**UNIVERSIDAD NACIONAL SEDE REGIONAL BRUNCA**

**INGENIERIA EN SISTEMAS DE INFORMACION**

**SEGURIDAD INFORMÁTICA-EIF440O**

**PROFESOR: PABLO CHAVES MURILLO**

**EXAMEN I**

Nombre: Breiner Muñoz Fallas\_\_\_\_\_\_\_\_\_\_\_ Fecha: 10 /10 /2024

Total de puntos: 20 Puntos obtenidos: Nota:

Tiempo: 1.5 horas

**Instrucciones Generales:**

* Lea cuidadosamente todo el examen antes de empezar.
* Utilice lapicero de color azul o negro únicamente.
* La utilización de lápiz para la realización del examen elimina la posibilidad de reclamos.
* No se permite el uso de dispositivos electrónicos.

**II Parte. Responda si los enunciados son falsos o verdaderos. Tanto la respuesta de falso o verdadero como la justificación deben estar correctas para que la respuesta sea válida (15 pts)**

1. En general, los costes de construcción de mecanismos de defensa son siempre inferiores a las pérdidas de beneficio ante cualquier tipo de intrusión.  
   R/ Falsa: Depende del tipo de sistema y que recursos tenga disponibles. En algunos casos puede ser más costoso construir mecanismos de defensa que las perdidas potenciales.
2. La probabilidad de un ataque depende de la motivación económica de los atacantes.  
   R/ Verdadera: Suele estar relacionada con la motivación económica, aunque en algunos casos pueden estar motivados por otros factores como políticos o personales.
3. Existen varias maneras de evitar el riesgo asociado a una actividad.

R/ Verdadera: Por ejemplo, delegar la responsabilidad, mitigar los riesgos implementando controles o eliminando el riesgo.

1. Las técnicas SSO benefician la seguridad  
   R/ Verdadera: Al disminuir la cantidad de veces que el usuario necesita autenticarse disminuye el riesgo de ataques de phishing y la gestión de múltiples contraseñas, aunque centraliza el riesgo.
2. Una DMZ ayuda a contener los ataques internos de la red  
   R/ Falsa: Una DMZ está diseñada para proteger principalmente contra ataques externos, no necesariamente ayuda a contener ataques internos, ya que estos suelen originarse detrás de la DMZ.
3. El problema de certificarse en ISO 31000 es que debe volverse a certificarse porque no tienen la capacidad de adaptarse a los cambios   
   R/ Falsa: La ISO 31000 no es una certificación, más bien son un conjunto de directrices para la gestión de riesgos.
4. El proceso de apreciación del riesgo requiere que el tratamiento del riesgo se emitan recomendaciones que reduzcan el al minino la probabilidad de apreciación   
   R/ Verdadera: El objetivo es minimizar el riesgo a un nivel aceptable, pero siempre quedará cierto grado de riesgo residual.
5. No es posible implementar un SGSI sin certificarse en ISO 27001  
   R/ Falsa: La certificación es opcional, pero las empresas las practicas del estándar sin buscar una certificación.
6. La seguridad informática únicamente se enfoca en proteger infraestructura y la información   
   R/ Falsa: También se enfoca en proteger a las personas, los procesos y la disponibilidad de los servicios.
7. No es posible falsificar un No repudio  
   R/ Falsa: Puede ser falsificado en algunos casos, como en la manipulación de firmas digitales.
8. La suplantación de identidad únicamente se puede combatir con autenticación   
   R/ Falsa: También se debe usar sistemas de detección de anomalías y otras medidas como encriptación de los datos.
9. Una vulnerabilidad de hardware legacy solo puede ser explotada en un ambiente de acceso público.   
   R/ Falsa: Puede ser explotada incluso en sistemas de acceso restringido, si no se parchea, puede ser explotada internamente.
10. Un IDS no ayuda a tomar acciones de bloqueo dentro de una red   
    R/ Verdadera: Su función es detectar y alertar sobre posibles intrusiones.
11. Las técnicas de inyección están enfocas principalmente a funciones de identificación de usuarios.   
    R/ Verdadera: Se enfoca principalmente en introducir datos biométricos en un sistema de verificación para suplantar la identidad de una persona.
12. Las medidas técnicas son más importantes que las normativas ya que tienen la capacidad de actuar y tomar acciones sobre amenazas dentro de la infraestructura, mientras que las normativas son solo son reglas que se pueden romper fácilmente.  
    R/ Falsa: Ambas son igual de importantes, las normativas dan un marco para la gestión de seguridad y las técnicas implementan esos controles. Aunque las normas pueden romperse, su función es definir el contexto en que las técnicas se aplican.

**II Parte. Desarrollo. Responda ampliamente lo que se solicita. (Total 5 pts )**

1. Implemente el con SOC con el software TGuard

**https://github.com/tguard-soc-package/nusantara**