1. ¿Cuál de los siguientes describe mejor el concepto de 'Tríada de la Seguridad' (CIA) en el contexto académico?
   a) Conexión, Internet y Aplicaciones
   b) Cifrado, Identidad y Auntenticación
   c) Confidencialidad, Integridad y Disponibilidad
   d) Control, Informática y Almacenamiento

2. Un o una docente recibe un correo que parece ser de la plataforma de gestión escolar pidiendo 'urgentemente' que actualice su contraseña haciendo clic en un enlace. ¿Qué técnica de ataque es esta?
   a) Fuerza bruta
   b) Ransomware
   c) Spyware
   d) Phishing

3. ¿Qué característica hace que una contraseña sea considerada robusta según los estándares actuales?
   a) Que cumpla la regla 8:4.
   b) Que tenga solo letras pero que sea larga (más de 20 letras).
   c) Que se cambie cada 15 días obligatoriamente, aunque sea corta.
   d) Que sea el nombre de la mascota del docente más el año actual.

4. ¿En qué consiste el 'Principio de Menor Privilegio' en una red educativa?
   a) En dar privilegios de administrador a todos los docentes para que no dependan del técnico.
   b) En cobrar menos por las licencias de software a las unidades educativas.
   c) En que cada usuario tenga solo los permisos necesarios para realizar sus funciones específicas.
   d) En que las y los estudiantes no deben tener acceso a internet en el aula.

5. Si un o una docente necesita realizar copias de seguridad de sus materiales didácticos, ¿Cuál es la mejor práctica recomendada?
   a) La regla 3-2-1
   b) Enviar los archivos por correo electrónico a sí mismo como única copia.
   c) Confiar en que la computadora de la unidad educativa nunca fallará.
   d) Guardarlo todo en un único pendrive que siempre lleva consigo.

6. Para proteger la navegación en internet de la institución, ¿Qué protocolo indica que la comunicación con un sitio web está cifrada?
   a) FTP
   b) HTTPS
   c) HTTP
   d) HTML

7. ¿Qué es la Autenticación de Múltiple Factor (MFA)?
   a) Usar la misma contraseña para varias cuentas para no olvidarlas.
   b) Un método que requiere dos o más pruebas de identidad antes de permitir el acceso.
   c) Cambiar el nombre de usuario cada vez que se inicia sesión.
   d) Permitir que varias personas usen la misma cuenta de usuario simultáneamente.

8. Un o una docente deja su sesión de la plataforma de calificaciones abierta en una computadora del aula mientras sale un momento al pasillo. ¿A qué riesgo se expone?
   a) Ataque de Denegación de Servicio (DDoS).
   b) Infección de virus mediante el monitor.
   c) Actualización automática del sistema operativo.
   d) Acceso físico no autorizado o ingeniería social.

9. ¿Qué debe hacer un o una docente si sospecha que su computadora institucional tiene un virus o malware?
   a) Formatear el equipo por su cuenta sin avisar a nadie.
   b) Desconectarla de la red y reportarlo inmediatamente al área de soporte técnico.
   c) Intentar instalar un antivirus gratuito desconocido para solucionarlo.
   d) Apagarla y no decir nada para evitar problemas.

10. En el marco de la protección de datos, ¿Qué se considera información sensible en una unidad educativa?
    a) El menú del comedor escolar del mes.
    b) La lista de libros recomendados para el curso.
    c) El calendario de días festivos del año escolar.
    d) Nombres, direcciones, calificaciones, conducta de las y los estudiantes.