Examen para IDC04

Intento 1.

Pregunta 1

¿En caso de ausencia de procedimientos de actuación, qué suele ocurrir en los momentos iniciales de afectación por un incidente?:

a. Se levantan inmediatamente todos los escudos antimalware.
b. Se cortan súbitamente las comunicaciones LAN/WAN.
c. Por lo general hay un cierto desconcierto en lo relativo a las medidas que se deben tomar.

Pregunta 2

¿Cuál de las siguientes cuestiones no es un criterio para la toma de decisión en relación con la contención de un incidente?:

a. Daño potencial a la organización.
b. Tiempo de espera online.
c. Hurto de activos y detalle de su valor.
d. Premisas para preservar las evidencias, de cara a una investigación posterior.

Pregunta 3

Según el INCIBE, ¿cuándo se considera que se ha alcanzado un nivel de ciberresiliencia "Repetible"?:

a. Cuando se gestionan, actualizan y verifican los requisitos de ciberresiliencia.
b. Cuando se aplican acciones de mejora en la definición de requisitos de ciberresiliencia.
c. Cuando se han establecido requisitos de ciberresiliencia, pero no se han documentado.

Pregunta 4

¿Cuál de estas medidas de mitigación está ligada a la Filosofía Lean?:

a. Determinar las causas y los síntomas del ciberincidente para decidir la estrategia más eficaz.
b. Recuperar la última copia de seguridad limpia.
c. Identificar y eliminar todo el software utilizado por los atacantes.

Pregunta 5

La distribución Linux más popular en el área del Hacking Ético es:

a. SUSE.
b. Ninguna de las anteriores.
c. Red Hat.
d. Fedora.

Pregunta 6

¿A qué se debe principalmente la repetición de ataques anteriores?:

a. A no documentar adecuadamente la causa y el coste del incidente.
b. A no aplicar medidas preventivas.
c. A no actualizar las medidas antimalware.

Pregunta 7

La identificación de la Causa Raíz suele suponer:

a. El 10% del trabajo de análisis.
b. El 50% del trabajo de análisis.
c. El 80% del trabajo de análisis.
d. El 75% del trabajo de análisis.

Pregunta 8

¿Cuál es la orientación principal de la política de combate de los incidentes en la actualidad?:

a. Reactiva.
b. Proactiva y Preventiva.
c. De análisis forense y lecciones aprendidas.

Pregunta 9

¿Qué se deberá detallar durante el proceso de Documentación de un Ciberincidente?:

a. Todas las anteriores.
b. El coste del incidente, por compromiso de información o por impacto en los servicios que se hayan visto afectados.
c. La causa del incidente.
d. Las medidas a tomar para prevenir futuros incidentes similares.

Pregunta 10

¿A qué se debe normalmente la reproducción a corto plazo de un incidente ya identificado y contenido?:

a. A no tomar todas las precauciones necesarias.
b. A no mantener las cuarentenas requeridas.
c. Todas las anteriores.
d. A no dotar Planes de Respuesta de Emergencia.

Intento 2.

Pregunta 1

¿Cuáles son las Medidas de Ciberseguridad que se deben implantar para prevenir y combatir los incidentes?:

a. Bastionado, alerta temprana y cuestiones preventivas.
b. Procedimientos, capacidades, flujos de decisión y mecanismos de restablecimiento.
c. Instalación de IDS, IPS, SIEM y NAS cifrado.

Pregunta 2

La mayoría de las empresas están poco preparadas para enfrentarse a los ciberataques, debido a:

a. Falta de pruebas para evaluar la capacidad real ante los ataques.
b. Falta de formación o de recursos para hacer frente a los ataques.
c. Poca preparación para detener los ataques.
d. Falta de medidas técnicas para mitigar los ataques.
e. Todas las anteriores.

Pregunta 3

¿Cuál de las siguientes cuestiones deberá estar recogida en la estrategia de ciberseguridad de una empresa?:

a. La Integración Continua del software.
b. Los umbrales de Seis Sigma.
c. Las cuestiones de Lean Manufacturing.
d. La definición y caracterización de los Niveles de Operación.

Pregunta 4

La Ciberresiliencia es:

a. La capacidad para resistir, proteger y defender el uso del ciberespacio frente a los atacantes.
b. La resistencia frente a la repetición de incidentes conocidos.
c. La resistencia informática extrema.
d. La resistencia a los incidentes recursivos.

Pregunta 5

Tras un incidente de ciberseguridad, la cuarentena es:

a. El período de tiempo establecido con medidas adicionales de monitorización.
b. La espera de 40 días antes de reactivar la funcionalidad afectada.
c. La vigilancia específica de 40 días por si se repite el incidente.
d. Las pruebas de penetración durante 40 días tras la resolución del incidente.

Pregunta 6

¿Cuál de los siguientes detalles no resulta relevante durante la reflexión tras un incidente de seguridad?:

a. Qué problemas han estado asociados a la gestión del incidente.
b. Los Planes Productivos para la siguiente etapa.
c. El análisis de las causas del problema.
d. Cómo se ha desarrollado la actividad durante la manifestación del incidente.

Pregunta 7

¿Cuáles son las principales ventajas de disponer de un SOC?:

a. Todas las anteriores.
b. El análisis de los datos con posterioridad a una incidencia.
c. El almacenamiento de datos relevantes en relación con los incidentes.
d. La centralización de la actividad de ciberseguridad de la empresa.

Pregunta 8

Estadísticamente hablando, ¿cuáles son los ataques más frecuentes?:

a. Los que se efectúan utilizando brechas de los sistemas.
b. Los que instalan un troyano que pasa desapercibido mucho tiempo.
c. Los que se efectúan a través de servicios legítimos.

Pregunta 9

¿A qué metodología pertenece la Creación de Políticas de Lecciones Aprendidas?:

a. Agile.
b. Lean Manufacturing.
c. ITIL.
d. Seis Sigma.
e. PMI.

Pregunta 10

¿Qué organismo edita la publicación "Plan de Contingencia y Continuidad de Negocio"?:

a. El CCN.
b. El CNI.
c. El INCIBE.
d. El CSIRT.

Intento 3.

Pregunta 1

La clave de las Lecciones Aprendidas es:

a. La Ciber-Resiliencia de la organización.
b. La calidad de las evidencias recopiladas.
c. La precisión del análisis del incidente.
d. La documentación del incidente.

Pregunta 2

¿Qué es fundamental a la hora de diseñar un flujo de toma de decisión y escalado de incidentes?:

a. La Metodología Agile.
b. La Metodología PMI.
c. La adhesión a las comunidades del ámbito de la ciberseguridad.
d. La Excelencia Operativa.

Pregunta 3

¿Qué resulta clave durante la fase de recuperación tras un incidente?:

a. No precipitarse en la puesta en producción de sistemas que se hayan visto implicados en ciberincidentes.
b. Devolver el nivel de operación a su estado normal.
c. Que las áreas de negocio afectadas puedan retomar su actividad cuanto antes.

Pregunta 4

Ante la proliferación masiva de incidentes de Ciberseguridad, se deben efectuar:

a. Labores de registro y documentación de las lecciones aprendidas.
b. Todas las anteriores.
c. Labores preventivas, para protegerse frente a esta plaga.
d. Labores operativas en caso de la manifestación de un incidente.

Pregunta 5

¿Qué compañía desarrolla y mantiene la distro de hacking ético Kali Linux?:

a. Offensive Security.
b. Elastic Enterprise.
c. Kaspersky Lab.
d. McAfee.
e. Norton.