|  |  |
| --- | --- |
| **DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA** | |
| **Nombre de la Actividad** | **Conceptos de marcos de seguridad en la auditoría técnica en *cloud*** |
| **Objetivo de la actividad** | **Afianzar algunos de los conceptos más importantes de la ciberseguridad en *cloud*** |
| **Tipo de actividad sugerida** | **Selección múltiple.** |
| **Archivo de la actividad**  **(Anexo donde se describe la actividad propuesta)** | **Anexo Actividad didáctica 1** |

**Selección múltiple**

**1. ¿Cuáles son las metodologías de aplicación que tienen mejor observancia en el análisis y evaluación de riesgos?**

a. ISO 27001

b. Magerit, Octave, Coras, Mehari, NistSP-830

c. Definir una política de gestión de la seguridad

d. Seguimiento y control al proveedor de servicios en la nube

**2. ¿Qué objetivos son requeridos para la evaluación de activos?**

a. Una reducción de riesgos aceptable, a la vez que se detectan posibles debilidades

b. Hacer una medición en la toma de decisiones

c. Los riesgos no deben existir de ninguna forma

d. Tener un óptimo proceso de gestión de calidad

**3. Un objetivo directo de la metodología Magerit es**

a. Preparar a la organización para procesos de evaluación

b. Tener certificación o acreditación de un ente auditor

c. Realizar evaluaciones periódicas a los proveedores de servicios en la nube

d. Ofrecer un método sistemático para analizar tales riesgos

**4. ¿Para qué es específica la metodología Coras?**

a. Procesos diferentes al análisis de documentos

b. Instalar el plugin de Java en el navegador

c. Análisis de riesgos

d. Instalar UML

**5. Uno de los pasos de la metodología NIST SP-830 es:**

a. Estimación de riesgo

b. Análisis de alto nivel

c. Análisis de controles

d. Aprobación de objetivos y análisis

**6. ISO/IEC 27002 es el complemento de la norma ISO 27001, se encarga específicamente de:**

a. Certificación de riesgos

b. Establecer dominios, objetivos de control y controles recomendados

c. Definición de los sistemas de gestión de seguridad de la información

d. Apoyo en la elección de controles para los planes de tratamiento de la seguridad

**7. En la seguridad del recurso humano, antes de la contratación, se requiere tener en cuenta:**

a. Responsabilidad de la gestión

b. Claridad de los términos de la contratación

c. Determinación de los puestos de trabajo

d. Tener un manual procedimental a nivel de sanciones

**8. Uno de los controles criptográficos es:**

a El uso de técnicas y estándares

b. La documentación de procedimientos de operación

c. Las copias de seguridad de la información

d. La gestión de claves

**9. En los controles de cumplimiento, uno de los objetivos que se busca es:**

1. Establecer acuerdos de nivel de seguridad ajustados a cada proveedor, que permitan mantener una provisión adecuada y alineada de los servicios con estos acuerdos
2. Garantizar que la seguridad de la información se implemente y gestione de acuerdo con las políticas y los procedimientos establecidos por la organización
3. Disminuir el impacto que podría generar el realizar actividades de auditoría en los sistemas en producción
4. Registrar los eventos provocados por incidentes de seguridad de la información y generar y conservar las evidencias

1. **El Dominio 12, que trata sobre la Gestión de incidentes de seguridad, considera como uno de sus controles:**
   1. Protección de datos y privacidad de la información personal
   2. Verificación del cumplimiento
   3. Protección de los registros de la organización
   4. Respuesta a los incidentes de seguridad