Challenge - U.1 | S.20

Esta evaluación contiene preguntas que pueden recibir crédito parcial o negativo.

Descartar

3 DE 30 PREGUNTAS RESTANTES

Contenido del cuestionario

Pregunta 1

1 punto

¿Qué es un SGSI?

- **A** Un sistema de almacenamiento de información
- **B** Un conjunto de políticas para gestionar información confidencial
- **C** Un programa de software para la gestión de proyectos
- **D** Un protocolo de comunicación para redes.

Pregunta 2

1 punto

¿Cuál es el objetivo principal de un SGSI?

- **A** Aumentar las ventas de una organización.
- **B** Gestionar las operaciones financieras.
- **C** Proteger la información de la organización.
- **D** Optimizar los recursos humanos.

Pregunta 3

1 punto

¿Qué metodologías son comunes en la gestión de seguridad?

- **A** ISO 9000, COBIT y ITIL
- **B** COBIT, CMMI y Six Sigma

C SCRUM, PMI y PRINCE2.

D ISO 27000, NIST, ENISA y SANS

Pregunta 4

1 punto

¿Qué define ISO 27001?

A Los requisitos para implementar un Sistema de Información (SI).

B Un estándar nacional para gestionar los proyectos de tecnología en los entes Publicos.

C Los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

D Un estándar que incluye a la seguridad de las redes y de la seguridad física en la organización.

Pregunta 5

1 punto

¿Qué es la vigilancia de ciberamenazas?

A La supervisión del software de protección antivirus.

B La supervisión del sistema de encriptación de datos

C La contratación de equipos externos de seguridad.

D La supervisión constante para identificar posibles ciberamenazas

Pregunta 6

1 punto

¿Cuál es el propósito del Equipo Púrpura en ciberseguridad?

A Coordinar las actividades administrativas.

B Educar al personal sobre seguridad

C Combinar las funciones ofensivas y defensivas

D Supervisar los sistemas de finanzas

Pregunta 7

1 punto

¿Qué es el cumplimiento normativo?

A Estar en conformidad con leyes y regulaciones aplicables.

B La implementación de un sistema de gestión de información.

C La adopción de estándares de seguridad para sistemas internos.

D La creación de sistemas de respaldo de información.

Pregunta 8

1 punto

¿Qué es una amenaza en seguridad de la información?

A Una acción que fortalece el sistema.

B Una acción que explota una vulnerabilidad para atacar un sistema.

C Un software que protege el sistema.

D Un protocolo para mejorar la seguridad en la red.

Pregunta 9

1 punto

¿Qué es la continuidad de negocio (SGCN)?

A La planificación para mantener las operaciones normales de la organización

B La planificación para mantener las operaciones durante y después de una interrupción.

C La capacidad de una organización para realizar transacciones en línea

D La capacidad de una organización para realizar transacciones con proveedores

Pregunta 10

1 punto

¿Qué diferencia hay entre un Sistema de Información y un Sistema de Gestión?

A El Sistema de Información maneja herramientas tecnológicas y el Sistema de Gestión políticas y procedimientos.

B El Sistema de Gestión se usa solo para servicios externos y el Sistema de Información gestiona los servicios internos.

C Uno gestiona a las personas y el otro gestiona los datos finanzas

D Ambos son lo mismo.

Pregunta 11

1 punto

¿Qué es la gestión del riesgo?

A La creación de nuevas políticas de seguridad.

B La implementación de medidas físicas en la empresa.

C La identificación, evaluación y mitigación de riesgos.

D El desarrollo de software de protección.

Pregunta 12

1 punto

¿Qué es un activo dentro de la seguridad de la información?

A Un sistema informático

B Un documento sin valor.

C Un conjunto de datos sin importancia

D Cualquier elemento que tiene valor para la organización

Pregunta 13

1 punto

¿Qué es Data Leak/Loss Prevention (DLP)?

A Un método para controlar el acceso físico a la información.

B Un sistema para prevenir la pérdida o filtración de datos confidenciales.

C La instalación de software de gestión.

D Un protocolo para gestionar copias de seguridad.

Pregunta 14

1 punto

¿Qué implica el cumplimiento normativo en ciberseguridad?

A Cumplir con las leyes y regulaciones aplicables a la seguridad de la información

B Adaptar los sistemas a las tecnologías emergentes

C Desarrollar nuevos controles de acceso a la información.

D Cumplir con las políticas internas aplicables a la seguridad de la información

---

Pregunta 15

1 punto

¿Qué significa integridad en el contexto de la seguridad de la información?

A Que la información puede modificarse sin problemas.

B Que los archivos sean accesibles desde cualquier lugar.

C Que los usuarios no puedan borrar datos.

D Que los datos sean precisos y completos.

Pregunta 16

1 punto

¿Cómo se define el riesgo en ciberseguridad?

A La probabilidad de que un sistema funcione sin fallos.

B La capacidad de un sistema para resistir ataques.

C La posibilidad de que una amenaza explote una vulnerabilidad.

D La velocidad con la que se responde a un incidente.

Pregunta 17

1 punto

Selecciona todas las que son vulnerabilidades

A Phishing

B Errores de configuración.

C Espionaje, sabotaje y vandalismo

D Carencias de procedimiento y controles.

Pregunta 18

1 punto

Las Políticas de seguridad, formación y concienciación del personal, controles de acceso, y uso de software antivirus, son ejemplso de controles

A Detección

B Represión

C Preventivos

D Correctivos

Pregunta 19

1 punto

¿Cuál de estos es un ejemplo de amenaza?

A Fraude asistido por computadora.

B Respaldo de datos.

C Control de acceso físico.

D Uso de contraseñas fuertes.

Pregunta 20

1 punto

El analisis forence es un buen ejemplo de que tipo de control

A Correctivo

B Evaluación

C Preventivos

D Represión

Pregunta 21

1 punto

¿Qué significa GRC en ciberseguridad?

A Gestión de Recursos Corporativos.

B Gobierno, Riesgo y Cumplimiento.

C Grupo de Respuesta a Ciberataques.

D Gestión de Riesgos Cibernéticos.

Pregunta 22

1 punto

Algunos ejemplos de KPI para ciberseguridad son:

A Número de Incidentes de Ciberseguridad

B Cantidad de equipos que no están en el inventario

C Histórico del parcheo de la plataforma

D Listado de los visitantes de la organización

Pregunta 23

1 punto

¿Qué es ISO 27000?

A Un estándar para la gestión de proyectos.

B Un conjunto de estándares Nacionales para la seguridad de la información.

C Un conjunto de estándares internacionales para la seguridad de la información.

D Un conjunto de estándares obligatorios para la seguridad de la información.

Pregunta 24

1 punto

Selecciona todas los que son ejemplos de Riesgos

A Phishing

B Errores de configuración.0

C Ramsonware

D Carencias de procedimiento y controles.

Pregunta 25

1 punto

¿Qué es la fase "Hacer" del ciclo PDCA en ciberseguridad?

A Implementar y ejecutar los controles y procesos definidos

B Establecer los objetivos de seguridad de la información

C Monitorear y medir los resultados de los controles

D Revisar y mejorar los procesos de seguridad

Pregunta 26

1 punto

Cual es la Guia del CCN que me indica las evidencias para un proceso de auditoria del ENS, por ejemplo: Logs de acceso, reportes de incidentes de seguridad, certificaciones de auditorías internas, entre otros

A 804

B 808

C 815

D 801

Pregunta 27

1 punto

En la declaracion de aplicabilidad que controles deben aparecer

A Medidas/Controles Seleccionados

B Medidas/Controles Descartados

C Medidas Compensatorias

D Todos

Pregunta 28

1 punto

El ENS tiene las siguientes medidas de seguridad que se deben implementar en un conjunto de controles o medidas que incrementara la ciberseguridad. Selecicone los que crea que son:

A Marco organizativo (ORG), Marco operacional (OP) y Medidas de Protección (MP)

B Marco organizativo (ORG), Operación protegida (OP) y Marco periodico (MP)

C Marco organizativo (ORG), Marco operacional (OP) y Marco periodico (MP)

D Marco orgabnico (ORG), Marco operacional (OP) y Medidas de Protección (MP)

Pregunta 29

1 punto

Cuales son las 2 dimensiones adicionales del ENS a la triada tradicional de ciberseguridad.

A Confidencialidad (C)

B Trazabilidad (T)

C Disponibilidad (D)

D Autenticidad (A)

Pregunta 30

1 punto

Seleccióna 2 fases que estan dentro del modelo CCM de Capacidad y Madurez

A Repetible

B Gestionado y Evaluable

C Repetible pero intuitivo

Guardado por última vez 20:11:57

Filtro de preguntas (30)

Guardar y cerrar

Enviar