**CUESTIONARIO DE PREGUNTAS**

**Bloque 1: Introducción a ISO 27001 y el SGSI**

1. ¿Cuál es el objetivo principal de ISO 27001?
2. ¿Qué significa SGSI?
3. ¿Cuáles son las tres dimensiones clave de la seguridad de la información?
4. ¿Qué es la política de seguridad de la información?
5. ¿Qué son los activos de información?
6. ¿Por qué es importante la confidencialidad en el SGSI?
7. Define “integridad” en el contexto de la seguridad de la información.
8. ¿Qué es la disponibilidad de la información?
9. ¿Qué es el ciclo PDCA?
10. ¿Qué se entiende por "mejora continua"?

**Bloque 2: Contexto de la Organización (Capítulo 4)**

1. ¿Qué se debe considerar al entender el contexto interno de una organización?
2. ¿Cómo influye el contexto externo en la gestión de seguridad de la información?
3. ¿Qué se incluye en el alcance del SGSI?
4. ¿Cómo afecta el alcance en la implementación del SGSI?
5. ¿Qué son las partes interesadas en ISO 27001?
6. ¿Por qué es importante identificar las necesidades de las partes interesadas?
7. ¿Qué implica la comprensión de la organización en un SGSI?
8. ¿Qué información debe incluirse en la declaración de aplicabilidad?
9. ¿Qué aspectos clave se evalúan al establecer el contexto de la organización?
10. ¿Qué es un riesgo en el contexto de ISO 27001?

**Bloque 3: Liderazgo (Capítulo 5)**

1. ¿Cuál es el rol de la alta dirección en el SGSI?
2. ¿Por qué es importante la política de seguridad de la información?
3. ¿Cómo puede la alta dirección demostrar compromiso con el SGSI?
4. ¿Qué responsabilidades tienen los líderes en ISO 27001?
5. ¿Cuál es el propósito de asignar roles y responsabilidades en el SGSI?
6. ¿Qué significa “gobernanza” en el contexto del SGSI?
7. ¿Qué se debe incluir en una política de seguridad de la información?
8. ¿Qué responsabilidades tiene un oficial de seguridad de la información?
9. ¿Qué es la cultura de seguridad y por qué es importante?
10. ¿Cómo afecta la participación de la alta dirección al éxito del SGSI?

**Bloque 4: Planificación del SGSI (Capítulo 6)**

1. ¿Qué es la evaluación de riesgos?
2. ¿Por qué es fundamental gestionar los riesgos en el SGSI?
3. ¿Qué factores se consideran en el análisis de riesgos?
4. ¿Qué es una matriz de riesgos?
5. ¿Cómo se establecen los objetivos de seguridad de la información?
6. ¿Qué se debe considerar al definir un plan de tratamiento de riesgos?
7. ¿Qué es una acción correctiva en ISO 27001?
8. ¿Cuál es la diferencia entre mitigar y transferir un riesgo?
9. ¿Qué implica el tratamiento de riesgos?
10. ¿Cómo se definen los controles en el SGSI?

**Bloque 5: Soporte (Capítulo 7)**

1. ¿Qué tipo de recursos son necesarios para un SGSI efectivo?
2. ¿Por qué es importante la competencia del personal en el SGSI?
3. ¿Qué tipo de formación necesita el personal en seguridad de la información?
4. ¿Qué son las comunicaciones internas en ISO 27001?
5. ¿Cuál es la importancia de la documentación en el SGSI?
6. ¿Qué es la información documentada en ISO 27001?
7. ¿Qué aspectos se deben comunicar a las partes interesadas?
8. ¿Cómo se gestiona la información documentada en el SGSI?
9. ¿Qué tipo de evidencias se deben registrar?
10. ¿Por qué es esencial el soporte en un SGSI?

**Bloque 6: Operación (Capítulo 8)**

1. ¿Qué implica la implementación de controles en el SGSI?
2. ¿Qué es la evaluación de riesgos en la operación?
3. ¿Cuál es el propósito de los procedimientos operativos?
4. ¿Cómo se gestionan los cambios en el SGSI?
5. ¿Qué es un incidente de seguridad de la información?
6. ¿Cuál es el propósito de un plan de respuesta a incidentes?
7. ¿Qué es la continuidad de negocio en el contexto del SGSI?
8. ¿Cómo se gestionan los activos de información durante la operación?
9. ¿Qué es el control de acceso?
10. ¿Cuál es el propósito de las copias de seguridad?

**Bloque 7: Evaluación del Desempeño (Capítulo 9)**

1. ¿Qué es el monitoreo en el SGSI?
2. ¿Cuál es el objetivo de una auditoría interna en ISO 27001?
3. ¿Qué se evalúa en una revisión por la dirección?
4. ¿Por qué es importante la medición en el SGSI?
5. ¿Cómo se mide el desempeño del SGSI?
6. ¿Qué información debe incluir un informe de auditoría interna?
7. ¿Qué se hace con los hallazgos de una auditoría interna?
8. ¿Por qué es fundamental la revisión por la dirección?
9. ¿Qué significa "mejora continua" en el SGSI?
10. ¿Qué herramientas se pueden utilizar para el monitoreo de la seguridad de la información?

**Bloque 8: Mejora Continua (Capítulo 10)**

1. ¿Qué es una acción correctiva?
2. ¿Qué significa "no conformidad"?
3. ¿Qué acciones se toman en caso de una no conformidad?
4. ¿Qué es una acción preventiva?
5. ¿Por qué es importante la mejora continua en ISO 27001?
6. ¿Qué rol juega el análisis de causas en la mejora continua?
7. ¿Cómo se implementa una mejora en el SGSI?
8. ¿Qué es la revisión posterior a una acción correctiva?
9. ¿Qué impacto tiene la mejora continua en el SGSI?
10. ¿Qué procesos se utilizan para evaluar la eficacia de las acciones correctivas?

**Bloque 9: Anexo A - Controles de Seguridad**

1. ¿Qué es el Anexo A en ISO 27001?
2. ¿Cuántos controles de seguridad se incluyen en el Anexo A?
3. ¿Qué es un control organizativo?
4. ¿Qué son los controles físicos?
5. ¿Cuál es el propósito de los controles de acceso?
6. ¿Qué es un control de respuesta a incidentes?
7. ¿Qué son los controles de continuidad del negocio?
8. ¿Qué tipo de controles se aplican a la criptografía?
9. ¿Cuál es el rol de los controles de protección contra malware?
10. ¿Qué significa “control tecnológico” en el contexto del Anexo A?

**Bloque 10: Auditoría y Cumplimiento**

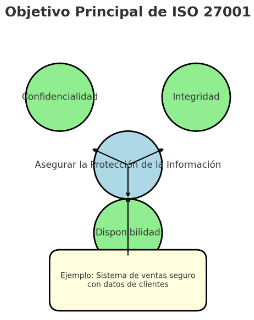
1. ¿Cuál es el propósito de una auditoría de certificación?
2. ¿Qué rol tiene el auditor en ISO 27001?
3. ¿Qué significa conformidad en ISO 27001?
4. ¿Qué es una no conformidad mayor?
5. ¿Cuál es la diferencia entre una auditoría interna y una externa?
6. ¿Qué documentación se requiere para la auditoría de ISO 27001?
7. ¿Qué se evalúa en una auditoría de seguimiento?
8. ¿Cuál es el propósito de una auditoría de recertificación?
9. ¿Qué es la declaración de aplicabilidad en el contexto de una auditoría?
10. ¿Por qué es importante la evidencia en una auditoría?

**RESOLUCION DE PREGUNTAS**

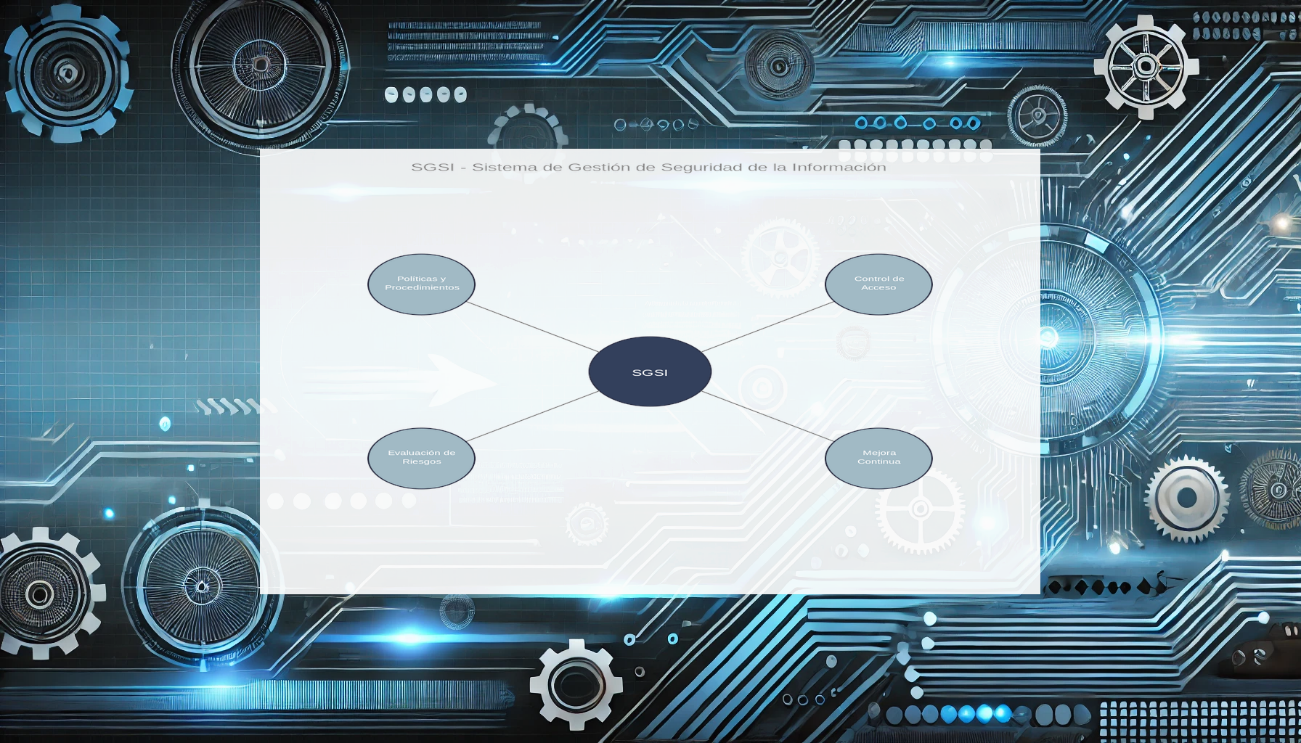
**Bloque 1: Introducción a ISO 27001 y el SGSI**

1. **¿Cuál es el objetivo principal de ISO 27001?**  
   Asegurar la protección de la información dentro de una organización.  
   *Ejemplo*: Garantizar que los datos de clientes estén seguros en un sistema de ventas.

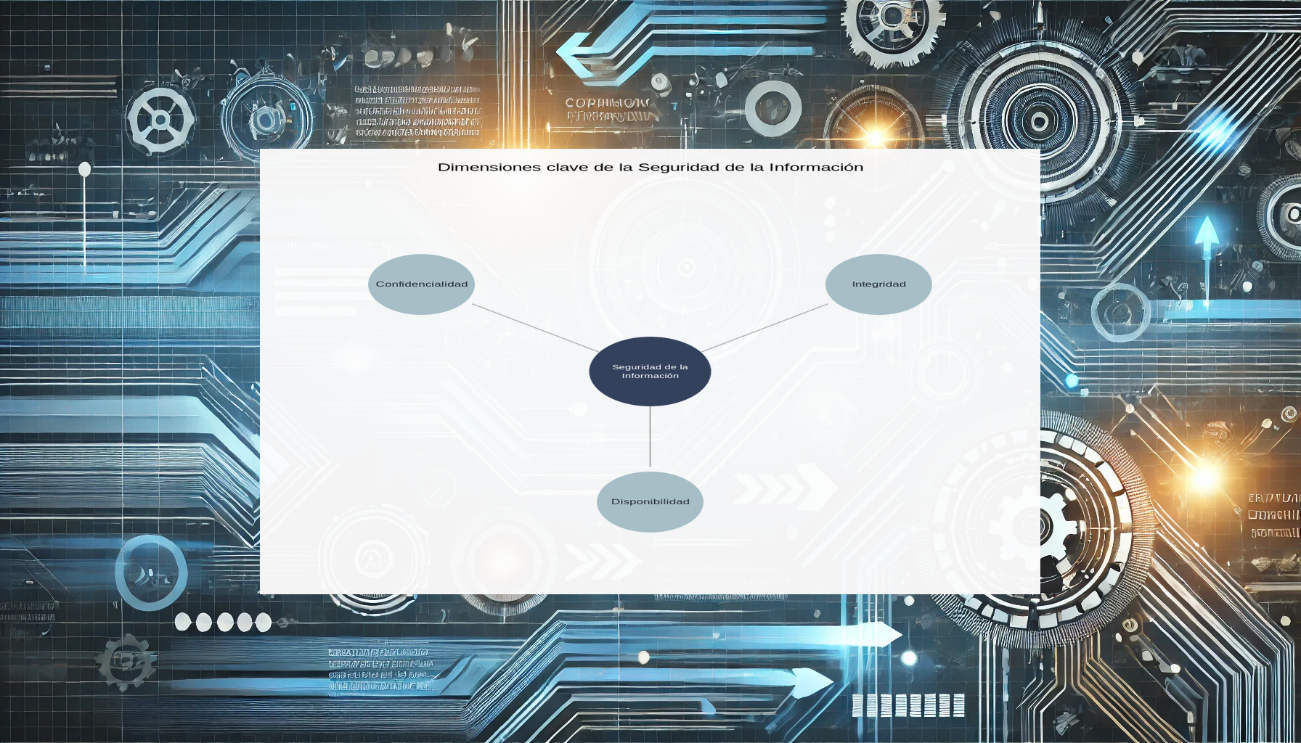
* **Confidencialidad:** Mantener la información accesible solo para quienes estén autorizados.
* **Integridad:** Asegurar que la información esté completa y no sea alterada sin autorización.
* **Disponibilidad**: Garantizar que la información esté disponible para quienes la necesiten, en el momento adecuado**.**



1. **¿Qué significa SGSI?**  
   Sistema de Gestión de Seguridad de la Información, una estructura para gestionar la seguridad de la información.  
   *Ejemplo*: Un sistema que define cómo proteger archivos confidenciales.



1. **¿Cuáles son las tres dimensiones clave de la seguridad de la información?**  
   Confidencialidad, integridad y disponibilidad.  
   *Ejemplo*: Proteger una base de datos para que solo personal autorizado acceda (confidencialidad), sin alteraciones (integridad), y que esté disponible cuando se necesite (disponibilidad).



1. **¿Qué es la política de seguridad de la información?**  
   Un documento que establece las normas y directrices para proteger la información.  
   *Ejemplo*: Un manual que indica quién puede acceder a ciertos archivos en una empresa.
2. **¿Qué son los activos de información?**  
   Recursos que contienen información valiosa para la empresa, como bases de datos o documentos.  
   *Ejemplo*: La lista de clientes en un archivo Excel.
3. **¿Por qué es importante la confidencialidad en el SGSI?**  
   Para evitar que personas no autorizadas accedan a información sensible.  
   *Ejemplo*: Proteger los datos personales de los clientes en una aplicación.
4. **Define “integridad” en el contexto de la seguridad de la información.**  
   Asegurarse de que la información no sea alterada sin autorización.  
   *Ejemplo*: Mantener intacta la lista de precios sin cambios no aprobados.
5. **¿Qué es la disponibilidad de la información?**  
   Garantizar que la información esté accesible cuando se necesite.  
   *Ejemplo*: Un sistema de inventario que esté disponible para consulta las 24 horas.
6. **¿Qué es el ciclo PDCA?**  
   Un ciclo de mejora continua que implica Planificar, Hacer, Verificar y Actuar.  
   *Ejemplo*: Planear una política de seguridad, implementarla, revisarla y ajustarla según resultados.
7. **¿Qué se entiende por "mejora continua"?**  
   Proceso constante de mejorar el SGSI para adaptarse a nuevos riesgos.  
   *Ejemplo*: Revisar y actualizar protocolos de seguridad cada año en una empresa de software.

**Bloque 2: Contexto de la Organización (Capítulo 4)**

1. **¿Qué se debe considerar al entender el contexto interno de una organización?**  
   Factores como la estructura organizativa, políticas internas y recursos disponibles.  
   *Ejemplo*: Evaluar si el equipo de TI es suficiente para manejar la seguridad en una pequeña empresa.
2. **¿Cómo influye el contexto externo en la gestión de seguridad de la información?**  
   Factores externos como leyes, regulaciones y amenazas tecnológicas afectan la estrategia de seguridad.  
   *Ejemplo*: Adaptarse a una nueva ley de protección de datos en el país.
3. **¿Qué se incluye en el alcance del SGSI?**  
   Las áreas, procesos, sistemas y ubicaciones que estarán protegidos por el SGSI.  
   *Ejemplo*: Definir que el SGSI incluye solo la seguridad de la red de oficinas.
4. **¿Cómo afecta el alcance en la implementación del SGSI?**  
   Define qué recursos y controles específicos se necesitan según las áreas cubiertas.  
   *Ejemplo*: Si el SGSI cubre solo TI, no se aplican controles para otras áreas.
5. **¿Qué son las partes interesadas en ISO 27001?**  
   Personas o grupos que afectan o son afectados por la seguridad de la información.  
   *Ejemplo*: Clientes, empleados, proveedores y reguladores.
6. **¿Por qué es importante identificar las necesidades de las partes interesadas?**  
   Para asegurarse de que el SGSI cumple con sus expectativas y requisitos.  
   *Ejemplo*: Asegurar la confidencialidad de los datos de clientes según la ley de privacidad.
7. **¿Qué implica la comprensión de la organización en un SGSI?**  
   Conocer cómo factores internos y externos afectan la seguridad de la información.  
   *Ejemplo*: Evaluar el impacto de cambios en la dirección de la empresa en la seguridad.
8. **¿Qué información debe incluirse en la declaración de aplicabilidad?**  
   Una lista de controles de seguridad seleccionados y su justificación.  
   *Ejemplo*: Incluir un firewall para proteger la red, indicando su función.
9. **¿Qué aspectos clave se evalúan al establecer el contexto de la organización?**  
   Entorno interno y externo, partes interesadas, y objetivos de seguridad.  
   *Ejemplo*: Analizar si el entorno competitivo presenta riesgos a la información.
10. **¿Qué es un riesgo en el contexto de ISO 27001?**  
    La posibilidad de que una amenaza afecte la confidencialidad, integridad o disponibilidad de la información.  
    *Ejemplo:* Riesgo de que un virus informático afecte los sistemas de la empresa.

**Bloque 3: Liderazgo (Capítulo 5)**

1. **¿Cuál es el rol de la alta dirección en el SGSI?**  
   Asegurar el compromiso y proporcionar recursos para implementar y mantener el SGSI.  
   *Ejemplo*: La gerencia aprueba y financia un nuevo sistema de protección de datos.
2. **¿Por qué es importante la política de seguridad de la información?**  
   Establece las directrices y el compromiso de la organización con la seguridad de la información.  
   *Ejemplo*: La política detalla que todos los empleados deben proteger la información de clientes.
3. **¿Cómo puede la alta dirección demostrar compromiso con el SGSI?**  
   Asignando recursos, promoviendo la cultura de seguridad y participando en revisiones del SGSI.  
   *Ejemplo*: La gerencia asiste a reuniones periódicas de evaluación del SGSI.
4. **¿Qué responsabilidades tienen los líderes en ISO 27001?**  
   Definir y comunicar los objetivos de seguridad y asegurar el cumplimiento de la norma.  
   *Ejemplo*: El director de TI supervisa la implementación de controles de acceso.
5. **¿Cuál es el propósito de asignar roles y responsabilidades en el SGSI?**  
   Garantizar que todos sepan su rol y contribución en la protección de la información.  
   *Ejemplo*: El equipo de soporte TI se encarga de monitorear incidentes de seguridad.
6. **¿Qué significa “gobernanza” en el contexto del SGSI?**  
   Supervisar y dirigir las políticas y procesos del SGSI para asegurar el cumplimiento.  
   *Ejemplo*: La alta dirección establece un comité para revisar la eficacia del SGSI.
7. **¿Qué se debe incluir en una política de seguridad de la información?**  
   Los objetivos de seguridad, el compromiso de la organización y las directrices de protección.  
   *Ejemplo*: La política indica que solo personal autorizado puede acceder a información sensible.
8. **¿Qué responsabilidades tiene un oficial de seguridad de la información?**  
   Coordinar y supervisar las actividades de seguridad, como la evaluación de riesgos.  
   *Ejemplo*: El oficial revisa los controles de acceso y responde a incidentes de seguridad.
9. **¿Qué es la cultura de seguridad y por qué es importante?**  
   Actitudes y prácticas de los empleados que promueven la protección de la información.  
   *Ejemplo*: Los empleados informan incidentes de seguridad y siguen las políticas.
10. **¿Cómo afecta la participación de la alta dirección al éxito del SGSI?**  
    La participación activa de la dirección motiva al personal y asegura los recursos necesarios.  
    *Ejemplo:* La gerencia asigna presupuesto para nuevas herramientas de seguridad.

**Bloque 4: Planificación del SGSI (Capítulo 6)**

1. **¿Qué es la evaluación de riesgos?**  
   Identificar y analizar posibles amenazas que puedan afectar la seguridad de la información.  
   *Ejemplo*: Evaluar el riesgo de ataques cibernéticos en la red corporativa.
2. **¿Por qué es fundamental gestionar los riesgos en el SGSI?**  
   Permite implementar controles adecuados para reducir los riesgos a niveles aceptables.  
   *Ejemplo*: Identificar y minimizar el riesgo de pérdida de datos de clientes.
3. **¿Qué factores se consideran en el análisis de riesgos?**  
   Amenazas, vulnerabilidades y el impacto en la información si ocurre un incidente.  
   *Ejemplo*: Considerar el impacto de un fallo de seguridad en el sistema de pago en línea.
4. **¿Qué es una matriz de riesgos?**  
   Una herramienta que clasifica los riesgos según su probabilidad y su impacto.  
   *Ejemplo*: Un riesgo alto puede ser un ataque de phishing con alto impacto y probabilidad.
5. **¿Cómo se establecen los objetivos de seguridad de la información?**  
   Definiendo metas claras que alineen la seguridad con las necesidades del negocio.  
   *Ejemplo*: Reducir los incidentes de acceso no autorizado en un 20% en un año.
6. **¿Qué se debe considerar al definir un plan de tratamiento de riesgos?**  
   Seleccionar las medidas o controles para mitigar, evitar, transferir o aceptar riesgos.  
   *Ejemplo*: Implementar autenticación multifactor para reducir el riesgo de acceso no autorizado.
7. **¿Qué es una acción correctiva en ISO 27001?**  
   Medida tomada para corregir y prevenir la recurrencia de una no conformidad.  
   *Ejemplo*: Cambiar contraseñas y fortalecer controles tras un acceso no autorizado.
8. **¿Cuál es la diferencia entre mitigar y transferir un riesgo?**  
   Mitigar reduce el impacto/probabilidad del riesgo; transferir delega el riesgo a un tercero.  
   *Ejemplo*: Contratar un seguro de ciberseguridad para transferir el riesgo.
9. **¿Qué implica el tratamiento de riesgos?**  
   Implementar controles y medidas para reducir el impacto o la probabilidad de los riesgos.  
   *Ejemplo*: Instalar un firewall para minimizar el riesgo de intrusiones en la red.
10. **¿Cómo se definen los controles en el SGSI?**  
    Seleccionando medidas basadas en el análisis de riesgos para proteger la información.  
    *Ejemplo*: Elegir cifrado para proteger la información sensible almacenada.

**Bloque 5: Soporte (Capítulo 7)**

1. **¿Qué tipo de recursos son necesarios para un SGSI efectivo?**  
   Recursos humanos, tecnológicos y financieros para implementar y mantener el SGSI.  
   *Ejemplo*: Asignar un equipo de TI y presupuesto para implementar controles de seguridad.
2. **¿Por qué es importante la competencia del personal en el SGSI?**  
   El personal capacitado puede aplicar correctamente los controles y prevenir incidentes.  
   *Ejemplo*: Entrenar a los empleados para reconocer intentos de phishing.
3. **¿Qué tipo de formación necesita el personal en seguridad de la información?**  
   Formación en políticas de seguridad, detección de amenazas y buenas prácticas.  
   *Ejemplo*: Capacitar a empleados en el uso seguro de contraseñas.
4. **¿Qué son las comunicaciones internas en ISO 27001?**  
   El proceso para compartir información relevante del SGSI dentro de la organización.  
   *Ejemplo*: Informar a los empleados sobre nuevas políticas de seguridad por correo interno.
5. **¿Cuál es la importancia de la documentación en el SGSI?**  
   Asegura que las políticas y procedimientos sean claros, accesibles y consistentes.  
   *Ejemplo*: Tener un manual de seguridad accesible a todos los empleados.
6. **¿Qué es la información documentada en ISO 27001?**  
   Documentación oficial que incluye políticas, procedimientos y registros del SGSI.  
   *Ejemplo*: Un registro de incidentes de seguridad.
7. **¿Qué aspectos se deben comunicar a las partes interesadas?**  
   Aspectos como políticas de seguridad, riesgos, incidentes y mejoras en el SGSI.  
   *Ejemplo*: Informar a los clientes sobre cómo se protegen sus datos.
8. **¿Cómo se gestiona la información documentada en el SGSI?**  
   Asegurando su disponibilidad, actualización y protección contra accesos no autorizados.  
   *Ejemplo*: Usar un sistema de gestión de documentos con control de acceso.
9. **¿Qué tipo de evidencias se deben registrar?**  
   Evidencias de cumplimiento, como registros de auditorías, capacitaciones y evaluaciones de riesgos.  
   *Ejemplo*: Un informe de auditoría interna como evidencia de cumplimiento.
10. **¿Por qué es esencial el soporte en un SGSI?**  
    Sin el soporte adecuado, el SGSI no se puede implementar ni mantener eficazmente.  
    *Ejemplo*: Proporcionar recursos para mantener actualizados los sistemas de seguridad.

**Bloque 6: Operación (Capítulo 8)**

1. **¿Qué implica la implementación de controles en el SGSI?**  
   Poner en práctica las medidas necesarias para reducir los riesgos de seguridad.  
   *Ejemplo*: Instalar un sistema de autenticación multifactor en los sistemas de TI.
2. **¿Qué es la evaluación de riesgos en la operación?**  
   Revisar y monitorear los riesgos durante el funcionamiento del SGSI para adaptarse a cambios.  
   *Ejemplo*: Identificar nuevos riesgos si se introduce una tecnología en la red.
3. **¿Cuál es el propósito de los procedimientos operativos?**  
   Guiar a los empleados sobre cómo realizar tareas de manera segura y conforme a la política.  
   *Ejemplo*: Tener un procedimiento para el manejo seguro de datos de clientes.
4. **¿Cómo se gestionan los cambios en el SGSI?**  
   Evaluando el impacto de los cambios y adaptando los controles de seguridad necesarios.  
   *Ejemplo*: Revisar las políticas de seguridad tras actualizar el software de la empresa.
5. **¿Qué es un incidente de seguridad de la información?**  
   Un evento que pone en riesgo la confidencialidad, integridad o disponibilidad de la información.  
   *Ejemplo*: Un acceso no autorizado a una base de datos de clientes.
6. **¿Cuál es el propósito de un plan de respuesta a incidentes?**  
   Definir los pasos a seguir para gestionar y minimizar el impacto de incidentes de seguridad.  
   *Ejemplo*: Tener un plan para desconectar un sistema comprometido y notificar a los usuarios.
7. **¿Qué es la continuidad de negocio en el contexto del SGSI?**  
   Garantizar que los servicios críticos se mantengan en funcionamiento durante una interrupción.  
   *Ejemplo*: Tener copias de seguridad para recuperar datos en caso de un fallo del sistema.
8. **¿Cómo se gestionan los activos de información durante la operación?**Manteniéndolos actualizados, protegidos y con acceso controlado para evitar riesgos.  
   *Ejemplo*: Registrar cada equipo de TI que contiene información crítica.
9. **¿Qué es el control de acceso?**  
   Restringir el acceso a la información solo a las personas autorizadas.  
   *Ejemplo*: Permitir solo a los gerentes acceder a los datos financieros.
10. **¿Cuál es el propósito de las copias de seguridad?**  
    Asegurar que la información pueda recuperarse en caso de pérdida o daño.  
    *Ejemplo*: Realizar copias de seguridad diarias de la base de datos de clientes.

**Bloque 7: Evaluación del Desempeño (Capítulo 9)**

1. **¿Qué es el monitoreo en el SGSI?**  
   Supervisar continuamente los controles y procesos para asegurar su efectividad.  
   *Ejemplo*: Revisar regularmente los registros de acceso a sistemas críticos.
2. **¿Cuál es el objetivo de una auditoría interna en ISO 27001?**  
   Evaluar si el SGSI cumple con los requisitos de la norma y detectar áreas de mejora.  
   *Ejemplo:* Verificar si los procedimientos de seguridad se siguen correctamente.
3. **¿Qué se evalúa en una revisión por la dirección?**  
   El rendimiento del SGSI y su alineación con los objetivos de la organización.  
   *Ejemplo*: La gerencia revisa los incidentes de seguridad y el cumplimiento de objetivos.
4. **¿Por qué es importante la medición en el SGSI?**  
   Permite evaluar la efectividad de los controles y ajustarlos según los resultados.  
   *Ejemplo*: Medir el número de incidentes reportados para evaluar la efectividad de los controles.
5. **¿Cómo se mide el desempeño del SGSI?**  
   A través de indicadores de rendimiento, auditorías y revisiones periódicas.  
   *Ejemplo*: Usar el tiempo de respuesta ante incidentes como un indicador de desempeño.
6. **¿Qué información debe incluir un informe de auditoría interna?**  
   Hallazgos, no conformidades, áreas de mejora y acciones recomendadas.  
   *Ejemplo*: Un informe que señale falta de capacitación en seguridad para algunos empleados.
7. **¿Qué se hace con los hallazgos de una auditoría interna?**  
   Se implementan acciones correctivas y se revisa su efectividad.  
   *Ejemplo*: Corregir una deficiencia en los procedimientos de control de acceso.
8. **¿Por qué es fundamental la revisión por la dirección?**  
   Asegura el compromiso de la alta dirección y la alineación del SGSI con los objetivos de la empresa.  
   *Ejemplo*: La gerencia revisa y aprueba el presupuesto para mejoras en seguridad.
9. **¿Qué significa "mejora continua" en el SGSI?**  
   Ajustar y actualizar el SGSI regularmente para adaptarse a cambios y nuevos riesgos.  
   *Ejemplo*: Actualizar las políticas de seguridad cada año.
10. **¿Qué herramientas se pueden utilizar para el monitoreo de la seguridad de la información?**  
    Sistemas de detección de intrusiones, registros de acceso y auditorías periódicas.  
    *Ejemplo*: Usar un sistema de detección de intrusiones para monitorear actividades sospechosas.

**Bloque 8: Mejora Continua (Capítulo 10)**

1. ¿**Qué es una acción correctiva?**  
   Medida para eliminar una no conformidad y prevenir su repetición.  
   *Ejemplo*: Implementar una nueva política de contraseñas tras detectar accesos no autorizados.
2. ¿**Qué significa "no conformidad"?**  
   Cuando algo no cumple con los requisitos de la norma o el SGSI.  
   *Ejemplo*: No realizar copias de seguridad diarias cuando la política lo requiere.
3. ¿**Qué acciones se toman en caso de una no conformidad?**  
   Se implementan acciones correctivas para resolver el problema y evitar su repetición.  
   *Ejemplo*: Cambiar los procedimientos de acceso tras una auditoría que revele deficiencias.
4. ¿**Qué es una acción preventiva?**  
   Medida para evitar la ocurrencia de una no conformidad antes de que suceda.  
   *Ejemplo*: Implementar una capacitación en seguridad para reducir el riesgo de errores humanos.
5. ¿**Por qué es importante la mejora continua en ISO 27001?**  
   Permite adaptar el SGSI a cambios en el entorno y mejorar su eficacia.  
   *Ejemplo*: Revisar y mejorar controles tras un incidente de seguridad.
6. ¿**Qué rol juega el análisis de causas en la mejora continua?**  
   Identifica las causas raíz de los problemas para implementar acciones efectivas.  
   *Ejemplo*: Analizar por qué un incidente ocurrió para prevenir su recurrencia.
7. ¿**Cómo se implementa una mejora en el SGSI?**  
   Identificando áreas de mejora, planificando cambios y verificando su efectividad.  
   *Ejemplo*: Mejorar los controles de acceso basándose en los hallazgos de una auditoría.
8. ¿**Qué es la revisión posterior a una acción correctiva?**  
   Evaluar si la acción correctiva fue efectiva y resolvió la no conformidad.  
   *Ejemplo*: Revisar si un nuevo protocolo de contraseñas ha reducido los accesos no autorizados.
9. ¿**Qué impacto tiene la mejora continua en el SGSI?**  
   Fortalece el SGSI y mejora su capacidad de adaptación frente a nuevos riesgos.  
   *Ejemplo*: La actualización periódica de políticas refuerza la seguridad frente a amenazas cambiantes.
10. ¿**Qué procesos se utilizan para evaluar la eficacia de las acciones correctivas?**  
    Revisiones de auditoría, monitoreo de resultados y análisis de desempeño.  
    *Ejemplo: Realizar una auditoría de seguimiento para verificar la implementación de cambios.*

**Bloque 9: Anexo A - Controles de Seguridad**

1. ¿**Qué es el Anexo A en ISO 27001?**  
   Una lista de controles de seguridad que ayuda a mitigar los riesgos de información.  
   *Ejemplo*: Usar cifrado para proteger datos sensibles.
2. **¿Cuántos controles de seguridad se incluyen en el Anexo A?**Hay 114 controles agrupados en 14 categorías.  
   *Ejemplo*: Controles de acceso, criptografía y gestión de incidentes.
3. **¿Qué es un control organizativo?**Medidas para establecer políticas y procedimientos que apoyan la seguridad.  
   *Ejemplo*: Tener una política de seguridad de la información.
4. **¿Qué son los controles físicos?**Medidas para proteger los activos físicos contra accesos no autorizados.  
   *Ejemplo*: Colocar cerraduras en las salas de servidores.
5. **¿Cuál es el propósito de los controles de acceso?**Asegurar que solo personas autorizadas tengan acceso a la información.  
   *Ejemplo*: Requerir credenciales para acceder al sistema.
6. **¿Qué es un control de respuesta a incidentes?**Procedimientos para manejar y minimizar el impacto de incidentes de seguridad.  
   *Ejemplo*: Tener un plan para reaccionar ante un ataque cibernético.
7. **¿Qué son los controles de continuidad del negocio?**Medidas para asegurar que la operación continúe durante incidentes.  
   *Ejemplo*: Tener un respaldo de datos en caso de fallo del sistema.
8. **¿Qué tipo de controles se aplican a la criptografía?**Medidas para proteger la información mediante cifrado y manejo de claves.  
   *Ejemplo*: Cifrar los datos de clientes en la base de datos.
9. **¿Cuál es el rol de los controles de protección contra malware?**Prevenir y detectar software malicioso que podría dañar o comprometer datos.  
   *Ejemplo*: Usar un software antivirus actualizado.
10. **¿Qué significa “control tecnológico” en el contexto del Anexo A?**Medidas que se implementan mediante tecnología para proteger la información.  
    *Ejemplo*: Firewalls para controlar el tráfico de la red.

**Bloque 10: Auditoría y Cumplimiento**

1. **¿Cuál es el propósito de una auditoría de certificación?**Verificar si el SGSI cumple con los requisitos de ISO 27001 para obtener la certificación.  
   *Ejemplo*: Realizar una auditoría anual para obtener la certificación ISO 27001.
2. **¿Qué rol tiene el auditor en ISO 27001?**Evaluar la conformidad del SGSI y recomendar mejoras.  
   *Ejemplo*: El auditor revisa si se siguen los procedimientos de seguridad.
3. **¿Qué significa conformidad en ISO 27001?**Cumplir con los requisitos de la norma y las políticas establecidas por el SGSI.  
   *Ejemplo*: Que la empresa aplique correctamente las políticas de acceso.
4. **¿Qué es una no conformidad mayor?**Un incumplimiento significativo que afecta la efectividad del SGSI.  
   *Ejemplo*: No tener controles de acceso en una base de datos sensible.
5. **¿Cuál es la diferencia entre una auditoría interna y una externa?**La auditoría interna la realiza la organización; la externa, un auditor externo.  
   *Ejemplo*: Auditoría interna anual y auditoría externa para certificación.
6. **¿Qué documentación se requiere para la auditoría de ISO 27001?**Documentos como la declaración de aplicabilidad, políticas y registros de auditoría.  
   *Ejemplo*: Registro de incidentes y políticas de acceso.
7. **¿Qué se evalúa en una auditoría de seguimiento?**La implementación de las acciones correctivas tras una auditoría previa.  
   *Ejemplo*: Verificar que se solucionaron las no conformidades detectadas.
8. **¿Cuál es el propósito de una auditoría de recertificación?**Renovar la certificación asegurando que el SGSI sigue cumpliendo con ISO 27001.  
   *Ejemplo*: Realizar una auditoría cada tres años para mantener la certificación.
9. **¿Qué es la declaración de aplicabilidad en el contexto de una auditoría?**Un documento que especifica los controles implementados y su justificación.  
   *Ejemplo*: Incluir cifrado como control en la declaración de aplicabilidad.
10. **¿Por qué es importante la evidencia en una auditoría?**Permite al auditor verificar que los controles del SGSI funcionan adecuadamente.  
    *Ejemplo*: Proporcionar registros de accesos como evidencia de control de acceso.