Instituto de Ciencias Tecnológicas

FECHA: 27-04-2017

Solemne Nº 1

NOMBRE: _____

CODIGO: CA402 **Puntaje Final 100 %**

I. Seleccione Verdadero o Falso **34 puntos 0.2 puntos cada una.**

1. La fortaleza que presenta una organización frente a las contingencias que tienen lugar en el entorno del procesamiento de datos se denomina Vulnerabilidad _____ F

2. Los tipos de medidas de Seguridad pueden ser Preventivos, Detectivos y Evolutivos _____F

3. La información es un valor operativo en las empresas, cuya pérdida tiene una causa _____F

4. La Seguridad Informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad. _____V

5. La Integridad en Seguridad de la Información corresponde a la información que debe ser protegida de modificaciones autorizadas _____F

6. La Disponibilidad en Seguridad de la Información corresponde a la información y servicios que debe estar disponibles siempre que se necesiten. _____V

7. La Confidencialidad en Seguridad de la Información se relaciona con que se debe garantizar que la información es conocida únicamente por a quien le interese _____V

8. Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y por los administradores informáticos. _____F

9. La información constituye el activo más importante de las empresas, pudiendo verse afectada por muchos factores tales como levantamiento de información y pruebas de usuarios _____F

10. El respaldo de datos debe ser completamente automático y continuo. Debe funcionar de forma transparente, interviene en las tareas que se encuentra el usuario _____F

11. La Gestión de Riesgo es un método que se puede aplicar en diferentes contextos donde se debe incluir y trabajar con las consideraciones de la seguridad _____V

12. Contingencia es una amenaza al conjunto de los peligros a los que están expuestos los recursos informáticos de una organización _____V

13. Los tipos de medidas Preventivas limitan las posibilidades que se concreten las contingencias _____ V

14. Los tipos de medidas Correctivas están orientadas a recuperar la operación normal _____ V

15. Los métodos de encriptación usan algoritmos matemáticos en función de cadenas validas o passwords y son valiosos para la protección de datos y redes _____V

16. El Plan de Seguridad es una amenaza al conjunto de los peligros a los que están expuestos los recursos informáticos de una organización. _____F

17. El spoofing consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP. _____F

II. Selección múltiple, en algunas preguntas la respuesta correcta es una alternativa, en otra dos. 66 puntos 0.3 puntos cada una.

1. El proceso de auditar requiere de un proceso de planificación, es decir se debe:

a) Confrontar que se va a auditar, quien lo va a hacer y cuando.
b) Determinar que se va a auditar, cuando y quien lo va a hacer.
c) Verificar que se va a auditar, quien lo va a hacer y cuando.
d) Determinar que se va a auditar, como y quien lo va a hacer.

2. El auditor informático al detectar irregularidades en el transcurso de la auditoria informática que le indiquen la ocurrencia de un delito informático, deberá realizar lo siguiente:

a) Informar a autoridades regulatorias cuando es un requerimiento legal.
b) Establecimiento de planes de contingencia efectivos.
c) Determinar los vacíos de la seguridad existentes y que permitieron el delito.
d) Adquisición de herramientas de control.

3. La auditoría se puede clasificar por la procedencia del auditor, por su área de aplicación, áreas especializadas, y sistemas computacionales, dentro de esta última pueden considerarse:

a) Auditoría contable, Auditoría con y sin el computador.
b) Auditoría outsourcing, Auditoría al manejo de mercancías.
c) Auditoría informática, Auditoría a la gestión informática.
d) Auditoría laboral, Auditoría a la gestión informática.

4. El estudio de entorno auditable requiere del examen de las funciones y actividades generales de la informática. Para realizar este examen el auditor debe conocer:

a) Aplicaciones bases de datos y archivos.
b) Arquitectura y configuración de Hardware y Software.
c) La organización y el entorno operacional.
d) Inventario de Hardware y Software.

5. En relación a la Seguridad de la Información:

a) Debe incluir copias de seguridad incompleta y copias de seguridad decrementales.
b) Debe incluir copias de seguridad incompleta y copias de seguridad incrementales.
c) Debe incluir copias de seguridad completa y copias de seguridad decrementales.
d) Debe incluir copias de seguridad completa y copias de seguridad incrementales.

6. El programa de auditoría es fundamental para el proceso de auditoría ya que da la seguridad de que el trabajo se planeó adecuadamente. De los siguientes conceptos, cuales definen correctamente un programa de auditoría:

a) Permite identificar y clasificar para su posterior análisis, todos los aspectos de mayor significación y que en un momento dado pueden afectar la operatividad de la entidad auditada.
b) Conjunto de diagramas, diseñados para alcanzar los objetivos planificados en una auditoria.
c) Confronta información producida por diferentes unidades administrativas o instituciones, en relación con una misma operación o actividad.
d) El programa de auditoría es fundamental para el proceso de auditoría ya que da la seguridad de que el trabajo se planeó adecuadamente.

7. Dada la siguiente afirmación: ”El examen de cualquier operación, actividad, área, programa, proyecto o transacción, se realiza mediante la aplicación de técnicas, y el auditor debe conocerlas para seleccionar la más adecuada, de acuerdo con las características y condiciones del trabajo que realiza”.

a) Dada la experiencia del auditor puede omitir el uso de algunas de las técnicas de auditoría y utilizar solo aquellas con las más se sienta cómodo para desarrollar su trabajo.
b) Todo proceso de auditoría se basa en la utilización de técnicas pero hay algunas excepciones, como es el caso de la auditoría interna.
c) La utilización de las técnicas de auditoría se basa en la acción que se va a desarrollar, pudiendo hacer uso de técnicas documentales, físicas, analíticas entre otras.
d) La experiencia del auditor le permite aplicar técnicas de auditoría solo el algunos casos, dado que puede realizar el análisis por simple observación.

8. La planificación de una auditoria comienza con la obtención de información necesaria para definir la estrategia a emplear y culmina con la definición detallada de las tareas a realizar en la fase de ejecución.

a) Planificar una auditoria implica familiarizarse con las operaciones para analizar las deficiencias y posibles causas y definir los medios de comprobación que se van a utilizar.
b) Planificar es obtener y estudiar documentos e información sobre la unidad a auditarse.
c) Realizar o no una planificación de auditoría no tiene injerencia en los resultados de la misma.
d) La planificación implica fijar una metodología inmodificable en el proceso de auditoría.

9. En esta área la Auditoria Informática, entorno del Software, analizará los sistemas de prevención y detección de fraudes, los exámenes a aplicaciones concretas, los controles a establecer, en definitiva, todo lo relacionado con la fiabilidad, integridad y seguridad del SW.

a) Revisar la seguridad lógica de las librerías de los programadores.
b) Examinar los controles sobre el datacenter.
c) Revisar la seguridad lógica de los datos y programas.
d) Examinar metodología de construcción en uso.

10. Los planes principales de un programa de administración de la seguridad de sistemas están apoyados por:

a) Nivel superior, técnico u operativo de la organización.
b) Nivel inferior, técnico o operativo de la organización,
c) Nivel auxiliar o de apoyo de la organización.
d) Nivel intermedio ejecutivo o directivo de la organización.

11. El conjunto de procedimientos que luego de producido un desastre, pueden ser rápidamente ejecutados para restaurar las operaciones normales con máxima rapidez y mínimo impacto, corresponde a:

a) Plan de Pruebas.
b) Plan de Seguridad.
c) Plan de RollBack.
d) Plan de Contingencia.

12. En el Departamento de Desarrollo de Software, área importante donde la auditoría deberá velar por la adecuación de la informática a las necesidades reales de la Empresa, se considera dentro de los objetivos:

a) Examinar metodología de construcción en uso.
b) Evaluar la eficiencia y eficacia de operación del área de producción.
c) Revisar la definición de los objetivos del sistema, analizar si cumple con las necesidades de los usuarios.
d) Comprende la evaluación de los equipos de computación, procedimientos de entradas de datos, controles, archivos, seguridad y obtención de la información.
e) Revisar el control y planificación del proyecto.

13. En la distribución de un Datacenter se puede encontrar:

a) Configuración de Pasillos Fríos y Calientes.
b) Ubicaciones de Gabinetes.
c) Láminas de Piso falso.
d) Instalación de Racks sobre el piso falso.
e) Especificaciones.

14. Algunas consecuencias inmediatas en relación a la Vulnerabilidad corresponden a:

a) Imposibilidad de procesar.
b) Perdida de archivos y registros.
c) Lectura indebida.
d) Legales y Económicas/financieras.
e) Incidencia en otros sistemas.

15. Los objetivos esenciales del plan de contingencia son:

a) Minimizar el impacto y promover una lenta recuperación de la operatividad.
b) Minimizar el impacto y promover una lenta recuperación de la operatividad.
c) Minimizar el impacto y promover una rápida recuperación de la operatividad.

16. El objetivo del Plan de Seguridad es:

a) Proteger los pasivos informáticos en cuanto a integridad, confidencialidad, privacidad y continuidad.

b) Proteger los activos informáticos en cuanto a integridad, confidencialidad, privacidad y discontinuidad.

c) Proteger los activos informáticos en cuanto a integridad, confidencialidad, privacidad y continuidad.

d) Proteger los activos informáticos en cuanto a integridad, confidencialidad, generalidad y continuidad.

17. Los Métodos de encriptación son:

a) Valiosos para la protección de datos y redes y usan algoritmos complejos en función de cadenas válidas o passwords.

b) Valiosos para la protección de datos y redes y usan algoritmos simples en función de cadenas válidas o passwords.

c) Valiosos para la protección de datos y redes y usan algoritmos matemáticos en función de cadenas válidas o passwords.

d) Valiosos para la protección de datos y redes y usan algoritmos estadísticos en función de cadenas válidas o passwords.

18. Una pista de Auditoria es:

a) Una huella o registro generado manualmente que está orientado a un análisis anterior y permite reconstruir los flujos de información, es un camino hacia atrás.

b) Una huella o registro generado automáticamente que está orientado a un análisis anterior y permite reconstruir el procesamiento, es un camino hacia adelante.

c) Una huella o registro generado automáticamente que está orientado a un análisis posterior y permite reconstruir el procesamiento, es un camino hacia atrás.

d) Una huella o registro generado manualmente que está orientado a un análisis anterior y permite reconstruir el procesamiento, es un camino hacia atrás.

19. La Administración de Riesgos se relaciona con:

a) Establecer un marco general, identificar alternativas, análisis de riesgos, evaluar y priorizar riesgos, tratamiento del proceso, monitorear y revisar, proceso de administración de riesgos.

b) Establecer un marco general, identificar políticas, análisis de riesgos, evaluar y priorizar riesgos, tratamiento del riesgo, monitorear y revisar, proceso de administración de riesgos.

c) Establecer un marco general, identificar riesgos, análisis de riesgos, evaluar y priorizar alternativa de solución, tratamiento del riesgo, monitorear y revisar, proceso de administración de riesgos.

d) Establecer un marco general, identificar riesgos, análisis de riesgos, evaluar y priorizar riesgos, tratamiento del riesgo, monitorear y revisar, proceso de administración de riesgos.

20. La inseguridad en la información no genera solo pérdidas de información, se relaciona con::

a) Accesos autorizados a la información sensible, vulnerables a acciones mal.

b) Alteraciones en la información, cambios de información no autorizados.

c) La documentación de la metodología de la fábrica de software esta siempre disponible.

d) Disponibilidad de la información, pérdidas de productividad.

21. La gestión de riesgos está relacionada con:

a) Características o amenazas en el sistema de seguridad que pueden ser explotadas para causar daños o perdidas, facilitan la ocurrencia de una amenaza.

b) Características o fortalezas en el sistema de seguridad que pueden ser explotadas para causar daños o perdidas, facilitan la ocurrencia de una amenaza.

c) Características o oportunidades en el sistema de seguridad que pueden ser explotadas para causar daños o perdidas, facilitan la ocurrencia de una amenaza.

d) Características o debilidades en el sistema de seguridad que pueden ser explotadas para causar daños o perdidas, facilitan la ocurrencia de una amenaza.

22. En la gestión de riesgos de Seguridad Informática la interrupción indica:

a) Un activo se pierde, está disponible, o no se puede utilizar.

b) Un activo se pierde, no está disponible, y se puede utilizar.

c) Un activo se pierde, no está disponible, o no se puede utilizar.

d) Un activo se pierde, está disponible, y se puede utilizar.