Platzi

Curso de Estrategia de Seguridad Informática para Empresas

¡Felicidades!

Aprobaste el curso. Ya puedes acceder a tu **diploma digital**.

10	20 / 20
Calificación	Aciertos

1. ¿Cuál de las siguientes afirmaciones describe mejor el propósito de alinear el Programa de Seguridad de la Información con los objetivos de la organización?

- Para asegurar que el programa apoye los objetivos estratégicos de la organización, aborde los riesgos específicos y aplique controles de seguridad que protejan los activos de información sin obstaculizar las operaciones ✓

2. En el contexto de la seguridad de la información, la eficacia de un Programa de Seguridad depende de varios componentes integrales. ¿Cuál de las siguientes combinaciones incluye aspectos esenciales que deben ser cubiertos por dicho programa?

- Respuesta a incidentes, Recuperación ante desastres y continuidad del negocio, Cumplimiento normativo, Gestión de vulnerabilidades ✓

3. Una vez establecida una Política General de Seguridad de la Información, es importante desarrollar políticas específicas que aborden áreas críticas de la seguridad. ¿Cuál de las siguientes políticas considera que debería ser la primera en desarrollarse a continuación?

- Política de Uso Aceptable: Define las reglas de comportamiento para los usuarios de los sistemas de información, asegurando el uso adecuado de los recursos de TI ✓

4. ¿Cuál de las siguientes acciones es más efectiva para asegurar la integridad de los datos en nuestra organización?

- Implementar controles de acceso para restringir quién puede modificar la información ✓

5. La gestión de incidentes es un componente crítico en la seguridad de la información. ¿En qué consiste este proceso?

Identificación, análisis y respuesta a incidentes de seguridad de la información para minimizar el impacto negativo en la organización y restaurar los servicios normales ✓

6. Según el marco de gestión del riesgo del NIST 800-39, ¿cuáles son las etapas clave que las organizaciones deben seguir para gestionar el riesgo de manera efectiva?

Establecer un contexto sobre el riesgo (Framing Risk), evaluar el riesgo (Assessing Risk), responder al riesgo (Responding to Risk), y monitorear el riesgo (Monitoring Risk) ✓

7. En el contexto de la gestión de riesgos en seguridad de la información, ¿cuál es la principal diferencia entre una evaluación de riesgos cualitativa y una cuantitativa?

La evaluación cuantitativa mide el riesgo en términos financieros específicos, mientras que la cualitativa utiliza categorías como 'alto', 'medio' y 'bajo' para describir el nivel de riesgo ✓

8. ¿En qué consiste la Declaración de Aplicabilidad o Statement of Applicability (SoA) en el marco de la gestión de la seguridad de la información?

Un documento que enumera todos los controles de seguridad considerados dentro de un estándar específico, como ISO 27001 o el NIST 800-53, e indica cuáles son aplicables y justifica aquellos que no se implementan ✓

9. ¿Cuál es el principal objetivo de incorporar la continuidad del negocio en un programa de seguridad de la información?

Garantizar que la organización pueda continuar operando sus funciones críticas en el caso de un evento disruptivo, mediante la identificación de recursos mínimos necesarios como personal, recursos computacionales y backups ✓

10. El Objetivo de Tiempo de Recuperación (RTO) se refiere al tiempo máximo aceptable que podría transcurrir desde la ocurrencia de un desastre hasta la reanudación de las operaciones comerciales y los procesos críticos.

Verdadero ✓

11. ¿Cuál es el propósito principal de un Acuerdo de Nivel de Servicio (SLA) entre un proveedor de servicios y su cliente?

Detallar los servicios específicos a ser proporcionados, los estándares de calidad esperados, y las métricas para medir el servicio, estableciendo expectativas claras y un marco para la rendición de cuentas ✓

12. ¿Qué caracteriza al Ciclo de Vida de Desarrollo de Software Seguro (SSDLC)?

Una metodología que integra prácticas de seguridad en cada fase del desarrollo de software, desde la planificación hasta el mantenimiento, para minimizar vulnerabilidades ✓

13. La incorporación de prácticas de seguridad en cada fase del SSDLC aumenta significativamente los costos de desarrollo en comparación con los métodos tradicionales de desarrollo de software

Falso ✓

14. Implementar un enfoque SSDLC garantiza que el software esté completamente libre de vulnerabilidades de seguridad una vez lanzado

Falso ✓

15. ¿Cómo puede ayudarte OWASP en el campo de la seguridad de la información?

Proporcionando recursos y guías para mejorar la seguridad del software. ✓

16. ¿Cómo puede una empresa conocer los riesgos principales a los que está expuesta una aplicación?

Realizando pruebas regulares para identificar vulnerabilidades y consultando el OWASP Top 10. ✓

17. El proyecto OWASP Top 10 se refiere sólo a riesgos en Aplicaciones Web

Falso ✓

18. ¿Cómo puede un equipo de seguridad aprovechar el modelo de madurez para mejorar sus prácticas?

Identificando áreas de mejora en sus prácticas actuales y estableciendo metas específicas para alcanzar niveles más altos de madurez. ✓

19. ¿Por qué es necesario que todos los empleados estén capacitados en seguridad de la información?

Porque las personas son el eslabón más débil en la cadena de seguridad y su desconocimiento puede conducir a brechas de seguridad. ✓

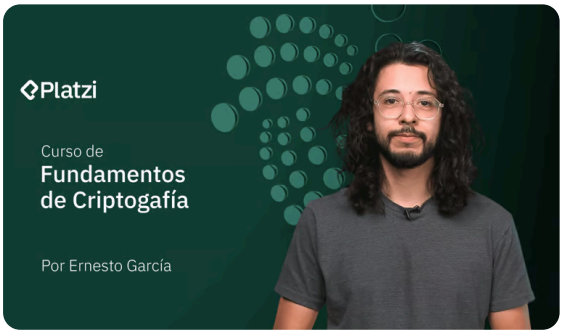
20. En el contexto de un programa de seguridad de la información efectivo, ¿cuál es la responsabilidad principal de cada uno de los siguientes roles?

Líder del Programa de Seguridad: Asegurar una estrategia clara; Analista/Ingeniero de Seguridad de la Información: Implementación técnica adecuada; Responsable de Políticas y Cumplimiento: Cumplimiento de políticas y regulaciones ✓

Ver menos

Cursos que podrían interesarte

Curso Gratis de Ciberseguridad: Simulador Práctico en WhatsApp
Por Juan José Torres



Curso de Fundamentos de Criptografía
Por Ernesto García

Curos de
Por Alex To

Ir a Inicio

Siguiente curso →