**Pregunta 1:**¿Qué es la seguridad de la información?  
a) Un conjunto de herramientas para realizar copias de seguridad.  
b) Un sistema para proteger exclusivamente los datos personales.  
c) **Un conjunto de medidas preventivas y reactivas que permiten almacenar y proteger la información.**   
d) Un sistema informático que evita errores humanos.

**Pregunta 2:**¿Cuál es el objetivo principal de la seguridad informática?  
a) **Proteger la integridad y privacidad de la información**.  
b) Aumentar la velocidad de los sistemas informáticos.  
c) Realizar copias de seguridad de los datos.  
d) Optimizar los procesos de información.

**Pregunta 3:**¿Qué protege la ciberseguridad?  
a) Solo los datos almacenados en servidores.  
b) La integridad de la información sin acceso externo.  
c) **Todos los equipos informáticos mediante prácticas ofensivas**.  
d) Exclusivamente las redes de comunicación.

**Pregunta 4:**¿Qué es un Sistema de Información (SI)?  
a) Un software de gestión de recursos humanos.  
b) **Un conjunto de recursos que administra y procesa información**.  
c) Una base de datos que almacena solo datos financieros.  
d) Un protocolo de seguridad en redes informáticas.

**Pregunta 5:**¿Cuál es uno de los recursos de un SI?  
a) Antivirus.  
b) **Humanos**.  
c) Exclusivamente procesadores.  
d) Firewalls.

**Pregunta 6:**¿Qué etapa del funcionamiento de un SI incluye la toma de decisiones?  
a) Entrada de datos.  
b) **Procesamiento de la información**.  
c) Almacenamiento de la información.  
d) Salida de la información.

**Pregunta 7:**¿Qué ISO se utiliza como base para un Sistema de Gestión de Seguridad de la Información (SGSI)?  
a) ISO 9001.  
b) **ISO 27001 y 27002**.  
c) ISO 14001.  
d) ISO 50001.

**Pregunta 8:**¿Qué fase del ciclo de Deming corresponde a "Verificar"?  
a) Planificar.  
b) Hacer.  
c) **Verificar**.  
d) Actuar.

**Pregunta 9:**¿Cuál de los siguientes es un activo que se protege en un SI?  
a) Parches de software.  
b) **Datos e información**.  
c) Antivirus.  
d) Sensores biométricos.

**Pregunta 10:**¿Cuál es una vulnerabilidad de diseño en un SI?  
a) **Puertas traseras en el software**.  
b) Política de seguridad inexistente.  
c) Configuración inadecuada del SI.  
d) Falta de formación del personal.

**Pregunta 11:**¿Qué es una vulnerabilidad del día cero?  
a) Un error en la red de comunicación.  
b) **Una vulnerabilidad que aún no tiene solución**.  
c) Una amenaza malintencionada.  
d) Un riesgo compartido por varias entidades.

**Pregunta 12:**¿Qué es una amenaza en un SI?  
a) Una acción malintencionada por empleados internos.  
b) **Cualquier evento que comprometa la seguridad del SI.**  
c) Una forma de prevenir daños en el sistema.  
d) Un fallo eléctrico que inutiliza el sistema.

**Pregunta 13:**¿Qué es una contramedida en seguridad informática?  
a) Un mecanismo para aumentar la velocidad del SI.  
b) **Una acción preventiva ante amenazas**.  
c) Un ataque contra una amenaza.  
d) Una herramienta de auditoría de seguridad.

**Pregunta 14:**¿Qué implica la opción de "evitar el riesgo"?  
a) Compartir el riesgo con otras entidades.  
b) **Rechazar la acción que genera el riesgo**.  
c) Reducir el riesgo a niveles aceptables.  
d) Aceptar las consecuencias del riesgo.

**Pregunta 15:**¿Qué se logra con la automatización de procedimientos de detección en un análisis de vulnerabilidades?  
a) Eliminar amenazas automáticamente.  
b) **Atenuar vulnerabilidades**.  
c) Compartir riesgos con otras empresas.  
d) Aumentar el tamaño de los datos procesados.

**Pregunta 16:**¿Cuál es una herramienta utilizada en un análisis de vulnerabilidades?  
a) Cortafuegos.  
b) Hardware de respaldo.  
c) **Control de servicios instalados**.  
d) Gestión de sistemas operativos.

**Pregunta 17:**¿Qué acción se toma cuando no es posible reducir ni evitar un riesgo?  
a) Transferir el riesgo.  
b) **Asumir el riesgo**.  
c) Reducir el riesgo.  
d) Evitar el riesgo.

**Pregunta 18:**¿Qué tipo de amenaza ocurre debido a un accidente?  
a) Robo de información.  
b) Sabotaje interno.  
c) **Avería del sistema informático**.  
d) Ataque informático externo.

**Pregunta 19:**¿Cuál de las siguientes es una amenaza física?  
a) Virus informáticos.  
b) Fallos en el hardware.  
c) **Empleados descuidados**.  
d) Mala utilización de aplicaciones.

**Pregunta 20:**¿Qué amenaza garantiza disponibilidad pero no confidencialidad ni integridad?  
a) **Interceptación**.  
b) Modificación.  
c) Interrupción.  
d) Fabricación.

**Pregunta 21:**¿Qué técnica se utiliza para detectar intrusos en los sistemas informáticos?  
a) Instalación de software antivirus.  
b) Parches de seguridad del sistema operativo.  
c) **Test de penetración**.  
d) Uso de cuentas de usuario limitadas.

**Pregunta 22:**¿Qué es una medida de seguridad pasiva?  
a) Instalar un cortafuegos.  
b) **Recuperar el sistema tras un incidente**.  
c) Configurar herramientas antivirus.  
d) Destruir información obsoleta.

**Pregunta 23:**¿Cuál es una técnica de seguridad física?  
a)Uso de RAID en servidores.  
b) **Instalación de detectores de metales**.  
c) Realización de copias de seguridad.  
d) Recuperación de datos dañados.

**Pregunta 24:**¿Cuál es un lugar adecuado para un CPD?  
a) Planta baja.  
b) Sótano.  
c) **Planta intermedia**.  
d) Última planta.

**Pregunta 25:**¿Cuál es el objetivo principal de un SAI (Sistema de Alimentación Ininterrumpida)?  
a) Proteger la integridad de la información.  
b) **Proporcionar energía eléctrica en caso de cortes**.  
c) Realizar copias de seguridad automáticamente.  
d) Optimizar el procesamiento de datos.

**Pregunta 26:**¿Qué tipo de SAI se utiliza comúnmente en entornos domésticos?  
a) ON-LINE.  
b) IN-LINE.  
c) **OFF-LINE**.  
d) Diferencial.

**Pregunta 27:**¿Qué tipo de copia de seguridad solo guarda los cambios desde la última copia completa?  
a) Completa.  
b) **Incremental**.  
c) Diferencial.  
d) Progresiva.

**Pregunta 28:**¿Qué técnica se utiliza para recuperar información lógica?  
a) Uso de extintores.  
b) RAID.  
c) **TestDisk**.  
d) UPS.

**Pregunta 29:**¿Qué método garantiza que no se podrá acceder a la información de un dispositivo en desuso?  
a) **Sobreescritura de datos**.  
b) Realización de copias de seguridad.  
c) Encriptación de archivos.  
d) Instalación de un cortafuegos.

**Pregunta 30:**¿Qué se debe evitar al ubicar servidores?  
a) Plantas intermedias.  
b) **Zonas cercanas a paredes exteriores**.  
c) Espacios sin luz natural.  
d) Lugares con aire acondicionado.

**Pregunta 31:**¿Qué técnica de destrucción de información consiste en sobrescribir los datos para impedir su recuperación?  
a) Destrucción física.  
b) **Sobreescritura de datos**.  
c) Encriptación.  
d) RAID.

**Pregunta 32:**¿Qué sistema de archivo mejora la seguridad del almacenamiento mediante listas de control de acceso (ACL)?  
a) FAT32.  
b) **NTFS**.  
c) EXT4.  
d) Cualquier sistema de archivos sin ACL.

**Pregunta 33:**¿Cuál de las siguientes técnicas se emplea en la seguridad física y ambiental?  
a) **Termografía**.  
b) RAID.  
c) Cortafuegos lógico.  
d) Encriptación de datos.

**Pregunta 34:**¿Qué función tiene el personal de seguridad física en un CPD?  
a) Recuperar información dañada.  
b) Monitorear el sistema informático.  
c) **Restringir el acceso no autorizado.**  
d) Realizar análisis de vulnerabilidades.

**Pregunta 35:**¿Qué tipo de SAI estabiliza mejor la corriente eléctrica y se activa en caso de cortes o tensión anómala?  
a) SAI OFF-LINE.  
b) **SAI INTERACTIVO (IN-LINE).**  
c) SAI ON-LINE.  
d) SAI sin baterías.

**Pregunta 36:**¿Qué herramienta se usa para recuperar datos de dispositivos con fallos lógicos en sistemas operativos Linux?  
a) CHKDSK.  
b) DISM.  
c) **fsck**.  
d) PhotoRec.

**Pregunta 37:**¿Cuál es el objetivo de un análisis de vulnerabilidades en una organización?  
a) Optimizar el rendimiento del sistema informático.  
b) **Identificar y corregir posibles debilidades que comprometan la seguridad del SI.**  
c) Reducir el tamaño de la información almacenada.  
d) Mejorar la interfaz del sistema.

**Pregunta 38:**¿Qué tipo de amenaza es un incendio en un CPD?  
a) Amenaza lógica.  
b) **Amenaza física**.  
c) Amenaza interna.  
d) Amenaza malintencionada.

**Pregunta 39:**¿Cuál de las siguientes NO es una amenaza malintencionada?  
a) Sabotaje.  
b) **Error en la ejecución de procedimientos**.  
c) Robo de información.  
d) Ataque informático.

**Pregunta 40:**¿Qué es la seguridad pasiva?  
a) Un conjunto de medidas aplicadas antes de un incidente para evitar su impacto.  
b) **Un conjunto de medidas aplicadas después de un incidente para minimizar su impacto.**  
c) Medidas para evitar amenazas lógicas.  
d) El uso de detectores ultrasónicos y barreras infrarrojas.

**Pregunta 41:**¿Qué fase del ciclo de Deming se centra en establecer el contexto del SGSI?  
a) Hacer (Do).  
b) Verificar (Check).  
c) Actuar (Act).  
d) **Planificar (Plan).**

**Pregunta 42:**¿Cuál de las siguientes medidas asegura la confidencialidad de los datos?  
a) Permitir el acceso público a la información.  
b) **Uso de listas de control de acceso (ACL) y encriptación**.  
c) Implementar sistemas RAID.  
d) Realizar copias de seguridad.

**Pregunta 43:**¿Cuál es un ejemplo de amenaza por agentes internos?  
a) Inundaciones.  
b) **Empleados descuidados**.  
c) Virus informático.  
d) Sabotaje externo.