Comenzado el	miércoles, 5 de noviembre de 2025, 18:30
Estado	Finalizado
Finalizado en	miércoles, 5 de noviembre de 2025, 18:48
Tiempo empleado	17 minutos 41 segundos
Calificación	**75,6** de 100,0

Pregunta **1**

Finalizado

Se puntúa 4,0 sobre 4,0

Según ISO 27013, ¿qué paso es esencial al iniciar la integración de un SGSI y un SGS-TI?

Seleccione una:

- a. Eliminar todos los controles de seguridad existentes.
- b. Realizar un análisis de brechas para identificar solapamientos.
- c. Contratar un proveedor externo de servicios en la nube.
- d. Implementar políticas separadas para cada sistema.

Pregunta **2**

Finalizado

Se puntúa 4,0 sobre 4,0

En el ámbito de la gestión de riesgos informáticos, ¿Cuál de los siguientes conceptos, aunque no se enfoca estrictamente en la prevención física, es crucial para anticiparse a posibles problemas?

Seleccione una:

- a. Diseño de interfaces de usuario atractivas y seguras
- b. Identificación y análisis de amenazas y vulnerabilidades
- c. Mejora de la seguridad del cliente
- d. Monitoreo de la salud física de los servidores

Pregunta **3**

Finalizado

Se puntúa 4,0 sobre 4,0

¿Cuál es el objetivo principal de la ISO 27007?

Seleccione una:

- a. Evaluar la eficacia del sistema de gestión y proporcionar recomendaciones para mejorarlo.
- b. Evaluar la eficacia y adecuación del sistema de gestión y proporcionar recomendaciones para mejorarlo.
- c. Evaluar la confidencialidad y adecuación del sistema de gestión y proporcionar recomendaciones para mejorarlo.
- d. Evaluar la adecuación del sistema de gestión con el objetivo de sacra conclusiones.

Pregunta **4**

Finalizado

Se puntúa 4,0 sobre 4,0

Dentro de la gestión de riesgos informáticos, aunque la prioridad no es directamente el monitoreo de sistemas físicos, ¿Qué proceso es esencial para reducir la probabilidad de incidentes?

Seleccione una:

- a. Capacitación en desarrollo de software agiles y seguros
- b. Instalación de antivirus en activos de la información
- c. Evaluación continua de la efectividad de los controles de seguridad
- d. Auditoría de los recursos financieros e internos cada cierto tiempo

Pregunta **5**

Finalizado

Se puntúa 4,0 sobre 4,0

Si bien no se trata de una estrategia de marketing digital, la gestión de riesgos en TI implica una importancia indirecta para cuál de las siguientes prácticas que previene amenazas?

Seleccione una:

- a. Desarrollo de políticas de comunicación interna
- b. Implementación de controles de acceso y autenticación con mínimo 2 tipos de los 3 que se tienen
- c. Publicidad segura en redes sociales
- d. Estrategias de fidelización de clientes con acceso seguro a las plataformas

Pregunta **6**

Finalizado

Se puntúa 4,0 sobre 4,0

¿Qué aspecto es crítico para medir el éxito de la gobernanza según ISO 27014?

Seleccione una:

- a. Cantidad de incidentes reportados.
- b. Número de empleados capacitados en cifrado.
- c. Evaluación continua del desempeño mediante métricas.
- d. Eliminación de duplicidades en la documentación.
- e. Ninguna de las anteriores

Pregunta **7**

Finalizado

Se puntúa -0,2 sobre 4,0

¿Cuál es el principal aporte de ISO 27017 frente a ISO 27002?

Seleccione una:

- a. Adaptar controles genéricos a servicios en la nube y añadir controles cloud-exclusivos.
- b. Reemplazar todos los controles de ISO 27002 en entornos on-premise.
- c. Centralizar la gestión de incidentes en autoridades gubernamentales.
- d. liminar la necesidad de acuerdos de nivel de servicio (SLAs).

Pregunta **8**

Finalizado

Se puntúa 0,0 sobre 4,0

Los requisitos generales a los que hace referencia la ISO-27006 son:

Seleccione una o más de una:

- a. Orientación especifica del SGSI en relacion con la imparcialidad
- b. Listado del trabajo que pudiera estar en conflicto dentro de la empresa en cuestion
- c. Inclusión de una lista de todas las actividades que se pueden realizar fuera
- d. Son correctas a), b) y c)
- e. Son correctas solo a) y c)
- f. Son correctas solo b) y c)

Pregunta **9**

Finalizado

Se puntúa 4,0 sobre 4,0

La ISO/IEC 27021 se enfoca en diversas áreas de competencia necesarias para un profesional de SGSI. ¿Cuál de las siguientes áreas es considerada una competencia clave que trasciende lo puramente técnico, según la norma?

Seleccione una:

- a. Liderazgo, comunicación y gestión de partes interesadas.
- b. Diseño y administración de redes de área local (LAN).
- c. Exclusivamente el conocimiento de los controles de cifrado (criptografía).
- d. Auditoría interna y externa de sistemas operativos.

Pregunta **10**

Finalizado

Se puntúa -0,4 sobre 4,0

Qué control de ISO 27002 adapta ISO 27019 para entornos IACS/SCADA?

Seleccione una:

- a. Gestión de derechos de autor software.
- b. Política de teletrabajo.
- c. Cifrado de correos electrónicos.
- d. Segmentación de redes industriales (zonas desmilitarizadas OT/IT).

Pregunta **11**

Finalizado

Se puntúa 0,0 sobre 4,0

Aunque no se centra en reducir costos de TI, una gestión de riesgos efectiva prioriza indirectamente qué proceso para minimizar el impacto de los eventos adversos?

Seleccione una:

- a. Optimización de recursos de hardware para mejorar la seguridad
- b. Mejora en la capacitación general de empleados informaticos
- c. Aumento de la productividad en el equipo de TI en seguridad
- d. Desarrollo de un plan de respuesta y recuperación ante incidentes

Pregunta 12

Finalizado

Se puntúa 4,0 sobre 4,0

¿Cuál es una de las razones clave para implementar la ISO 27011 en una organización de telecomunicaciones?

Seleccione una:

- a. Incrementar la velocidad de las conexiones de red
- b. Mejorar la satisfacción del cliente en cuanto a calidad del servicio y asegurar la confidencialidad, integridad y disponibilidad de los datos en redes de telecomunicaciones
- c. Asegurar la confidencialidad, integridad y disponibilidad de los datos en redes de telecomunicaciones
- d. Mejorar la satisfacción del cliente en cuanto a calidad del servicio

Pregunta 13

Finalizado

Se puntúa 4,0 sobre 4,0

¿Cuál es el propósito principal de la norma ISO 27006?

Seleccione una:

- a. Establecer requisitos de gestión para las empresas certificadoras
- b. Proveer requisitos específicos para la acreditación de entidades de certificación en sistemas de gestión de seguridad de la información
- c. Evaluar el cumplimiento de sistemas de gestión integral
- d. Regular el uso de sistemas de gestión de calidad

Pregunta 14

Finalizado

Se puntúa 1,0 sobre 4,0

La norma **ISO/IEC 27016** se enfoca en la **gestión económica de la seguridad de la información**. Empareje las definiciones a su correspondiente

Optimización de inversiones	Asignación eficiente de recursos para maximizar la protección.
Métricas financieras:	Proporciona directrices para evaluar y optimizar la relación costo-beneficio de los controles de seguridad
Alineación con objetivos de negocio:	Uso de indicadores como ROSI (Return on Security Investment) para medir efectividad.
Análisis costo-beneficio:	Vinculación de la seguridad con la rentabilidad y sostenibilidad organizacional.

Pregunta **15**

Finalizado

Se puntúa 4,0 sobre 4,0

Aunque la gestión de riesgos informáticos no implica directamente la creación de nuevos sistemas, ¿Cuál es el enfoque clave que ayuda a mitigar la probabilidad de exposición a riesgos?

Seleccione una:

- a. Formación en ventas y atención al cliente, realizando una gestión de riesgos
- b. Optimización del diseño gráfico en aplicaciones con interfaces seguras
- c. Reducción de costos en servicios de TI, comprando solo los activos necesarios
- d. Análisis y priorización de activos críticos y amenazas, asegurando los mismos con controles seguros

Pregunta **16**

Finalizado

Se puntúa 4,0 sobre 4,0

¿Cuáles de los siguientes aspectos son clave en la ISO 27008?

Seleccione una:

- a. La capacitación de empleados en temas de calidad de servicios y seguridad
- b. La planificación de la seguridad lógica y física en la organización
- c. La revisión independiente y evaluación objetiva de los controles de seguridad.
- d. La evaluación de la satisfacción del cliente en el SGSI

Pregunta **17**

Finalizado

Se puntúa 4,0 sobre 4,0

¿Cómo se relaciona directamente la ISO/IEC 27021 con la norma de requisitos **ISO/IEC 27001**?

Seleccione una:

- a. La 27021 establece las métricas exactas para medir la eficacia del SGSI definido en la 27001.
- b. La 27021 es la lista de controles de seguridad que se deben implementar para la certificación ISO/IEC 27001.
- c. La 27021 reemplaza a la 27001 al ser una versión más reciente y específica.
- d. La 27021 define la cualificación necesaria para los individuos que ayudan a la organización a cumplir e implementar los requisitos de la 27001.

Pregunta **18**

Finalizado

Se puntúa 4,0 sobre 4,0

Si un cliente solicita eliminar sus datos personales, ¿qué debe garantizar el CSP según ISO 27018?

Seleccione una:

- a. Transferirlos a otro proveedor sin notificación.
- b. Eliminación verificable de todas las copias (incluidas backups).
- c. Conservar una copia "anónima" para análisis futuros.
- d. Desactivar el acceso pero retener datos 90 días.

Pregunta **19**

Finalizado

Se puntúa 4,0 sobre 4,0

Según ISO 27010, ¿Qué aspecto es clave para el intercambio de información entre organizaciones?

Seleccione una:

- a. Eliminación de registros después de 30 días.
- b. Gestión de riesgos compartidos y controles de acceso.
- c. Establecimiento de acuerdos de confidencialidad (SLAs).
- d. Uso exclusivo de redes privadas.

Pregunta **20**

Finalizado

Se puntúa 4,0 sobre 4,0

Según ISO 27018, ¿qué acción está PROHIBIDA para un proveedor cloud respecto a datos personales?

Seleccione una:

- a. Usarlos para publicidad segmentada con consentimiento explícito.
- b. Almacenarlos en múltiples regiones geográficas.
- c. Realizar copias de seguridad automáticas y venderlas.
- d. Usarlos para publicidad segmentada sin consentimiento explícito.

Pregunta **21**

Finalizado

Se puntúa 4,0 sobre 4,0

El objetivo de las directrices proporcionadas por ISO/IEC 27022 es:

Seleccione una:

- a. Asegurar que los incidentes de seguridad se gestionen de manera efectiva para reducir el daño y el tiempo de inactividad.
- b. Requerir la implementación de todos los controles del Anexo A de la ISO/IEC 27001 sin excepción.
- c. Ser un estándar certificable que reemplace a la ISO/IEC 27001.
- d. Establecer los requisitos contractuales obligatorios para todos los proveedores de servicios en la nube.

Pregunta **22**

Finalizado

Se puntúa 3,6 sobre 4,0

Segun **ISO/IEC 27013, Entre sus aspectos clave destacan:** 😉

Seleccione una o más de una:

- a. **Integración de procesos**
- b. **Analisis de brechas**
- c. **Gestión de riesgos**
- d. **Enfoque práctico**

Pregunta **23**

Finalizado

Se puntúa 4,0 sobre 4,0

Uno de los aspectos clave abordados por la ISO/IEC 27017 es la **responsabilidad compartida** en el entorno cloud. ¿Cuál es el objetivo de este control?

Seleccione una:

- a. Establecer que la responsabilidad del cifrado de datos recae únicamente en el cliente, independientemente del modelo de servicio.
- b. Eliminar la necesidad de que los clientes implementen cualquier control de seguridad al usar servicios cloud.
- c. Definir claramente los roles y las responsabilidades de seguridad de la información entre el cliente y el proveedor del servicio cloud.
- d. Asegurar que toda la responsabilidad de seguridad recaiga sobre el proveedor de servicios en la nube (CSP).

Pregunta **24**

Finalizado

Se puntúa -0,4 sobre 4,0

En el ciclo de gestión de incidentes que promueven normas como la ISO/IEC 27022, ¿cuál de las siguientes es una fase clave que ocurre después de la detección del incidente?

Seleccione una:

- a. Creación de la política de seguridad de la información.
- b. Evaluación, respuesta y recuperación.
- c. Evaluación, respuesta, corrección y mitigacion.
- d. Selección de la Declaración de Aplicabilidad (SoA).

Pregunta **25**

Finalizado

Se puntúa 4,0 sobre 4,0

Uno de los principios clave de la Gobernanza de la Seguridad de la Información (GSI) en la ISO/IEC 27014 es **'Adoptar una aproximación basada en el riesgo'**. ¿Qué implica este principio?

Seleccione una:

- a. Delegar la responsabilidad de la gestión de riesgos exclusivamente al área de Tecnologías de la Información (TI).
- b. Evitar cualquier inversión en seguridad si el riesgo es menor a un umbral predefinido.
- c.
  Asegurar que las decisiones de seguridad se tomen en función del riesgo y se alineen con el apetito al riesgo de la organización.

  Asegurar que las decisiones de seguridad se tomen en función del riesgo y se alineen con el apetito al riesgo de la organización.
- d. Asegurar el cumplimiento total de todas las regulaciones externas sin considerar el costo.

◀ ISO-27018 y 19

Ir a...