¡Felicitaciones! ¡Aprobaste!

Calificación recibida 100 % **Para Aprobar** 75 % o más

Ir al siguiente elemento

1. ¿Qué tipos de riesgos abordan los planes de seguridad? Selecciona tres respuestas. **1 / 1 punto**

- [ ] Cambio de condiciones empresariales
- [x] Pérdida de información

Correcto
Los planes de seguridad abordan riesgos como daños a los activos, pérdida de información y divulgación de datos.

- [x] Los daños a los activos

Correcto
Los planes de seguridad abordan riesgos como daños a los activos, pérdida de información y divulgación de datos.

- [x] Divulgación de datos

Correcto
Los planes de seguridad abordan riesgos como daños a los activos, pérdida de información y divulgación de datos.

2. ¿Cuáles son los elementos básicos de un plan de seguridad? Selecciona tres respuestas. **1 / 1 punto**

- [x] Los estándares

Correcto
Los elementos básicos de un plan de seguridad son las políticas, los estándares y los procedimientos. Las políticas son reglas que reducen el riesgo y protegen la información. Los estándares son referencias que informan sobre cómo establecer las políticas. Y los procedimientos son instrucciones paso a paso para realizar una tarea de seguridad específica.

- [x] Procedimientos

Correcto
Los elementos básicos de un plan de seguridad son las políticas, los estándares y los procedimientos. Las políticas son reglas que reducen el riesgo y protegen la información. Los estándares son referencias que informan sobre cómo establecer las políticas. Y los procedimientos son instrucciones paso a paso para realizar una tarea de seguridad específica.

- [x] Políticas

Correcto
Los elementos básicos de un plan de seguridad son las políticas, los estándares y los procedimientos. Las políticas son reglas que reducen el riesgo y protegen la información. Los estándares son referencias que informan sobre cómo establecer las políticas. Y los procedimientos son instrucciones paso a paso para realizar una tarea de seguridad específica.

D. Reglamentos

Feedback: Los elementos básicos de un plan de seguridad son las políticas, los estándares y los procedimientos. Las políticas son reglas que reducen el riesgo y protegen la información. Los estándares son referencias que informan sobre cómo establecer las políticas. Y los procedimientos son instrucciones paso a paso para realizar una tarea de seguridad específica. Los reglamentos, en cambio, son reglas establecidas por los gobiernos y otras autoridades que a veces influyen en cómo se diseñan los planes de seguridad.

3. Completa el espacio en blanco: El CSF del NIST es un marco _____ que consiste en estándares, pautas y prácticas recomendadas para gestionar el riesgo de ciberseguridad. **1 / 1 punto**

- (•) voluntario
- ( ) obligatorio
- ( ) limitado
- ( ) rígido

Correcto
El CSF del NIST es un marco voluntario que consiste en estándares, pautas y prácticas recomendadas para gestionar el riesgo de ciberseguridad. Es un marco integral con un diseño flexible que se puede utilizar en cualquier sector.

4. ¿Cuáles son algunas de las ventajas del Marco de Ciberseguridad (CSF) del NIST? Selecciona tres respuestas. 1 / 1 punto

- [x] Se puede utilizar para identificar y evaluar los riesgos.

Correcto
Algunas de las ventajas del CSF son que se puede adaptar a las necesidades de cualquier empresa, ayuda a las organizaciones a cumplir los estándares reglamentarios y se puede utilizar para identificar y evaluar los riesgos.

- [x] Ayuda a las organizaciones a cumplir los estándares reglamentarios.

Correcto
Algunas de las ventajas del CSF son que se puede adaptar a las necesidades de cualquier empresa, ayuda a las organizaciones a cumplir los estándares reglamentarios y se puede utilizar para identificar y evaluar los riesgos.

- [ ] Es necesario para hacer negocios en línea.
- [x] Es adaptable a las necesidades de cualquier empresa.

Correcto
Algunas de las ventajas del CSF son que se puede adaptar a las necesidades de cualquier empresa, ayuda a las organizaciones a cumplir los estándares reglamentarios y se puede utilizar para identificar y evaluar los riesgos.