EXAMEN PARCIAL

¿Cuál es la versión más reciente del estándar ISO para un Sistema de Gestión de Seguridad de Información?

Ocultar opciones de respuesta

A ISO/IEC 20000:2011

Correcta:
ISO/IEC 27001:2022
Respuesta correcta

C ISO/IEC 27001:2013

D ISO/IEC 37000:2023

Pregunta 2

0,5 / 0,5

¿Por qué el SGSI es un proceso continuo?

Ocultar opciones de respuesta

A Porque los riesgos no se eliminan

Correcta:
Porque los riesgos se evalúan y actualizan constantemente
Respuesta correcta

C Porque se actualiza después de cada evento

D Porque la norma marca un ciclo de mejora

Pregunta 3

0,5 / 0,5

La seguridad de la información busca preservar:

Ocultar opciones de respuesta

A Autenticidad, privacidad, seguridad

Correcta:
Confidencialidad, Integridad, Disponibilidad
Respuesta correcta

C Riesgos, amenazas e impactos

D Vulnerabilidades

Pregunta 4

0,5 / 0,5

Debilidad de un activo o control que puede ser explotada por una amenaza, es:

Ocultar opciones de respuesta

Correcta:
Vulnerabilidad

Respuesta correcta

B Riesgo

C Confidencialidad

D Impacto

Pregunta 5

0,5 / 0,5

¿Qué estándar podríamos emplear como referencia para un proceso de Gestión de la Evidencia Digital (Identificación, Recolección, Adquisición y Preservación)

Ocultar opciones de respuesta

A ISO 37000

B ISO 9001

Correcta:
ISO 27037

Respuesta correcta

D ISO 31000

Pregunta 6

0,5 / 0,5

¿Seguridad de la información se entiende como un proceso de negocio más?

- V **Verdadero** — Respuesta correcta
- F Falso

Pregunta 7

0 / 0,5

Tercerizar el proceso de respaldo de la información es un ejemplo de:

Ocultar opciones de respuesta

- **Incorrecta:** Transferir el riesgo
- B Mitigar el riesgo — Respuesta correcta
- C Evitar el Riesgo
- D Tercerizar el Riesgo

Pregunta 8

0,5 / 0,5

¿Qué es ISO 27001?

Ocultar opciones de respuesta

- A Es un estándar internacional que provee un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SMS.
- **Correcta:** Es un estándar internacional que provee un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un ISMS. — Respuesta correcta
- C Es un conjunto de mejores prácticas de la industria de TI para Seguridad de la Información.
- D Es un marco de referencia teórico para asegurar el apego normativo de Seguridad de la Información.

Pregunta 10

0,5 / 0,5

El compromiso y soporte de la alta dirección hacia la seguridad informática se puede obtener MEJOR a través de presentaciones que:

Ocultar opciones de respuesta

A usen ejemplos ilustrativos de ataques exitosos.

B expliquen el riesgo técnico para la organización.

C evalúen la organización comparándola contra buenas prácticas de seguridad.

Correcta:
vinculen los riesgos de seguridad con los objetivos clave del negocio.

Respuesta correcta

Pregunta 9

0,5 / 0,5

La sala de ordenadores está protegida por un lector de tarjetas. Sólo el departamento de gestión de sistemas posee una tarjeta. ¿Qué tipo de medida de seguridad es ésta?

Ocultar opciones de respuesta

A Una medida seguridad correctiva

Correcta:
Una medida de seguridad física

Respuesta correcta

C Una medida de seguridad lógica

D Una medida de seguridad e inhibidora

Pregunta 11

0,5 / 0,5

El proceso de Respuesta a Incidentes de seguridad de la información, debe incluir:

Ocultar opciones de respuesta

A la realización de análisis forenses

B análisis BIA

C escalamiento, según corresponda

D Todas las opciones anteriores son correctas

Correcta:
Solamente las opciones "A" y "C" son correctas

Respuesta correcta

Pregunta 12

0,5 / 0,5

¿De qué es responsable el comité de gestión de seguridad de la información?

Ocultar opciones de respuesta

A De mantener actualizado el SGSI.

Correcta:
De revisar y aprobar las distintas actividades del SGSI

Respuesta correcta

C De comunicar a la organización los avances del SGSI

D De presentar las auditorías de certificación

Pregunta 13

0,5 / 0,5

¿Cuántas cláusulas tiene la norma ISO 27001 (Estructura de Alto Nivel - SL)?

Ocultar opciones de respuesta

A 7

B 8

C 9

Correcta:
10

Respuesta correcta

Pregunta 14

0,5 / 0,5

¿Cuáles son las fases del ciclo PDCA?

Ocultar opciones de respuesta

A Plantear, Hacer, Verificar, Actuar

B Planear, Hacer, Verificar, Asegurar

Correcta:
Planear, Hacer, Verificar, Actuar

Respuesta correcta

D Planear, Validar, Verificar, Actuar

Pregunta 15

0 / 0,5

En relación a la "Recolección de Evidencia", a qué se denomina el proceso de: Crear una copia de los datos dentro de un conjunto definido

Ocultar opciones de respuesta

A Identificación

B Recolección

C Adquisición

Respuesta correcta

Incorrecta:
Preservación

Pregunta 16

0 / 0,5

¿Cómo se les llama a las personas que intentan robar información personal?

Ocultar opciones de respuesta

A Oportunistas

B Delincuentes informáticos

Incorrecta:
Especialistas de ingeniería social

D Ladrones de identidad — Respuesta correcta

Pregunta 17

0,5 / 0,5

Para determinar el riesgo residual se necesita:

Ocultar opciones de respuesta

Correcta:
Riesgo inherente y efectividad de controles — Respuesta correcta

B El residuo de la división de la probabilidad y el impacto

C Las amenazas y las vulnerabilidades

D El inventario de activos

Pregunta 18

0,5 / 0,5

¿Luego de la evaluación de riesgos, en cuales debería enfocarme?

Ocultar opciones de respuesta

A En aquellos con Mayor impacto

B En aquellos con mayor probabilidad

Correcta:
En aquellos con Mayor Impacto y Mayor Probabilidad a la vez — Respuesta correcta

D En todos, pues eso es lo que indica la norma

Pregunta 19

0,5 / 0,5

¿Cuál es el objetivo principal de un programa de gestión de riesgos?

Ocultar opciones de respuesta

Correcta:
Mantener el riesgo residual en un nivel aceptable

Respuesta correcta

B Instaurar controles para todos los riesgos declarados

C Eliminar todo riesgo inherente

D Reducir el riesgo residual a cero

Pregunta 20

0,5 / 0,5

Quién es más importante que apruebe el Plan de Tratamiento de los riesgos identificados en el Sistema que soporta el proceso Contable

Ocultar opciones de respuesta

A Jefe de Seguridad de la Información

Correcta:
Gerente de Contabilidad

Respuesta correcta

C Gerente de Sistemas

D Gerente de Auditoría Interna

Pregunta 21

0,5 / 0,5

Frente a un riesgo de fraude electrónico para transacciones menores a 60 soles, la empresa VISAXX decide no implementar mecanismos para reducir su probabilidad o impacto. ¿Qué decisión está tomando en su respuesta al riesgo?

Ocultar opciones de respuesta

A Transferir el riesgo

B Evitar el riesgo

C Mitigar el riesgo

Correcta:
Aceptar el Riesgo

Respuesta correcta

Pregunta 22

0,5 / 0,5

¿En qué cláusula se establece el presupuesto del SGSI?

Ocultar opciones de respuesta

Correcta:
Cláusula 7: Soporte

Respuesta correcta

B Cláusula 4: Contexto de la Organización

C Cláusula 5: Liderazgo

D Cláusula 6: Planificación

Pregunta 23

0 / 0,5

¿Qué acción se debe realizar primero para implementar Seguridad de la Información como un proceso de negocio?

Ocultar opciones de respuesta

Incorrecta:
Implementar las políticas y procedimientos de seguridad definidos

B Realizar un assessment, consultoría, implementación y mejora de un ISMS

C Obtener el presupuesto necesario

D Reunirse con todas las funciones claves del negocio

Respuesta correcta

Pregunta 24

0,5 / 0,5

La información a protegerse en un SGSI, abarca:

Ocultar opciones de respuesta

A Información Impresa

B Información almacenada y procesado en Sistemas Informáticos

C Información trasmitida de forma verbal

Correcta:
Todas las anteriores

Respuesta correcta

Pregunta 25

0,5 / 0,5

¿Qué apartado de la norma ISO 27001 están integrado por los controles?

Ocultar opciones de respuesta

A 4, 5, 6, 7 y 8

Correcta:
Sólo Anexo A

Respuesta correcta

C ISO 27005

D Sólo Anexo B

Pregunta 26

0,5 / 0,5

¿En qué cláusula se realiza la Concienciación de los grupos de interés del SGSI?

Ocultar opciones de respuesta

Correcta:
Cláusula 7: Soporte

Respuesta correcta

B Cláusula 4: Contexto de la Organización

C Cláusula 9: Evaluación de desempeño

D Cláusula 6: Planificación

Pregunta 28

0,5 / 0,5

Cuando una organización establece una relación con un proveedor de servicio de TI externo, ¿cuál de las opciones siguientes es uno de los temas MÁS importantes que se deben incluir en el contrato desde el punto de vista de la seguridad?

Ocultar opciones de respuesta

A Cumplimiento de los estándares de seguridad internacionales

B Uso de un sistema de autenticación de dos factores

C Existencia de un sitio de respaldo alterno completamente equipado (hot site) en caso de interrupción de las operaciones del negocio

Correcta:
Cumplimiento de los requerimientos de seguridad informática de la organización

Respuesta correcta

Pregunta 27

0,5 / 0,5

En el marco de un SGSI: NO es necesario monitorear la seguridad de la información de la Organización, procesada en un servicio de NUBE de un proveedor reconocido, pues es entera responsabilidad de dicho proveedor.

V **Verdadero**

F **Falso**

Respuesta correcta

Pregunta 29

0,5 / 0,5

CASO: Determine si en el siguiente caso se cumple o no se cumple lo requerido por la norma ISO27001:La organización establece intercambio de información con el organismo supervisor, esta información es enviada por medio electrónico, la organización definió una excelente política de intercambio de información y por lo tanto no fue necesario definir el procedimiento de intercambio de información:

Ocultar opciones de respuesta

Correcta:
No cumple

Respuesta correcta

B Cumple

Pregunta 30

0,5 / 0,5

¿En qué cláusula se determina el alcance del SGSI?

Ocultar opciones de respuesta

A Cláusula 7: Soporte

Correcta:
Cláusula 4: Contexto de la Organización
Respuesta correcta

C Cláusula 5: Liderazgo

D Cláusula 6: Planificación

Pregunta 33

0,5 / 0,5

Descripción de lo que se quiere lograr como resultado de la aplicación de los controles

Ocultar opciones de respuesta

Correcta:
Objetivo de Control
Respuesta correcta

B Control Remanente

C Objetivo de Riesgo

D Control

Pregunta 34

0,5 / 0,5

Te proponen realizar una inversión riesgosa pero con potenciales altas ganancias. Si decides no invertir, estarías aplicando la opción de:

Ocultar opciones de respuesta

A Mitigar

B Aceptar

Correcta:
Evitar
Respuesta correcta

D Transferir

Pregunta 31

0,5 / 0,5

Salvaguardar la exactitud y totalidad de la información, así como los métodos de procesamiento y transmisión, es:

Ocultar opciones de respuesta

A Confidencialidad

B Disponibilidad

C No repudio

Correcta:
Integridad
Respuesta correcta

Pregunta 32

0,5 / 0,5

No es obligatorio cubrir todos los controles de la norma en una implementación del ISO 27001

V Verdadero
Respuesta correcta

F Falso

Pregunta 35

0,5 / 0,5

Causa potencial de un incidente no deseado, que puede resultar en daño a la organización

Ocultar opciones de respuesta

A Probabilidad

B Riesgo

C Covid-19

Correcta:
Amenaza

Respuesta correcta

Pregunta 36

0,5 / 0,5

En relación al control de Clasificación de la Información,

Ocultar opciones de respuesta

A La clasificación debe considerar los requisitos legales

B Se debe revisar la clasificación en el tiempo

C La organización debe obligatoriamente emplear los mismos niveles de clasificación que las otras empresas del mismo sector

D Todas las opciones anteriores son correctas

Correcta:
Solamente las opciones "A" y "B" son correctas

Respuesta correcta

Pregunta 37

0,5 / 0,5

Exposición de información privada de los clientes, es un impacto que afecta a la:

Ocultar opciones de respuesta

Correcta:
Confidencialidad

Respuesta correcta

B Disponibilidad

C Amenaza

D Integridad

Pregunta 38

0,5 / 0,5

La política de Seguridad de la Información, debe considerar:

Ocultar opciones de respuesta

A La inclusión de los objetivos de seguridad

B El compromiso de cumplir con requisitos aplicables

C El Compromiso de mejora continua

Correcta:
Todas las anteriores

Respuesta correcta

E Sólo B y C

Pregunta 39

0,5 / 0,5

Si se detectan incumplimientos a las Políticas y Normas de la Organización, la gerencia debería:

Ocultar opciones de respuesta

A identificar las causas del incumplimiento

B implementar las acciones correctivas apropiadas

C revisar la acción correctiva tomada, para comprobar su eficacia e identificar las deficiencias y debilidades

Correcta:
Todas las opciones anteriores son correctas

Respuesta correcta

E Solamente las opciones "A" y "B" son correctas

Pregunta 40

0,5 / 0,5

Elija el orden correcto de las cláusulas de la norma.

Ocultar opciones de respuesta

A Liderazgo, Contexto, Planificación, Soporte, Operación, Evaluación Desempeño

B Liderazgo, Planificación, Soporte, Operación, Evaluación Desempeño, Contexto

Correcta:
Contexto, Liderazgo, Planificación, Soporte, Operación, Evaluación Desempeño

Respuesta correcta

D Ninguna de las anteriores