**Seguridad Informática**

Año: 6to B

Docente: Laurito, Ernesto

Actividad: responder y justificar la respuesta según consideres que está bien

# Actividad 1: Protección de contraseñas

1. ¿Cuál de las siguientes prácticas es la más segura para proteger las contraseñas?

o A) Usar la misma contraseña en todas las cuentas para mayor comodidad.

* B) Utilizar un administrador de contraseñas para generar y almacenar contraseñas fuertes. X

JUST: Es mas seguro para proteger debido a que las contraseñas fuertes contienen caracteres especiales

o C) Escribir las contraseñas en una hoja de papel y guardarla en un lugar visible.

# Actividad 2: Phishing

2. ¿Qué acción deberías tomar si recibes un correo electrónico sospechoso solicitando tu información personal?

o A) Responder con los datos solicitados si parece urgente.

o B) Hacer clic en el enlace para verificar si el sitio web se ve confiable.

* C) No responder y reportar el correo como phishing. X

JUST: Al hacer esto no solo estas protegiendo tus datos personales sino que también te garantizas que no sigan mandando mensajes de ese estilo

# Actividad 3: Cifrado de datos

3. ¿Qué método es el más seguro para proteger datos sensibles durante su transmisión en Internet?

o A) Enviar la información sin cifrar si es urgente.

o B) Utilizar cifrado SSL/TLS para encriptar la comunicación. X

JUST: el utilizar un cifrado es importante debido a que hace que sea difícil para los hackers el descifrar tus datos

o C) Enviar los datos en un archivo comprimido sin cifrar.

# Actividad 4: Actualizaciones de software

4. ¿Cuál es la razón principal para mantener el software actualizado?

* A) Para obtener nuevas funcionalidades de inmediato.
* B) Para proteger el sistema de vulnerabilidades de seguridad descubiertas. X

JUST: Al actualizar el software, se incluye una actualización a los sistemas de seguridad del sistema operativo

o C) Para evitar que el software se vuelva lento.

# Actividad 5: Autenticación de dos factores (2FA)

5. ¿Cuál es el beneficio principal de activar la autenticación de dos factores (2FA)?

* A) Permite acceder a las cuentas más rápido.
* B) Agrega una capa adicional de seguridad, haciendo más difícil para atacantes acceder a la cuenta. X

JUST: Haciendo esto es menos probable que tu cuenta sufra un ataque o robo de informacion

* C) Evita que los usuarios olviden sus contraseñas.

# Actividad 6: Uso de redes públicas

6. ¿Qué es lo más seguro hacer al utilizar una red Wi-Fi pública para conectarte a Internet?

o A) Iniciar sesión en todas tus cuentas sin preocuparte.

O B) Usar una VPN para cifrar tu conexión y proteger tus datos. X

JUST: El utilizar una l VPN le dificulta a los hackers el rastrear la ubicación de el dispositivo

o C) Desactivar el firewall ya que puede interferir con la conexión.

# Actividad 7: Manejo de malware

7. Si tu computadora muestra comportamientos inusuales como lentitud o pop-ups inesperados, ¿cuál es la mejor acción a tomar?

o A) Ignorar los síntomas si no afectan demasiado el uso.

* B) Descargar e instalar un antivirus confiable para escanear el sistema en busca de malware. X

JUST: Es la mejor opción que podrías tomar debido a que te asegura a la vez que no tengas ningún virus

C) Desinstalar algunos programas al azar para ver si se soluciona el problema.