Cyber Security Ops

Reactivos

Pregunta 1

Después de renunciar a la empresa XYZ S.A., Francesco decide alterar la base de datos de la compañía y negar el acceso a los demás desarrolladores.

¿Qué norma internacional quebrantó Francesco y cuáles son los aspectos fundamentales que transgredió?

Opciones:

a. ISO/IEC 27002. Integridad, confidencialidad y disponibilidad.
b. ISO/IEC 27001. Integridad, confidencialidad y disponibilidad.
c. ISO/IEC 27032. Integridad, confidencialidad y seguridad.
d. ISO/IEC 27002. Integridad, confidencialidad y seguridad.

Pregunta 2

Después de un incidente con su base de datos, Misael realizó una auditoría de ciberseguridad en la empresa XYZ S.A.; al llevar a cabo la revisión, se percató de que, para acceder a información confidencial, solo se requiere colocar el nombre de un colaborador que todos conocían hasta antes del incidente.

¿Cuáles son los procesos de control que se deben aplicar para cada colaborador en la empresa?

Opciones:

a. > Selección
   > Aproximación
   > Autorización

b. > Identificación
   > Resolución
   > Resguardo

c. > Identificación
   > Autenticación
   > Autorización

d. > Individualización
   > Autenticación
   > Responsabilidad

Pregunta 3

En la gestión de cuentas privilegiadas, ¿qué función importante cumplen las soluciones PAM?

Opciones:

a. Las soluciones PAM proporcionan cuentas privilegiadas, sin restricciones, a todos los usuarios.
b. Las soluciones PAM cifran las credenciales, rotan contraseñas periódicamente, registran actividades y generan informes para auditoría.
c. Las soluciones PAM eliminan por completo las cuentas privilegiadas.
d. Las soluciones PAM comparten contraseñas en texto claro.

Pregunta 4

El uso de una autenticación biométrica, en conjunto con un NIP, aumenta la seguridad y la protección de cuentas. ¿De qué forma parte esta medida?

Opciones:

a. Acceso a bases de datos
b. Agilización del proceso para acceder a una cuenta
c. Transacciones bancarias
d. Múltiple factor de autenticación

Pregunta 5

Generalmente, identificación y autenticación se realizan mediante el empleo de "usuario y contraseña". En el proceso de autenticación, ¿qué diferencia clave existe entre ambos conceptos?

Opciones:

a. La identificación es un proceso que solo se aplica con usuarios administrativos, mientras que la autenticación se emplea con los regulares.
b. La identificación es el proceso de verificar que el usuario sí es quien dice ser, mientras que la autenticación se refiere a proporcionar un nombre de usuario.
c. La identificación es un proceso para reconocer al usuario, mientras que la autenticación permite verificar que sí es quien dice ser.
d. Identificación y autenticación son términos intercambiables, ya que se refieren al mismo proceso.

Pregunta 6

¿Por qué es importante gestionar y clasificar los activos de *hardware* y software en las organizaciones?

Opciones:

a. La gestión y clasificación de activos garantizan que una organización opere en las mejores condiciones de seguridad y, además, que ejecute procesos adecuados de protección.
b. La gestión y clasificación de activos son tareas opcionales, así que no tienen ningún impacto en la seguridad.
c. La gestión de activos solo es importante en plataformas físicas, pero no en la nube.
d. La gestión de activos se realiza únicamente para reducir costos operativos.

Pregunta 7

Según la definición de la International Organization for Standardization, ¿cómo se define un activo en una organización?

Opciones:

a. En una organización, un activo es cualquier elemento tangible, como muebles de oficina.
b. En una organización, un activo es aquello que cuesta dinero y tiene cierto valor.
c. En una organización, un activo es cualquier recurso independientemente de su costo o valor; de hecho, puede no tener un costo para la organización.
d. En una organización, un activo es solo el hardware de cómputo.

Pregunta 8

¿Cuáles son las etapas del ciclo de vida de la gestión de activos de hardware y qué actividades se asocian con cada una de ellas?

Opciones:

a. Las etapas son adquisiciones, despliegue, mantenimiento, soporte, así como retiro y eliminación. Algunas actividades asociadas con estas etapas incluyen la creación de órdenes de compra en la etapa de adquisiciones, la actualización de inventarios en la etapa de despliegue, la programación de escaneo de seguridad en la etapa de mantenimiento, la revisión de fechas de vencimiento en la etapa de soporte y, finalmente, la actualización del inventario de equipo en la etapa de retiro y eliminación.
b. Las etapas son adquisiciones, soporte y retiro y eliminación; por su parte, las actividades no son relevantes.
c. Las etapas son despliegue, mantenimiento y soporte; por su parte, las actividades consisten únicamente en la compra de activos y en su eliminación.
d. Las etapas son adquisiciones, despliegue, mantenimiento, soporte, retiro, eliminación y reciclado. Algunas actividades asociadas con estas etapas incluyen la creación de órdenes de compra en la etapa de adquisiciones, la revisión de fechas de vencimiento en la etapa de soporte, la actualización del inventario de equipo en la etapa de retiro, así como su reutilización y eliminación durante la mitad de su ciclo de vida.

Pregunta 9

En la fase de mantenimiento, ¿qué tipo de alerta se utiliza para notificar posibles problemas en los activos virtuales?

Opciones:

a. En la fase de mantenimiento, se utilizan mensajes de WhatsApp para notificar posibles problemas en los activos virtuales.
b. En la fase de mantenimiento, se utilizan cartas postales para notificar posibles problemas en los activos virtuales.
c. En la fase de mantenimiento, se utilizan alertas por correo electrónico o SMS para notificar posibles problemas en los activos virtuales.
d. En la fase de mantenimiento, se utilizan llamadas telefónicas para notificar posibles problemas en los activos virtuales.

Pregunta 10

¿Cuál es uno de los principales tipos de servicio en la gestión de activos en la nube?

Opciones:

a. Uno de los principales tipos de servicio en la gestión de activos en la nube es el *Software as a Service* (SaaS).
b. Uno de los principales tipos de servicio en la gestión de activos en la nube es la *Update as a Service* (UaaS).
c. Uno de los principales tipos de servicio en la gestión de activos en la nube es el *Hardware as a Service* (HaaS).
d. Uno de los principales tipos de servicio en la gestión de activos en la nube es el *Middleware as a Service* (MaaS).

Pregunta 11

¿Cuál es el tiempo recomendado para remediar una vulnerabilidad de categoría media?

Opciones:

a. El tiempo recomendado para remediar una vulnerabilidad de categoría media es de 15 días.
b. El tiempo recomendado para remediar una vulnerabilidad de categoría media es de 30 días.
c. El tiempo recomendado para remediar una vulnerabilidad de categoría media es de 90 días.
d. El tiempo recomendado para remediar una vulnerabilidad de categoría media es de 60 días.

Pregunta 12

¿Cómo se dividen las amenazas en términos de su intencionalidad?

Opciones:

a. Las amenazas se dividen en términos de frecuencia e impacto.
b. En función de su intencionalidad, las amenazas se dividen en dos tipos: intencionales y no intencionales.
c. En función de su intencionalidad, las amenazas se dividen en tres tipos: intencionales, semintencionales y no intencionales.
d. Las amenazas se dividen en primarias y secundarias.

Pregunta 13

¿Qué hacen las herramientas de escaneo de vulnerabilidades con la información recopilada en los primeros pasos del proceso de identificación?

Opciones:

a. Las herramientas de escaneo de vulnerabilidades eliminan la información recopilada para evitar riesgos.
b. Las herramientas de escaneo correlacionan la información recopilada con la base de vulnerabilidades conocidas.
c. Las herramientas de escaneo de vulnerabilidades utilizan la información recopilada para crear copias de seguridad.
d. Las herramientas de escaneo de vulnerabilidades almacenan la información recopilada en servidores externos.

Pregunta 14

En el sistema operativo Windows Server 2019, ¿cómo se identifican los parches de seguridad?

Opciones:

a. En Windows Server 2019, los parches de seguridad se identifican con un icono especial.
b. En Windows Server 2019, los parches de seguridad no tienen una identificación específica.
c. En Windows Server 2019, los parches de seguridad se identifican con el prefijo "PS", seguido de un número.
d. En Windows Server 2019, los parches de seguridad se identifican con el prefijo "KB," seguido de un número.

Pregunta 15

¿Por qué los fabricantes generan soluciones de parches de seguridad?

Opciones:

a. Los fabricantes generan soluciones de parches de seguridad para aumentar la velocidad de la red.
b. Los fabricantes generan soluciones de parches de seguridad para disminuir la protección en caso de ataques.
c. Los fabricantes generan soluciones de parches de seguridad para abordar las vulnerabilidades identificadas y, además, para proporcionar correcciones a los problemas de seguridad.
d. Los fabricantes generan soluciones de parches de seguridad para identificar nuevas vulnerabilidades.

Pregunta 16

¿Cuáles son los tres tipos principales de controles internos?

Opciones:

a. Los tres tipos principales de controles internos son detectivos, preventivos y administrativos.
b. Los tres tipos principales de controles internos son técnicos, preventivos y compensatorios.
c. Los tres tipos principales de controles internos son administrativos, técnicos o lógicos y físicos.
d. Los tres tipos principales de controles internos son preventivos, correctivos y detectivos.

Pregunta 17

¿Qué tipo de políticas y prácticas se recomiendan para la implementación efectiva de controles preventivos?

Opciones:

a. Se recomiendan políticas y prácticas como la eliminación de contraseñas y la divulgación de información confidencial.
b. Se recomiendan políticas y prácticas como la exposición de sistemas a amenazas.
c. Se recomiendan algunas políticas y buenas prácticas, como estándares, mecanismos de encriptado, *firewalls*, aplicaciones para detectar *malware* y para mantener los sistemas actualizados y con parches de seguridad aplicados, así como la eliminación de cuentas de usuario, software o servicios innecesarios.
d. Se recomiendan políticas y prácticas como la promoción de interacciones de usuarios con sistemas.

Pregunta 18

¿Cuál es el propósito principal de los controles detectivos?

Opciones:

a. El propósito principal de los controles detectivos consiste en promover interacciones de usuarios con sistemas.
b. El propósito principal de los controles detectivos consiste en identificar problemas o riesgos que no se pueden gestionar a través de un control preventivo, así como localizar actividades no autorizadas o incidentes de seguridad.
c. El propósito principal de los controles detectivos consiste en prevenir incidentes de seguridad antes de que ocurran.
d. El propósito principal de los controles detectivos consiste en eliminar por completo las vulnerabilidades del sistema.

Pregunta 19

¿Cuál es el propósito principal de los controles correctivos?

Opciones:

a. El propósito principal de los controles correctivos es restaurar los sistemas o recursos de cómputo a su estado anterior, sobre todo después de un incidente de seguridad o actividad no autorizada.
b. El propósito principal de los controles correctivos es detectar amenazas antes de que se conviertan en incidentes de seguridad.
c. El propósito principal de los controles correctivos es minimizar la probabilidad de incidentes de seguridad.
d. El propósito principal de los controles correctivos es evitar que ocurran incidentes de seguridad.

Pregunta 20

¿Cuál es la diferencia entre los controles correctivos y los de recuperación?

Opciones:

a. Los controles correctivos y de recuperación son sinónimos.
b. Los controles correctivos previenen ataques a la organización, mientras que los de recuperación complementan su trabajo.
c. Los controles correctivos buscan restaurar el 100% de las operaciones de una organización, mientras que los de recuperación se enfocan en solucionar un problema específico.
d. Los controles correctivos se enfocan en solucionar un problema específico, mientras que los de recuperación buscan restaurar el 100% de las operaciones de una organización.

Pregunta 21

¿Cuál es el objetivo principal de una línea base de seguridad?

Opciones:

a. Proteger lo suficiente de las vulnerabilidades y las amenazas.
b. Establecer un conjunto de controles mínimos de seguridad para un sistema de información.
c. Establecer un conjunto de ajustes recomendados para diferentes niveles de impacto.
d. Trabajar eficiente y eficazmente.

Pregunta 22

¿Cuál es el objetivo principal del control de cambios?

Opciones:

a. Mantener seguros los sistemas y aplicativos.
b. Controlar los cambios frecuentes en los sistemas de información.
c. Mitigar las interrupciones en los activos de alto valor.
d. Optimizar los beneficios de los sistemas de información.

Pregunta 23

¿Qué es la gestión de versiones?

Opciones:

a. Un registro completo de cada cambio con su auditoría y otros detalles.
b. Un proceso de revisión de archivos o documentos.
c. Un mecanismo que rastrea el progreso de los cambios de un archivo.
d. Una alternativa expandida del control de versiones.

Pregunta 24

¿Cuál es una ventaja de utilizar un sistema de gestión de versiones?

Opciones:

a. Permite tener una visión global en cada uno de los pasos que conlleva el proceso de revisión de archivos o documentos.
b. Facilita la identificación de los cambios que han sufrido distintas versiones de documentos y/o archivos.
c. Permite corregir errores al retornar a un momento previo en el tiempo.
d. Registra el nombre del editor, fecha y hora de los cambios, así como aquello que fue modificado.

Pregunta 25

¿Cómo se identifican las versiones en un sistema de gestión de versiones?

Opciones:

a. Con líneas base usadas para marcar e identificar versiones aprobadas, o bien, aquellas que son particularmente importantes.
b. A partir del nombre del editor, fecha y hora de los cambios, así como de aquello que fue modificado.
c. A partir de un registro completo de cada cambio con su autoría y otros detalles.
d. Mediante etiquetas o rótulos.

Pregunta 26

¿Qué son los controles detectivos?

Opciones:

a. Son aquellos que actúan cuando ocurre un evento que afecta la disponibilidad, integridad o confidencialidad de la información.
b. Son controles que corrigen las vulnerabilidades explotadas en un incidente de seguridad.
c. Son aquellos que tratan de prevenir o evitar que se realice un evento que afecte la confidencialidad, integridad o disponibilidad de la información.
d. Son aquellos controles que regresan un sistema a un estado normal, estable y funcional, sobre todo después de que ha ocurrido un evento que afecta la integridad, disponibilidad o confidencialidad de la información.

Pregunta 27

¿Qué es una configuración insegura?

Opciones:

a. Es cuando se producen ataques a los componentes de un sistema, los cuales se originan debido a que algunos de ellos están configurados de manera segura.

b. Es cuando se producen ataques a los componentes de un sistema debido a un diseño inseguro.
c. Es cuando se producen ingresos no autorizados debido a vulnerabilidades relacionadas con el control de accesos, donde no se restringe adecuadamente el ingreso a recursos del sistema, de tal manera que se genera una exposición, modificación o eliminación de datos.
d. Es cuando se producen ataques en la capa aplicativa debido a que la aplicación no valida los datos de entrada para asegurarse de que sean del tipo y tamaño esperado, de tal manera que datos o parámetros maliciosos enviados por un atacante son interpretados o ejecutados en el servidor.

Pregunta 28

¿Qué es la detección basada en el comportamiento?

Opciones:

a. Analiza y monitorea el tráfico de una red; además, envía alertas cuando se detectan actividades sospechosas.
b. Puede detectar nuevos tipos de ataques.
c. Se basa en registros o bases de datos de ataques previos para identificar intentos de intrusión.
d. Utiliza una línea base para identificar actividades sospechosas al compararlas con aquellas que se esperan del comportamiento normal del sistema.

Pregunta 29

¿Qué es la generación de *logs*?

Opciones:

a. Registran eventos del sistema, por ejemplo, cuando se inician o detienen servicios en el sistema operativo.
b. Registran eventos relacionados con accesos a recursos del sistema, así como acciones de creación, modificación y eliminación.
c. Es un registro de las actividades y de su monitoreo con el objetivo de tener trazabilidad de las acciones realizadas en un sistema; de esta manera, se pueden identificar eventos sospechosos, así como reconstruir situaciones para asignar responsabilidades en el uso del sistema.
d. Los logs se relacionan con las actividades de un firewall, por ejemplo, con el tráfico de entrada y salida, IPs y conexiones a puertos TCP.

Pregunta 30

¿Qué son los logs de seguridad?

Opciones:

a. Eventos que se registran desde una aplicación; regularmente, el desarrollador define los eventos que se van a *loguear*.
b. Registran eventos relacionados con accesos a recursos del sistema, así como acciones de creación, modificación y eliminación.
c. Logs relacionados con las actividades de un firewall, por ejemplo, con el tráfico de entrada y salida, IPs y conexiones a puertos TCP.
d. Registra eventos del sistema, como cuando se inician o detienen servicios.

Pregunta 31

¿Qué son los controles detectivos?

Opciones:

a. Cualquier evento con efecto negativo en la confidencialidad, integridad y disponibilidad en los activos de información de la organización.
b. Un evento intencional que compromete la seguridad de una red o computadora.
c. Un evento accidental que compromete la seguridad de una red o computadora.
d. Cualquier evento que afecte la disponibilidad de los sistemas de información de una organización.

Pregunta 32

¿Qué es un equipo especializado de atención a incidentes?

Opciones:

a. Un equipo con los conocimientos técnicos y experiencia para atender, de manera adecuada, un incidente de seguridad.
b. Un equipo encargado del monitoreo periódico de los sistemas de información.
c. Un equipo encargado del mantenimiento preventivo de los sistemas de información.
d. Un equipo con los conocimientos técnicos y experiencia adecuada para dar mantenimiento a los equipos.

Pregunta 33

¿Qué acción puede ayudar a mejorar el proceso de atención a incidentes?

Opciones:

a. Reducir el número de empleados en el equipo de atención a incidentes.
b. Aumentar el número de sistemas informáticos en la organización.
c. Detectar algunas áreas de oportunidad.
d. Aumentar el número de empleados en el equipo de atención a incidentes.

Pregunta 34

¿Por qué los controles que eran efectivos antes no pueden serlo hoy?

Opciones:

a. Debido a la falta de recursos tecnológicos.
b. Debido a la falta de tiempo.
c. Debido a la falta de recursos financieros.
d. Debido a que los ataques informáticos también evolucionan.

Pregunta 35

¿Por qué es importante tener un plan de atención de incidentes?

Opciones:

a. Para vender más.
b. Para reducir el número de incidentes que se puede generar en un año.
c. Para reducir la exposición a los ataques informáticos.
d. Para mitigar el impacto que un incidente puede causar, así como para recuperar el estado funcional y normal de un sistema después de un ataque exitoso.

Pregunta 36

¿Cuándo es el momento más adecuado para llevar a cabo las actividades y secuencias de recuperación?

Opciones:

a. Cuando se produce un incidente deliberado.
b. Cuando los sistemas de información no tienen la capacidad de soportar los procesos críticos del negocio.
c. Cuando se detecta cualquier incidente de seguridad.
d. Cuando se produce un incidente que no afecta los procesos críticos del negocio.

Pregunta 37

¿Qué documentos puede incluir un plan de recuperación de desastres?

Opciones:

a. Puede incluir un resumen ejecutivo que mencione detenidamente el objetivo y alcance del plan, estrategias no específicas, guías técnicas para el personal administrativo, así como listas no específicas para el equipo encargado de coordinar la ejecución del plan.
b. Puede incluir un resumen ejecutivo que mencione detenidamente el objetivo y alcance del plan, estrategias para áreas no específicas, guías técnicas para el personal administrativo, así como listas de verificación para el equipo encargado de coordinar la ejecución del plan.
c. Puede incluir un resumen ejecutivo que mencione detenidamente el objetivo y alcance del plan, estrategias para áreas específicas, guías técnicas para el personal de tecnología, así como listas de verificación para el equipo encargado de coordinar la ejecución del plan.
d. Puede incluir un resumen ejecutivo que mencione detenidamente el objetivo y alcance del plan, estrategias para áreas específicas, guías técnicas para el personal no técnico, así como listas de verificación para el personal de la empresa en general.

Pregunta 38

¿Por qué es importante realizar pruebas periódicas del DRP?

Opciones:

a. Porque los incidentes solo afectan a las empresas con información valiosa.
b. Porque los incidentes solo afectan a las empresas sin medidas de seguridad adecuadas.
c. Porque los incidentes solo afectan a las grandes empresas.
d. Porque la operación y las tecnologías cambian constantemente, así que es necesario mantener el DRP actualizado para cuando ocurra un cambio importante.

Pregunta 39

¿Cómo se puede identificar adecuadamente el RTO?

Opciones:

a. El RTO se puede identificar adecuadamente mediante esta pregunta: ¿cuánto tiempo puedo operar o llevar a cabo esta función de negocio en lo que cambio de sistema informático?
b. El RTO se puede identificar adecuadamente mediante esta pregunta: ¿cuánto tiempo puedo operar o llevar a cabo esta función de negocio sin el sistema informático afectado?
c. El RTO se puede identificar adecuadamente mediante esta pregunta: ¿cuánto tiempo puedo operar o llevar a cabo esta función de negocio sin importar si el sistema informático está afectado?
d. El RTO se puede identificar adecuadamente mediante esta pregunta: ¿cuánta información está dispuesta a perder la organización si el sistema informático se ve afectado?

Pregunta 40

¿Cuál es la finalidad del plan de continuidad del negocio (BCP)?

Opciones:

a. La finalidad del BCP es lograr que la organización lleve a cabo sus actividades, aun con recursos informáticos limitados.
b. La finalidad del BCP es prevenir cualquier contingencia.
c. La finalidad del BCP es garantizar que la organización cuente con recursos informáticos suficientes.
d. La finalidad del BCP es garantizar que la organización cuente con recursos informáticos de alta calidad.