1. La clasificación de la información se debe establecer bajo un esquema basado en:
   1. Criticidad y Sensibilidad
   2. Disponibilidad y Sensibilidad
   3. Importancia de la Información
   4. Ninguno

**Respuesta: A**

1. La política de Seguridad de la Información es un documento estratégico dentro de la entidad supervisada, el cual debe estar aprobado por:
   1. Gerencia General
   2. Gerencia Administrativa
   3. La Unidad de Seguridad de la Información
   4. Directorio u órgano equivalente

**Respuesta: D**

1. ¿Cuántas son las capas de Seguridad que tiene el modelo de defensa en profundidad
2. 5
3. 7
4. 8
5. 6

**Respuesta: B**

1. ¿Qué debería Solicitar una Entidad Financiera para el uso de Servicio de Computación en la nube?
2. Análisis de Riego
3. No Objeción
4. Permiso de Uso de Computación en la Nube.
5. Acuerdo de Nivel de Servicio (SLA)

**Respuesta: B**

1. Si tuviera que conocer las vulnerabilidades del IP remoto 200.23.12.198, ¿Que comando de Nmap usaría?

Seleccione una:

1. Nmap -sV 200.23.12.198
2. Nmap -sS 200.23.12.198
3. Nmap -O 200.23.12.198
4. Nmap –script vuln 200.23.12.198

**Respuesta: D**

1. ¿Cuántas veces es recomendable realizar el análisis de Riesgo Tecnologico?
2. Una vez al año
3. Dos veces al año
4. Cuando se identifique un nuevo riesgo tecnológico
5. Cuando lo indique el Gerente General.

**Respuesta: C**

1. ¿Cuál de los siguientes es un algoritmo hash?
2. MD5
3. PKCS12
4. AES
5. ROT13

**Respuesta: A**

1. Se le pidió a un ingeniero de seguridad que implemente una solución segura de acceso remoto que permitirá a los empleados conectarse a la red interna de la empresa. ¿Cuál de las siguientes opciones se puede implementar para minimizar la oportunidad de que ocurra el ataque man-in-the-middle?
2. SSL
3. Autenticacion mutua
4. IPSec
5. Direcciones IP estáticas

**Respuesta: C**

1. ¿Qué solución tecnológica permite la recolección de Logs de información?
2. SIM
3. SEM
4. SIEM
5. Ninguno

**Respuesta: C**

1. ¿Cuáles son los tres tipos de autenticación?
2. Algo que sabes, recuerdas, pruebas
3. Algo que tienes, sabes, eres
4. Algo que muestras, pruebas, eres
5. Algo que muestras, tienes, pruebas

**Respuesta: B**

1. ¿En qué Norma ISO especifica la gestión de Incidente?
2. 27035
3. 9001
4. 27032
5. 27038

**Respuesta: A**

1. ¿Cuántas secciones y controles tiene la Norma ISO 27001 2013?
2. 14 Secciones y 214 Controles
3. 16 Secciones y 114 Controles
4. 14 Secciones y 114 Controles
5. 14 Secciones y 104Controles

**Respuesta: C**

1. ¿En qué Sección de la Recopilación de Normas para el Servicio Financiero, se menciona el Registro, Cuantificación y Monitoreo de Incidentes de Seguridad de la Información?
2. Libro 3, Titulo Vll, Capitulo 2, Sección 8.
3. Libro 3, Titulo Vll, Capitulo 2, Sección 9.
4. Libro 3, Titulo Vll, Capitulo 3, Sección 7.
5. Libro 3, Titulo Vll, Capitulo 3, Sección 9.

**Respuesta: B**

1. ¿En qué Articulo de la Sección 4, del Capítulo 2 Titulo Vll del Libro 3 de la Recopilación de Normas para el Servicio Financiero, menciona la Administración de Privilegios?
2. Artículo 2º
3. Artículo 4º
4. Artículo 3º
5. Artículo 7º

**Respuesta: A**

1. ¿Cuál de los siguientes grupos puede clasificarse como incidentes de seguridad de la información?

|  |  |  |
| --- | --- | --- |
| a) | b) | c) |
| Denegación de servicio | Pérdida de servicio | Código malicioso |
| Código malicioso | Código malicioso | Mal funcionamiento de software |
| Ausencia de personal por cumpleaños | Incumplimiento de políticas o procedimientos | Pérdida del mouse de mi pc |

**Respuesta: B**

1. Según la Recopilación de Normas para el Servicio Financiero, la gestión de accesos debe realizarse en base a:
2. Política de Seguridad de la Información.
3. Análisis de riesgos
4. Mayor Privilegio
5. Menor Privilegio

**Respuesta: D**

1. ¿Qué debe de contener la documentación técnica asociada a la infraestructura de redes y telecomunicaciones?

**R: Características, topología y diagrama de red, Certificación del cableado estructurado de la red, Descripción de los elementos de cableado, planos de trayectoria del cableado y ubicación de puntos de salida, Diagrama del sistema de interconexión de cables de red, distribución de regletas y salidas.**

1. Mencione los pasos para la Gestión de Incidentes

**R: Notificación del incidente, Clasificación del incidente, Tratamiento del incidente, Cierre del incidente, Base de conocimiento**

1. ¿Considerarías que la Interrupción del servicio de pago de luz en una agencia es un incidente de Seguridad y Como lo catalogarías?

**R1: Si es un incidente, si la interrupción es a causa de nuestros enlaces de comunicación, y se cataloga como perdida de servicio**

**R2: No es un incidente, si es una caída de servicio por parte del proveedor.**

1. ¿Qué Datos mínimamente debe contener un registro de un Incidente de Seguridad de la Información?

**R: Activo Relacionado, Agencia Afectada, Servicios Afectados, Detalle, Fecha y Hora, Clasificación, Impacto y Evidencias**

1. Mencione 5 categorías de clasificación de incidentes de Seguridad de la información

**R:**

1. Mencione los criterios de la Seguridad de la Información según la ASFI

**R: Autenticación, Confiabilidad, Confidencialidad, Cumplimiento, Disponibilidad Integridad y No repudio.**

1. ¿Qué es un Incidente de Seguridad de la Información?

**R: Evento o serie de eventos, que tienen una probabilidad significativa de comprometer las operaciones de la entidad, amenazar la seguridad de la información y/o los recursos tecnológicos.**

1. Mencione por lo menos 5 Requisitos que deben tener los Sistemas de Transferencias y Transacciones Electrónicas según la RNSF en el Titulo Vll “Requisitos Mínimos de Seguridad”.

**R:**

1. **Seguridad del Sistema**
2. **Canal de Comunicación**
3. **Difusión de Políticas de Seguridad de la Información**
4. **Certificación Digital**
5. **Continuidad Operativa**
6. **Disponibilidad de la información**
7. **Registro de Pistas de Auditoria**
8. **Verificación y Control de transacciones y trasferencias electrónicas**
9. **Acuerdos Privados**
10. Mencione los pasos que son parte del enfoque de ciberseguridad

**R: Identificación de amenazas, Respuesta de Incidentes de Seguridad, Identificar el riesgo y las vulnerabilidades y Establecer planes de contingencia**