas posteriores ya que te sirve para reforzar tu aprendizaje. No es necesario que la envíes para su revisión.

Propósito de la actividad

Conocer y aplicar los principios y mecanismos del manejo seguro de la información propia y de terceros.

Practica lo que aprendiste

- I. Escribe la información faltante sobre los principios de la seguridad informática.

Características de la seguridad	Estados de los datos	Contramedidas
Confidencialidad		
	Almacenamiento	
		Capacitación

- II. Investiga las consecuencias de las siguientes amenazas

Internas (originadas por la falta de contar con prácticas en el resguardo de la información de clientes)

Externas (originadas por un ataque informático masivo a nivel mundial)



III. Completa la información (escribiendo cómo hacerlo) de cada una de las siguientes medidas de seguridad que debes aplicar para proteger tu privacidad cuando navegues en internet.

● Lee las políticas de privacidad de las plataformas
● Identifica el opción de “privacidad de datos” en la sección de “configuración”
● Relee tus aportaciones en redes
● Navega en internet de forma anónima
● Evita que las páginas que visitas ubiquen tu posición
● Crea una contraseña distinta para cada cuenta
● Agrega a tus redes sólo personas que conoces



IV. Con relación a la conexión a internet en lugares públicos, responde lo siguiente:

- a) ¿Por qué no es seguro conectarte a este tipo de redes?
- b) ¿A qué se refieren los conceptos “man in the middle” e “información personal expuesta”?

V. Describe en qué consisten las medidas de seguridad que a continuación se indican para verificar que un sitio web es seguro.

- Aviso de legalidad

- Certificado de seguridad

- Datos de contacto

- Diseño de la página web

VI. En caso de que recibas correos sospechosos donde detectes un posible fraude por **phishing** llena estos datos en un archivo de textos:

- Elemento de sospecha del correo electrónico
- Dirección del enlace
- Información que solicita
- Empresa
- Método que usaron para llamar tu atención



VII. Busca en internet las políticas de seguridad sobre el tratamiento de la información de terceros en tu organización e identifica los siguientes elementos:

- Alcance y objetivos:

- Responsabilidad:

- Niveles de privilegios:

- Monitoreo:

- Establecimiento de violaciones:

VIII. Elabora una contraseña fuerte siguiendo los 4 pasos:

1. Elige tu frase
2. Elimina los espacios
3. Sustituye letras por números y símbolos
4. Intercala mayúsculas y minúsculas



IX. Caso de estudio

Un empleado registró a un nuevo cliente en el sistema de manera física por lo cual le solicita su identificación oficial. Una vez que terminó el registro, recibe una llamada de uno de sus colegas y anota un recordatorio en la hoja de la impresión de la identificación del cliente.

Responde.

¿Qué tipo de política de seguridad no está cumpliendo? ¿Por qué?

¿Cuáles amenazas pueden presentarse ante este caso?

- X. Completa la siguiente lista de verificación sobre las medidas de seguridad para home office y un escritorio limpio y evalúa el nivel de protección que tienes.

Accción	Sí/No
Acceso por VPN desde redes que están bajo tu control	
Uso del modo de navegación privada	
Uso sólo las herramientas institucionales	
Envío de información sensible sólo si tus funciones lo requieren	
Guardado de todos los dispositivos electrónicos y de almacenamiento	
Bloqueo tu equipo de cómputo siempre que te ausentes de tu lugar.	



XI. Completa el siguiente diagrama sobre los controles de seguridad.

