

Examen para IDC05.

Intento 1.

Pregunta 1

Un ciberincidente sin respuesta se cerrará tras:

Seleccione una:

- a. 10 días.
- b. Un número de días que depende de su nivel de peligrosidad o impacto.
- c. 20 días.
- d. 15 días.

Pregunta 2

Si un incidente afecta a una infraestructura crítica, se debe notificar a:

Seleccione una:

- a. INCIBE-CERT.
- b. CNPIC.
- c. ESP-DEF-CERT.
- d. CCN-CERT.

Pregunta 3

¿Qué Nivel de Peligrosidad tiene la "Ingeniería Social"?

Seleccione una:

- a. Crítico.
- b. Bajo.
- c. Medio.
- d. Alto.
- e. Muy Alto.

Pregunta 4

¿Qué Nivel de Peligrosidad tiene la "Intrusión o Intento de Intrusión"?

Seleccione una:

- a. Crítico.
- b. Alto.
- c. Medio.
- d. Bajo.
- e. Muy Alto.

Pregunta 5

¿Qué Nivel de Peligrosidad tiene la "Denegación de Servicio Distribuida"?

Seleccione una:

- a. Crítico.
- b. Bajo.
- c. Medio.
- d. Muy Alto.
- e. Alto.

Pregunta 6

¿Cómo se actúa cuando un determinado suceso puede asociarse a más de un tipo de incidente contenido en la Tabla de Clasificación?:

Seleccione una:

- a. Se asociará a aquel tipo que tenga un Nivel de peligrosidad superior, de acuerdo con los criterios correspondientes.
- b. Se recopilará más información y se volverá a analizar el incidente, hasta que quede suficientemente clara la categoría a la que se debe asociar.
- c. Se asociará a todos los tipos de incidentes relacionados con él.

Pregunta 7

¿Qué Nivel de Peligrosidad tiene el "Contenido Sexual o Violento"?

Seleccione una:

- a. Alto.
- b. Muy Alto.
- c. Crítico.
- d. Medio.
- e. Bajo.

Pregunta 8

¿Cuál es la misión de un Equipo de Respuesta a Incidentes de Seguridad?:

Seleccione una:

- a. Es el SOC de una empresa privada.
- b. Notificar los incidentes a las Administraciones Públicas.
- c. Recibir, revisar y responder a informes y actividad sobre incidentes de seguridad.
- d. Evaluar el impacto de un incidente sobre una empresa privada.

Pregunta 9

¿Qué Nivel de Peligrosidad tiene la "Infección por Código Dañino?"

Seleccione una:

- a. Medio.
- b. Crítico.
- c. Alto.
- d. Muy Alto.
- e. Bajo.

Pregunta 10

¿Qué contiene, entre otras cosas, el ENS?:

Seleccione una:

- a. Nada de lo anterior.
- b. Los Niveles de Impacto de los incidentes.
- c. Los Niveles de Peligrosidad de los incidentes.
- d. La relación entre Niveles de Peligrosidad y Niveles de Impacto.

Intento 2.

Pregunta 1

Para la notificación de los incidentes de ciberseguridad se utiliza como referencia:

Seleccione una:

- a. Los datos recopilados por los sistemas de alerta temprana.
- b. El Nivel de Impacto.
- c. La Taxonomía de Referencia.
- d. El Nivel de Peligrosidad.

Pregunta 2

¿Cuál de los siguientes elementos no tiene por qué estar contenido en un procedimiento de notificación de incidentes de una empresa?:

Seleccione una:

- a. Las indicaciones relativas a la apertura del incidente.
- b. Las entidades destinatarias de la información.
- c. El impacto del incidente sobre el EBITDA.
- d. Las ventanas temporales de reporte del incidente.

Pregunta 3

¿Qué Nivel de Peligrosidad tienen las "Amenazas Persistentes Avanzadas"?

Seleccione una:

- a. Alto.
- b. Medio.
- c. Bajo.
- d. Crítico.
- e. Muy Alto.

Pregunta 4

¿Qué organismo edita y mantiene la Guía Nacional de Notificación y Gestión de Ciberincidentes?:

Seleccione una:

- a. El INCIBE.
- b. El Consejo Nacional de Ciberseguridad.
- c. El Esquema Nacional de Seguridad.

Pregunta 5

¿Qué Nivel de Peligrosidad tiene el "Fraude"?

Seleccione una:

- a. Bajo.
- b. Medio.
- c. Muy Alto.
- d. Alto.
- e. Crítico.

Pregunta 6

Señalar cuál de los siguientes incidentes tiene un nivel de peligrosidad Crítico:

Seleccione una:

- a. Infección por Código Dañino.
- b. Revelación de Información.
- c. Scanning o Sniffing.
- d. Amenaza Persistente Avanzada.

Pregunta 7

¿Qué Nivel de Peligrosidad tiene el "Discurso de Odio"?

Seleccione una:

- a. Bajo.
- b. Muy Alto.
- c. Medio.
- d. Crítico.
- e. Alto.

Pregunta 8

¿Qué Nivel de Peligrosidad tiene el "Scanning o Sniffing"?

Seleccione una:

- a. Crítico.
- b. Bajo.
- c. Alto.
- d. Muy Alto.
- e. Medio.

Pregunta 9

¿Qué Nivel de Peligrosidad tiene la "Revelación de Información"?

Seleccione una:

- a. Bajo.
- b. Alto.
- c. Muy Alto.
- d. Crítico.
- e. Medio.

Pregunta 10

¿Qué Nivel de Peligrosidad tiene el "Uso No Autorizado de Recursos"?

Seleccione una:

- a. Alto.
- b. Medio.
- c. Crítico.
- d. Muy Alto.
- e. Bajo.

Intento 3.

Pregunta 1

¿Qué Nivel de Peligrosidad tiene el "Phishing"?

Seleccione una:

- a. **Alto.**
- b. Medio.
- c. Crítico.
- d. Muy Alto.
- e. Bajo.

Pregunta 2

¿Qué Nivel de Peligrosidad tiene el "Distribución y Configuración de Malware"?

Seleccione una:

- a. Alto.
- b. Medio.
- c. Crítico.
- d. **Muy Alto.**
- e. Bajo.

Pregunta 3

¿Qué Nivel de Peligrosidad tiene la "Denegación de Servicio"?

Seleccione una:

- a. Crítico.
- b. Bajo.
- c. **Medio.**
- d. Muy Alto.
- e. Alto.

Pregunta 4

El CSIRT puede considerar Cerrado un incidente si:

Seleccione una:

- a. Está resuelto y sin respuesta por parte del organismo afectado.
- b. Si es un Falso Positivo.
- c. Permanece sin Resolución y con respuesta por parte del organismo afectado.
- d. **Todos los anteriores.**

Pregunta 5

¿Qué Nivel de Peligrosidad tiene la "Spam"?

Seleccione una:

- a. Crítico.
- b. **Bajo.**
- c. Medio.
- d. Muy Alto.
- e. Alto.