Universidad Nacional de Ingeniería

Facultad de Ciencias

Escuela Profesional de Ciencia de la Computación

Seguridad Informática

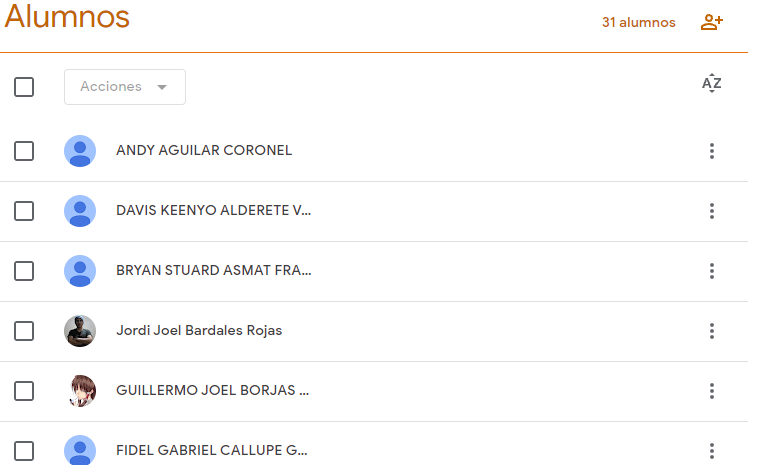
**Práctica de Seguridad Informática**

**SEG Ciclo: 2021-II Fecha:02/10/2021**

**Profesor: Sidney Valer Quispe**

Pregunta 1 (5 puntos)

El profesor desea obtener un listado de los alumnos matriculados en un curso.



|  |  |  |  |
| --- | --- | --- | --- |
| Nro | Nombre | Apellido Paterno | Apellido Materno |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
|  |  |  |  |
|  |  |  |  |

Pregunta 2 (5 puntos)

Extraer los datos de autos usados que se ofertan en internet(Elegir una página donde oferten autos usados).

Fecha:

URL Pagina:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nro. | Auto | Modelo | Precio | Año de Fabricación |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Teoría: Justificar su respuesta como el siguiente ejemplo: (8 puntos)

1. ¿Cuál de las siguientes opciones contiene las metas y objetivos principales de la seguridad?

1. El perímetro frontera de una red
2. La tríada CID
3. Un sistema autónomo
4. Internet

Ejemplo de solución

B. Las metas y objetivos principales de la seguridad son la confidencialidad, la integridad y la disponibilidad, comúnmente denominadas la tríada CID.

2. Las vulnerabilidades y los riesgos se evalúan en función de sus amenazas contra ……… Elegir una alternativa?

1. Uno o más principios de la tríada CID
2. La utilidad de los datos
3. La debida atención
4. Alcance de la responsabilidad

3. ¿Cuál de los siguientes principios de la tríada CID, refiere que los sujetos autorizados tienen acceso oportuno e ininterrumpido a los objetos?

1. Identificación
2. Disponibilidad
3. Encriptación
4. Estratificación

4. ¿Cuál de las siguientes alternativas no se considera una violación de la confidencialidad?

1. Robar contraseñas
2. Espiar
3. Destrucción de hardware
4. Ingeniería social

5. ¿Cuál de las siguientes opciones no es cierta?

1. Las violaciones de la confidencialidad incluyen errores humanos.
2. Las violaciones de la confidencialidad incluyen la supervisión de alta dirección.
3. Las violaciones de la confidencialidad se limitan a los ataques intencionados y directos.
4. Las violaciones de la confidencialidad pueden producirse cuando la transmisión del mensaje no está correctamente encriptada.

6. El STRIDE es un modelo de amenazas, se utiliza a menudo para evaluar las amenazas contra las aplicaciones o los sistemas operativos. ¿Cuál de los siguientes no es un elemento de STRIDE?

1. Suplantación
2. Elevación de privilegios
3. Repudio
4. Divulgación

7. Si un mecanismo de seguridad ofrece disponibilidad, entonces ofrece un alto nivel de garantía a los sujetos autorizados para poder ………………a los datos, objetos y recursos.

1. Controlar
2. Auditoría
3. Acceder
4. Repudiar

8. …………….. se refiere a mantener la confidencialidad sobre la información personal que podría causar daño, vergüenza o deshonra a alguien si se revela.

1. Aislamiento
2. Ocultación
3. Privacidad
4. Criticidad

9. ¿Qué garantiza, que el sujeto no pueda negar una actividad o evento que ocurrió?

1. La tríada CIA
2. Abstracción
3. No repudio
4. Hash

10. ¿Cuál de los siguientes no se considera un ejemplo de ocultamiento de datos?

1. Prevenir que un trabajador autorizado a leer un objeto borre dicho objeto
2. Evitar que visitantes no autorizados accedan a una base de datos
3. Impedir que un sujeto de un nivel de clasificación inferior acceda a datos de un nivel de clasificación superior.
4. Impedir que una aplicación acceda directamente al hardware

11. ¿Cuál es el objetivo principal de la gestión del cambio?

1. Mantener la documentación
2. Mantener a los usuarios informados de los cambios
3. Permitir la reversión de los cambios fallidos
4. Evitar que la seguridad se vea comprometida

12. ¿Cuál es el objetivo principal de los esquemas de clasificación de datos?

1. Controlar el acceso a los objetos por los sujetos autorizados
2. Formalizar y estratificar el proceso de seguridad de los datos en función de las etiquetas asignadas de importancia y sensibilidad
3. Establecer un rastro de transacciones para auditar la responsabilidad
4. Manipular los controles de acceso para proporcionar los medios más eficientes para conceder o restringir la funcionalidad

13. ¿Cuál de las siguientes opciones, normalmente no es una característica que se considere para clasificar los datos?

1. Valor
2. Tamaño del objeto
3. Vida útil
4. Implicaciones para la seguridad

14. Las clasificaciones de datos se utilizan para centrar los controles de seguridad en los siguientes casos excepto en una de ellas?

1. Almacenamiento
2. Procesamiento
3. Estratificación
4. Transferencia

15. ¿Cuál de los siguientes opciones es el elemento más débil de cualquier solución de seguridad?

1. Los productos de software
2. Las conexiones a Internet
3. Políticas de seguridad
4. Humanos

16. Cuando se busca contratar nuevos empleados, ¿cuál es el primer paso?

1. Crear una descripción del puesto de trabajo.
2. Establecer la clasificación del puesto.
3. Seleccionar a los candidatos.
4. Solicitar currículos.

17. Si una organización contrata a entidades externas para que le proporcionen funciones o servicios, como por ejemplo el soporte técnico o de cuentas, ¿cómo se denomina el proceso que se utiliza para garantizar que estas entidades proporcionan suficiente seguridad?

1. Identificación de activos
2. Gestión de tercerización
3. Entrevista de salida
4. Análisis cualitativo

18. ¿Cuál de las siguientes afirmaciones no es cierta?

1. La seguridad informática sólo proporcionar protección contra los ataques lógicos o técnicos.
2. El proceso mediante el cual se logran los objetivos de la gestión de riesgos se conoce como análisis de riesgo.
3. Los riesgos para una infraestructura de TI están todos basados en la informática.
4. Un activo es cualquier cosa utilizada en un proceso o tarea empresarial.

19. ¿Cuál de los siguientes no es un elemento del proceso de análisis de riesgos?

1. Analizar un entorno en busca de riesgos
2. Crear un informe de coste/beneficio de las salvaguardas para presentarlo a la alta dirección
3. Seleccionar las salvaguardias adecuadas y aplicarlas
4. Evaluar cada evento de amenaza en cuanto a su probabilidad de ocurrencia y el coste de los daños resultantes daños resultantes

20. ¿Cuál de los siguientes elementos no se considera generalmente un activo en un análisis de riesgos?

1. Un proceso de desarrollo
2. Una infraestructura de TI
3. Un recurso de un sistema propio
4. Los archivos personales de los usuarios

21. ¿Cuál de las siguientes opciones representa la explotación accidental o intencional de vulnerabilidades?

1. Eventos de amenaza
2. Riesgos
3. Agentes de amenaza
4. Infracciones

22. Cuando una salvaguarda o una contramedida no está presente o no es suficiente, ¿qué queda?

1. La vulnerabilidad
2. Exposición
3. Riesgo
4. Penetración

23. ¿Cuál de las siguientes no es una definición válida de riesgo?

1. Una evaluación de la probabilidad, la posibilidad o el azar
2. Cualquier cosa que elimine una vulnerabilidad o proteja contra una o más amenazas específicas
3. Riesgo = amenaza \* vulnerabilidad
4. Cada caso de exposición

24. Al evaluar las salvaguardias, ¿cuál es la regla que debe seguirse en la mayoría de los casos?

1. El coste anual previsto de la pérdida de activos no debe superar los costes anuales de salvaguardias.
2. Los costes anuales de las salvaguardas deben ser iguales al valor del activo.
3. Los costes anuales de las salvaguardias no deben superar el coste anual previsto de pérdida de activos.
4. Los costes anuales de las salvaguardias no deben superar el 10% del presupuesto de seguridad.

25. ¿Qué control de seguridad se centra directamente en la prevención de la colusión?

1. Principio de mínimo privilegio
2. Descripciones de puestos de trabajo
3. Separación de funciones
4. Análisis de riesgos cualitativos

26. ¿Qué proceso o evento suele organizar una organización y está dirigido a grupos de empleados con funciones de trabajo similares?

1. Educación
2. Concienciación
3. Formación
4. Terminación

27. ¿Cuál de las siguientes opciones no es específica o directamente relacionada con la gestión de la función de seguridad de una organización?

1. La satisfacción laboral de los trabajadores
2. Las métricas
3. Estrategias de seguridad de la información
4. Presupuesto

28. Al realizar un análisis de riesgos, usted identifica una amenaza de incendio y una vulnerabilidad porque no hay extintores. Basándose en esta información, ¿cuál de los siguientes es un posible riesgo?

1. Infección por virus
2. Daño al equipo
3. Mal funcionamiento del sistema
4. Acceso no autorizado a información confidencial

29. Has realizado un análisis de riesgo cuantitativo básico sobre una relación específica de amenaza/vulnerabilidad/riesgo. Seleccionas una posible contramedida. Al volver a realizar los cálculos, ¿cuál de los siguientes factores cambiará?

1. El factor de exposición
2. Expectativa de pérdida única (SLE)
3. Valor de los activos
4. Tasa de ocurrencia anualizada

Realizar paso a paso la guía y presentar la evidencia de haberlo realizado (captura de pantallas) 2 puntos

Modulo 2 Footprinting and Reconnaissance Pagina 3436 - 3608