Gestión de Seguridad de Información
Exam.Final 2023_02

1. Pregunta 1

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

Cuando un riesgo no puede mitigarse de manera suficiente mediante controles manuales o automáticos, ¿cuál de las siguientes opciones es la MEJOR para proteger la organización del posible impacto financiero del riesgo?

Ocultar opciones de respuesta

1. **Correcta:**
   Obtener un seguro contra el riesgo.

   Respuesta correcta
2. Actualizar registro de riesgo de TI.
3. Mejorar la capacitación del personal en el área de riesgo.
4. Tercerizar el proceso de negocios correspondiente.

2. Pregunta 2

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

¿Qué es ISO 27001?

Ocultar opciones de respuesta

1. Es un estándar internacional que provee un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SMS.
2. **Correcta:**
   Es un estándar internacional que provee un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un ISMS.

   Respuesta correcta
3. Es un conjunto de mejores prácticas de la industria de TI para Seguridad de la Información.
4. Es un marco de referencia teórico para asegurar el apego normativo de Seguridad de la Información.

3. Pregunta 3

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

¿Cuál de los siguientes factores debería tenerse en cuenta al momento de diseñar controles para mitigar riesgos?

Ocultar opciones de respuesta

1. Costo
2. Eficacia / Eficiencia
3. Factibilidad
4. **Correcta:**

   Todas las anteriores

   Respuesta correcta

4. Pregunta 4

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

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

Ocultar opciones de respuesta

1. 7
2. 8
3. 9
4. **Correcta:**

   10

   Respuesta correcta

5. Pregunta 5

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

Motivos para implantar un SGSI: Los motivos pueden ser: requisito legal, ventaja estratégica, requerimiento de clientes

1. **V**

   VerdaderoRespuesta correcta

2. **F**

   Falso

6. Pregunta 6

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

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

Ocultar opciones de respuesta

1. identificar las causas del incumplimiento
2. implementar las acciones correctivas apropiadas
3. revisar la acción correctiva tomada, para comprobar su eficacia e identificar las deficiencias y debilidades
4. **Correcta:** Todas las opciones anteriores son correctas

Respuesta correcta

5. Solamente las opciones "A" y "B" son correctas

7. Pregunta 7

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

¿Cuántos controles provee ISO 27002:2022?

Ocultar opciones de respuesta

1. 114
2. 17
3. 87
4. **Correcta:** 93

Respuesta correcta

8. Pregunta 8

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

Para determinar el riesgo residual se necesita:

Ocultar opciones de respuesta

1. **Correcta:**
   Riesgo inherente y efectividad de controles

   Respuesta correcta
2. El residuo de la división de la probabilidad y el impacto
3. Las amenazas y las vulnerabilidades
4. El inventario de activos

9. Pregunta 9

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

En la organización donde usted labora, se detectó que robaron equipos y medios de almacenamiento del centro de cómputo.
Al realizar la investigación se determinó que no se contaba con vigilantes, cámaras de seguridad, ni detectores de movimiento; por lo que no se pudo detectar oportunamente el evento; ni tampoco obtener la evidencia para identificar al autor de lo sucedido.
¿Qué control (o controles) de la norma ISO 27001:2022 fue (o fueron) incumplidos? Marque la alternativa correcta.

Ocultar opciones de respuesta

1. 7.4 Monitoreo de la Seguridad Física
2. 7.2 Entrada física
3. 7.11 Servicios de apoyo
4. **Correcta:** Las opciones "a" y "b" son correctas

Respuesta correcta

10. Pregunta 10

0/0,5

Calificado, 0 puntos de 0,5 puntos posibles

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

Ocultar opciones de respuesta

1. **Incorrecta:**
   Transferir el riesgo
2. Mitigar el riesgo

   Respuesta correcta
3. Evitar el Riesgo
4. Tercerizar el Riesgo

11. Pregunta 11

0/0,5

Calificado, 0 puntos de 0,5 puntos posibles

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

Ocultar opciones de respuesta

1. la realización de análisis forenses
2. análisis BIA
3. escalamiento, según corresponda
4. **Incorrecta:** Todas las opciones anteriores son correctas
5. Solamente las opciones "A" y "C" son correctas

Respuesta correcta

12. Pregunta 12

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

Elija el orden correcto de las cláusulas de la norma.

Ocultar opciones de respuesta

1. Liderazgo, Contexto, Planificación, Soporte, Operación, Evaluación Desempeño
2. Liderazgo, Planificación, Soporte, Operación, Evaluación Desempeño, Contexto
3. **Correcta:**
   Contexto, Liderazgo, Planificación, Soporte, Operación, Evaluación Desempeño

   Respuesta correcta
4. Ninguna de las anteriores

13. Pregunta 13

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

¿Quién es el responsable de la Seguridad de la Información en una organización?

Ocultar opciones de respuesta

1. **Correcta:**
   Toda la organización

   Respuesta correcta
2. CEO
3. Gerente de TI
4. Gerente de Seguridad de la Información

14. Pregunta 14

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

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

Ocultar opciones de respuesta

1. En aquellos con Mayor impacto
2. En aquellos con mayor probabilidad
3. **Correcta:**
   En aquellos con Mayor Impacto y Mayor Probabilidad a la vez

   Respuesta correcta
4. En todos, pues eso es lo que indica la norma

15. Pregunta 15

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

¿Qué es el Análisis de Riesgos de Seguridad de la Información?

Ocultar opciones de respuesta

1. Es el proceso para poder eliminar los riesgos de un activo de información.
2. **Correcta:**
   Es el proceso para determinar la probabilidad de que un activo de información sea comprometido causando un impacto en la organización.

   Respuesta correcta
3. Es el proceso para determinar los controles requeridos para evitar comprometer un activo de información.
4. Establece el riesgo que se tiene en una organización en temas de seguridad ambiental.

16. Pregunta 16

0/0,5

Calificado, 0 puntos de 0,5 puntos posibles

En la etapa de Evaluación del Riesgo:

Ocultar opciones de respuesta

1. Se compara el nivel de riesgo con los criterios de aceptación de los riesgos

   Respuesta correcta
2. Se calcula el riesgo inherente
3. **Incorrecta:**
   Se calcula el impacto y la probabilidad
4. Se calcula el riesgo residual

17. Pregunta 17

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

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

Ocultar opciones de respuesta

1. **Correcta:**
   Cláusula 7: Soporte

   Respuesta correcta
2. Cláusula 4: Contexto de la Organización
3. Cláusula 9: Evaluación de desempeño
4. Cláusula 6: Planificación

18. Pregunta 18

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

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

Ocultar opciones de respuesta

1. ISO/IEC 20000:2011
2. **Correcta:** ISO/IEC 27001:2022

   Respuesta correcta
3. ISO/IEC 27001:2013
4. ISO/IEC 37000:2023

19. Pregunta 19

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

Dentro del alcance de un SGSI, NO podría incluir a terceros, tales como proveedores

1. **V**

   Verdadero
2. **F**

   FalsoRespuesta correcta

20. Pregunta 20

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

¿Cuál era el código del estándar británico para Seguridad de la Información?

Ocultar opciones de respuesta

1. BS1500
2. BS2599
3. BS3870
4. **Correcta:**
   BS7799

   Respuesta correcta

21. Pregunta 21

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

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

1. **V**

   VerdaderoRespuesta correcta

2. **F**

   Falso

22. Pregunta 22

0/0,5

Calificado, 0 puntos de 0,5 puntos posibles

¿Cuáles son las fases del ciclo PDCA?

Ocultar opciones de respuesta

1. **Incorrecta:**
   Plantear, Hacer, Verificar, Actuar
2. Planear, Hacer, Verificar, Asegurar
3. Planear, Hacer, Verificar, Actuar

   Respuesta correcta

4. Planear, Validar, Verificar, Actuar

23. Pregunta 23

0/0,5

Calificado, 0 puntos de 0,5 puntos posibles

La ventaja MÁS importante de utilizar análisis cualitativo en lugar de análisis cuantitativo de riesgo es:

Ocultar opciones de respuesta

1. Mayor costo.
2. Menor objetividad.
3. **Incorrecta:**
   Mayor dependencia de personal calificado.
4. Rapidez para el proceso de análisis.

Respuesta correcta

24. Pregunta 24

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

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

1. Transferir el riesgo
2. Evitar el riesgo
3. Mitigar el riesgo
4. **Correcta:**
   Aceptar el Riesgo

Respuesta correcta

25. Pregunta 25

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

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

1. usen ejemplos ilustrativos de ataques exitosos.
2. expliquen el riesgo técnico para la organización.
3. evalúen la organización comparándola contra buenas prácticas de seguridad.

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

Respuesta correcta

26. Pregunta 26

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

En criptografía de llave pública, es correcto afirmar que

Ocultar opciones de respuesta

1. Si tengo la llave pública de una persona, entonces puedo deducir cuál es su llave privada
2. Si tengo la llave privada de una persona, entonces puedo deducir cuál es su llave pública
3. Si cifro un mensaje con la llave privada del emisor, solamente se podrá descifrar con la misma llave privada del emisor
4. **Correcta:** Si cifro un mensaje con la llave privada del emisor, solamente se podrá descifrar con la llave pública del emisor.

Respuesta correcta

27. Pregunta 27

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

¿Para que se puede emplear el DIGEST (cadena de caracteres obtenida al aplicar una función HASH)?

Ocultar opciones de respuesta

1. **Correcta:** Para validar la integridad del mensaje

Respuesta correcta

2. Para realizar un ataque por fuerza bruta
3. Para validar la mensaje de un receptor
4. Para cifrar un mensaje

28. Pregunta 28

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

Los métodos de cifrado que emplean solamente sustitución:

Ocultar opciones de respuesta

1. Son más seguros que los que emplean solamente transposición
2. Son menos seguros que los que emplean solamente transposición
3. Requieren mucha capacidad computacional
4. **Correcta:** Quedan expuestos al análisis de frecuencia de aparición de las letras en los distintos idiomas efectuado por los criptoanalistas

Respuesta correcta

29. Pregunta 29

0/0,5

Calificado, 0 puntos de 0,5 puntos posibles

No es un ejemplo de Fuerte Autenticación

Ocultar opciones de respuesta

1. Uso de contraseña + huella digital
2. Uso de huella digital + face ID

Respuesta correcta

3. **Incorrecta:** Uso de tarjeta de crédito + PIN de seguridad
4. Scan de retina + clave dinámica recibida por mensaje de texto

30. Pregunta 30

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

En criptografía de llave pública, si quiero preservar la confidencialidad, debería cifrar con:

Ocultar opciones de respuesta

1. La llave privada del emisor
2. La llave pública del emisor
3. **Correcta:** La llave pública del receptor

Respuesta correcta

4. La llave privada del receptor

31. Pregunta 31

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

En relación a las actualizaciones (parches) del sistema operativo emitidas por el fabricante, es **incorrecto** afirmar lo siguiente:

Ocultar opciones de respuesta

1. Es necesario probarlos antes de aplicarlos en los sistemas en producción
2. Se debe tener un plan de fallback / rollback (retroceso) en caso de fallas
3. La aplicación de los mismos puede contribuir a reducir o eliminar vulnerabilidades del sistema operativo
4. **Correcta:** No requieren ser probados, pues fueron elaborados por los propios fabricantes del sistema operativo

Respuesta correcta

32. Pregunta 32

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

La escítala lacedemonia emplea el método de:

Ocultar opciones de respuesta

1. Sustitución
2. **Correcta:** Transposición

Respuesta correcta

3. Combinación
4. Hash

33. Pregunta 33

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

En criptografía, cuál sería uno de los motivos para combinar los métodos de transposición y sustitución:

Ocultar opciones de respuesta

1. Para facilitar los procesos de cifrado y descifrado
2. Para compensar el desbalance computacional de ambos métodos
3. **Correcta:** Para fortalecer el algoritmo de cifrado

Respuesta correcta

4. Para transmitir de forma más segura la llave pública

34. Pregunta 34

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

El disco de Alberti emplea el método de:

Ocultar opciones de respuesta

1. **Correcta:** Sustitución

   Respuesta correcta

2. Transposición
3. KRI
4. Llave Pública

35. Pregunta 35

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

¿Por qué emplearía criptografía de llave pública para transferir la llave secreta de criptografía simétrica?

Ocultar opciones de respuesta

1. No tiene sentido, si ya tengo criptografía de llave pública debería cifrar con ella simplemente
2. **Correcta:** Porque la criptografía simétrica consume muchos menos recursos que la asimétrica, entonces esto sería útil para transmitir volúmenes importantes de datos

   Respuesta correcta

3. Porque así se puede transmitir la llave privada del emisor
4. Para verificar la vigencia del certificado digital

36. Pregunta 36

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

Una firma digital es:

Ocultar opciones de respuesta

1. La firma de una persona escaneada
2. La llave pública del emisor del mensaje
3. Un certificado digital del emisor del mensaje

4. **Correcta:** El resultado de cifrar con la llave privada del emisor al Digest (cadena de caracteres obtenida al aplicar una función HASH) del documento o mensaje.

Respuesta correcta

37. Pregunta 37

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

Marque la alternativa **incorrecta** considerando lo requerido por la ISO 27001

Ocultar opciones de respuesta

1. Las funcionalidades de seguridad establecidas en el requerimiento, deben ser probadas durante las diferentes fases del desarrollo
2. Los entornos de pruebas y producción debe mantenerse separados
3. **Correcta:** Si el desarrollo es externalizado (tercerizado) no es necesario supervisar ni monitorear esta actividad porque la responsabilidad es del tercero.

Respuesta correcta

4. No deben copiarse los datos sensibles del entorno de producción al entorno de pruebas

38. Pregunta 38

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

¿Qué se puede validar con una firma digital?

Ocultar opciones de respuesta

1. La identidad del emisor
2. La integridad del mensaje
3. **Correcta:** Opciones "a" y "b" son correctas

Respuesta correcta

4. Ninguna de las anteriores

39. Pregunta 39

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

Cuál NO es una buena práctica en relación al respaldo de la información

Ocultar opciones de respuesta

1. Realizar pruebas periódicas de restauración de las copias de respaldo
2. **Correcta:** Para facilitar el copiado y restauración, realizar las copias en un servidor en el mismo dominio y dentro del mismo centro de cómputo que el servidor de producción

Respuesta correcta

3. Almacenar las copias de respaldo en un lugar distinto a donde se encuentra ubicado el servidor de producción
4. Revisar el sistema de generación de copias a fin de determinar si la tarea culminó correctamente y sin errores

40. Pregunta 40

0,5/0,5

Calificado, 0,5 puntos de 0,5 puntos posibles

En los algoritmos de cifrado simétricos, la llave de cifrado y descifrado es distinta

1. **V**

Verdadero

2. **F**

Falso