EVALUACIÓN ESCRITA: SEGURIDAD EN INTERNET

Nombre del Estudiante: _____ Fecha: _____

BLOQUE I: RESPUESTA CORTA

Lee con atención cada enunciado y escribe la palabra o concepto correcto en el espacio en blanco.

1. **Método utilizado por ciberdelincuentes para estafar y obtener información confidencial (como contraseñas o datos bancarios) a través de correos electrónicos, mensajes o páginas web falsas, suplantando la identidad de empresas legítimas:**

Respuesta: _____

2. **Nombre que recibe el software malicioso diseñado para infiltrarse en un dispositivo, dañar el sistema o robar información sin el consentimiento del usuario:**

Respuesta: _____

3. **Proceso técnico que consiste en ocultar o codificar la información mediante una clave para que nadie pueda leerla a menos que tenga la contraseña de descifrado:**

Respuesta: _____

4. **Tipo de software dañino que bloquea el acceso a la computadora o a los archivos de la víctima y exige un pago económico (rescate) para poder recuperarlos:**

Respuesta: _____

BLOQUE II: OPCIÓN MÚLTIPLE

Marca con una "X" dentro del recuadro de la alternativa que consideres correcta.

5. **Recibes un mensaje de texto de un número totalmente desconocido que indica que has ganado un premio en efectivo y te solicita abrir un enlace para completar tus datos de envío. ¿Cómo debes actuar?**

[ ] A) Abrir el enlace de inmediato para evitar que el premio expire.

[ ] B) Eliminar el mensaje, bloquear el número remitente y evitar hacer clic en el enlace.

[ ] C) Compartir el enlace con amigos y familiares para comprobar si a ellos también les llegó.

6. **Al momento de crear una cuenta nueva en una red social, ¿cuál es la acción más recomendada respecto a la privacidad?**

[ ] A) Dejar el perfil completamente público para que más personas puedan interactuar.

[ ] B) Configurar las opciones de privacidad para que solo los amigos conocidos vean las publicaciones.

[ ] C) Compartir la ubicación en tiempo real en cada publicación para mantener informados a los contactos.

7. ¿Qué significa que un sitio web tenga el protocolo "https://" y un icono de candado cerrado en la barra de direcciones?

[ ] A) Que la página web es 100% inmune a cualquier tipo de fraude informático.

[ ] B) Que la conexión entre tu dispositivo y el sitio web está cifrada y es más segura.

[ ] C) Que el sitio web pertenece obligatoriamente a una entidad del gobierno.

8. ¿Qué medida de seguridad es indispensable aplicar al utilizar redes Wi-Fi públicas o abiertas (como las de un parque o cafetería)?

[ ] A) Aprovechar para realizar transferencias bancarias y compras en línea de forma rápida.

[ ] B) Evitar ingresar a cuentas personales con contraseñas y desactivar la conexión compartida.

[ ] C) Dejar activada la visibilidad del dispositivo para que otros usuarios se conecten.

9. ¿Cuál de las siguientes opciones describe el método de "Autenticación en Dos Pasos" (2FA)?

[ ] A) Utilizar dos contraseñas diferentes escritas una después de la otra.

[ ] B) Introducir la contraseña habitual y luego un código temporal enviado al teléfono celular.

[ ] C) Cambiar la contraseña de acceso de la cuenta de manera obligatoria dos veces por semana.

10. Si un compañero de clase empieza a publicar fotos humillantes o comentarios ofensivos sobre otra persona de forma constante en una red social, estamos ante un caso de:

[ ] A) Suplantación de identidad digital.

[ ] B) Ciberacoso (Cyberbullying).

[ ] C) Ingeniería social básica.

11. ¿Cuál es el riesgo de descargar e instalar aplicaciones o juegos fuera de las tiendas oficiales (como Google Play o App Store)?

[ ] A) Que el juego sea un poco más lento de lo normal.

[ ] B) Que la aplicación contenga virus ocultos que comprometan la seguridad del celular.

[ ] C) Que la aplicación requiera actualizarse con mayor frecuencia.

12. **¿Con qué frecuencia se recomienda realizar copias de seguridad (backups) de los archivos más importantes guardados en la computadora o celular?**

[ ] A) Únicamente cuando el dispositivo empiece a fallar o a ponerse lento.

[ ] B) De manera periódica (semanal o mensual) en un disco externo o servicio en la nube.

[ ] C) No es necesario si el dispositivo cuenta con un antivirus actualizado.

BLOQUE III: MENÚ DESPLEgABLE

Selecciona del recuadro la opción que complete de manera correcta cada una de las siguientes afirmaciones de seguridad.

13. **Para crear una contraseña que sea robusta y altamente protegida ante posibles hackeos o ataques informáticos, es indispensable que esté conformada por:**

Estructura ideal: [Seleccionar opción ▼] ***(Opciones en el sistema: Solo la fecha de nacimiento / El nombre de una mascota / Letras mayúsculas, minúsculas, números y símbolos)***

14. **El rastro de datos, comentarios, búsquedas y fotos que dejas de forma permanente al navegar, publicar o interactuar en la red se denomina:**

Concepto: [Seleccionar opción ▼] ***(Opciones en el sistema: Huella digital / Identidad anónima / Historial temporal)***

15. **Cuando un ciberdelincuente crea un perfil falso utilizando el nombre y las fotos reales de otra persona para engañar a sus contactos, está cometiendo:**

Delito: [Seleccionar opción ▼] ***(Opciones en el sistema: Robo de cookies / Suplantación de identidad / Phishing masivo)***

16. **Al recibir una actualización del sistema operativo de tu computadora o teléfono celular, la acción correcta es:**

Acción: [Seleccionar opción ▼] ***(Opciones en el sistema: Instalarla de inmediato / Ignorarla / Posponerla por varios meses)***

BLOQUE IV: UNIR CON FLECHAS

Une mediante una línea recta cada concepto de la izquierda con su definición correspondiente a la derecha.

CONCEPTO		DEFINICIÓN
17. Antivirus		Tipo de programa espía diseñado para recolectar datos de tus hábitos de navegación sin tu permiso.

CONCEPTO		DEFINICIÓN
18. Spyware		Barrera de seguridad que monitorea y controla el tráfico de red entrante y saliente en tu computadora.
19. Firewall		Software especializado diseñado específicamente para detectar, bloquear y eliminar programas maliciosos.

BLOQUE V: CLASIFICACIÓN (ARRASTRAR Y SOLTAR)

Ubica cada una de las siguientes conductas en el casillero correspondiente de la tabla, según consideres que representan un hábito seguro o un riesgo digital.

Conductas a evaluar:

- **Aceptar solicitudes de amistad de personas totalmente desconocidas en tus redes sociales.**
- **Cerrar la sesión de tus cuentas personales siempre que utilices una computadora pública o compartida.**
- **Utilizar exactamente la misma contraseña de acceso para todas tus cuentas de correo y plataformas.**

20. Tabla de Clasificación:

BUENAS PRÁCTICAS (Hábitos Seguros)	MALAS PRÁCTICAS (Riesgos Digitales)