Tarea online IC04.

Título de la tarea: Plan de respuesta ante Incidentes.

Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Incidentes de Ciberseguridad.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- **RA4.** Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas. .

Contenidos

1.- Desarrollar Procedimientos de Actuación Detallados para Dar Respuesta, Mitigar, Eliminar o Contener los Tipos de Incidentes.
2.- Implantar Capacidades de Ciberresiliencia.
3.- Establecer Flujos de Toma de Decisiones y Escalado Interno y/o Externo Adecuados.
4.- Tareas para Restablecer los Servicios Afectados por Incidentes.
5.- Documentación de los Incidentes.
6.- Seguimiento de Incidentes para Evitar una Situación Similar.
7.- Bibliografía.

1.- Descripción de la tarea.

Los Procedimientos de Actuación ante Incidentes

INCIBE. *Procedimiento Actuación ante Incidentes* (CC0)

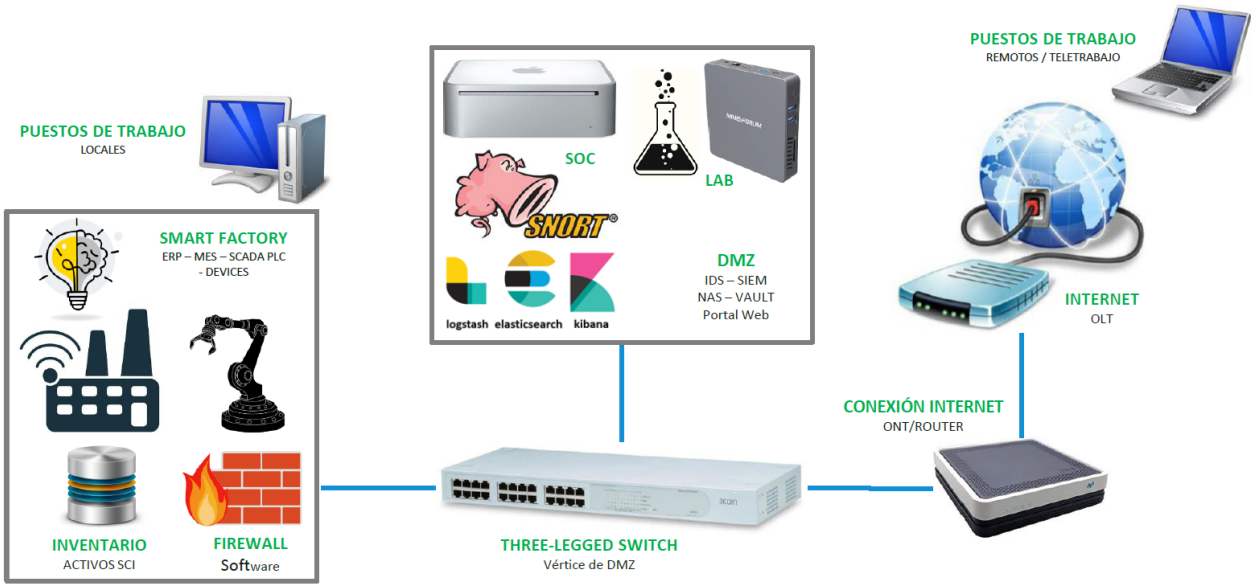
Como hemos estudiado en la Unidad 4, en los momentos iniciales de manifestación de un incidente suele existir un cierto desconcierto en lo relativo a las medidas que se deben tomar, por parte de quién y en qué orden, lo cual suele aumentar la afectación del incidente.

Este desconcierto se combate diseñando un Procedimiento de Actuación ante Incidentes. Este procedimiento suele ser de alto nivel y podrá desglosarse en tareas concretas en función del área involucrada en cada caso, o bien, en flujos de decisión y escalado para constituir la Estrategia de Contención de Incidentes de Ciberseguridad.

¿Qué te pedimos que hagas?

- **Introducción: Estructura de la Organización Empresarial.**

  Dada una empresa como la descrita en la tarea de la unidad de trabajo 1 en la que se sigue el siguiente diagrama de bloques:



Además, esta empresa sigue la siguiente estructura organizativa:

La determinación de la Estructura de la Empresa Ficticia nos permitirá identificar sus áreas de trabajo y las misiones de las mismas , con objeto de saber a qué equipos hay que involucrar en cada momento y cuándo se les debe informar acerca de los incidentes:

- CEO (Chief Executive Officer): Presidente. Gestión y Dirección administrativa.
- COO (Chief Operating Officer): Director de Operaciones.
- CFO (Chief Financial Officer): Director de Gestión Financiera.
- CMO (Chief Marketing Officer): Director de Actividades Comerciales y de Marketing.
- CIO (Chief Information Officer): Director de Sistemas de Información y Desarrollo de Aplicaciones.
- CTO (Chief Technology Officer): Director de Tecnología y Estrategia Tecnológica.
- CSO (Chief Security Officer): Responsable de Planificación y Estrategia de Seguridad.

- CISO (Chief Information Security Officer): Responsable de Ciberseguridad.
- CLO (Chief Legal Officer): Responsable del Departamento Jurídico. Es clave para la ciberseguridad.
- CDO (Chief Design Officer): Responsable de Diseño.

Con esta información proporcionada se tiene una idea general de la estructura de la empresa. El grupo de trabajadores de cada departamento y la inclusión de otros posibles departamentos queda a libre elección del alumno.

A continuación, se desglosan en apartados el desarrollo general de un Plan de Actuación ante Incidentes de Ciberseguridad. En este Plan de Actuación no se solicitan detalles a bajo nivel de herramientas a usar, solamente una **guía de actuación general.**

**Nota: Se debe realizar un único documento con los apartados, pero no en formato pregunta respuesta, sino como un documento de "Plan de Actuación ante incidentes" desarrollado para esta empresa.*

Aunque los recursos adicionales propuestos para consulta y ayuda son documentos de una extensión considerable, este documento no necesita una elevada extensión. La extensión puede estar comprendida entre 7 y 14 páginas contando portada e índice. Esta es una orientación, se pueden realizar entregas de otras extensiones.

- **Apartado 1: Manifestación y detección del incidente.**

  Deberás efectuar la siguiente tarea:

  - Describir procesos para identificación, recopilación de evidencias y evaluación inicial de incidentes.

- **Apartado 2: Definir los roles de las personas y formación del equipo de respuesta.**

  Deberás efectuar la siguiente tarea:

  - Definir que funciones tendrá asignadas cada rol definido en caso de un incidente. Llamada a filas del equipo en caso de incidente.
  - Indicar los miembros de alta prioridad a los que se les trasladará información preliminar.

- **Apartado 3: Concreción del incidente.**

  Deberás efectuar la siguiente tarea:

  - Indicar principales pasos o preguntas a realizar para detectar de forma más concreta el tipo de incidente que puede estar sucediendo.
  - Personal de empresa a los que informar.

- **Apartado 4: Medidas de actuación ante diferentes tipos de incidentes.**

  Deberás efectuar la siguiente tarea:

  - a. Descripción general de las fases de contención, mitigación, o eliminación de los incidentes.

- b. Describir de forma concreta estas fases para un tipo específico de incidente (Playbook). Los tipos a elegir son: infección por gusanos, phishing, malware en Windows, DDOS y ransomware.

- **Apartado 5: Proceso de revisión, documentación y mejora.**

  Deberás efectuar la siguiente tarea:

  - Definir el proceso de cierre de la incidencia, la documentación asociada, el aprendizaje adquirido y proceso de mejora.

  - Traslado de información a las personas o entidades necesarias.

  LOS RECURSOS PARA CONSULTA DE ESTA PRÁCTICA SE ENCUENTRAN EN LA SIGUIENTE SECCIÓN.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

Se trata de un ejercicio teórico de investigación, por lo que sólo hará falta:

- Un ordenador personal con Sistema Operativo Windows, Linux o MAC OS y un editor de textos.

Recursos opcionales

Adiocionalmente se pueden usar los siguientes recursos auxiliares:

- Plantilla traducida al español de “Respuesta a Incidentes” basada en la plantilla creada por el equipo de “Counteractive Security” bajo licencia apache 2.0. Se puede trabajar con la plantilla adaptada al español o directamente con la "Plantilla original en inglés de Counteractive Security".
  **Nota: Recurso recomendable para consulta – no entregar tal cual se genera.*
- Ejemplo de playbook: Phishing.
- Ejemplo de playbook: Malware en Windows.
- Ejemplo de playbook: Gusanos.
- Vídeo motivacional: Respuesta ante incidentes (Deloitte).
- Guía nacional de notificación y gestión de ciberincidentes.
- Ciber-resiliencia. Aproximación a un marco de medición.

Recomendaciones

- Antes de abordar la tarea:
  - lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
  - Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- No olvides elaborar el documento explicativo.

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_IC04_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna Begoña Sánchez Mañas para la cuarta unidad del MP de IC, debería nombrar esta tarea como...

sanchez_manas_begona_IC04_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicados

Criterios de evaluación RA4

- **a) Se han desarrollado procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.**
- b) Se han preparado respuestas ciberresilientes ante incidentes que permitan seguir prestando los servicios de la organización y fortaleciendo las capacidades de identificación, detección, prevención, contención, recuperación y cooperación con terceros.
- c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.
- **d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.**
- **e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de "lecciones aprendidas".**
- **f) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.**

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: Describe el mecanismo de detección de incidentes y recopilación de evidencias.	0,5 puntos (obligatorio)
Apartado 1: Define un proceso sencillo de evaluación inicial del incidente.	0,5 puntos (obligatorio)
Apartado 2: Define diferentes roles para el equipo de ciberseguridad.	0,6 puntos (obligatorio)
Apartado 2: Recoge un proceso de preparación del equipo de defensa.	0,8 puntos (obligatorio)
Apartado 2: Indica los miembros de alta prioridad que deben ser informados.	0,6 puntos (obligatorio)

Apartado 3: Describe el proceso para detectar de forma más precisa el tipo de incidente sufrido.	1 punto (obligatorio)
Apartado 3: Describe el proceso para detectar el posible alcance de la situación.	0,5 puntos (obligatorio)
Apartado 3: Indica el personal al que se le debe informar de estos nuevos progresos.	0,5 puntos (obligatorio)
Apartado 4: a. Describe las fases genéricas de actuación para contener, mitigar o eliminar incidentes.	1 punto (obligatorio)
Apartado 4: b. Define el método de actuación (playbook) ante el tipo de incidente elegido.	2 puntos (obligatorio)
Apartado 5: Define el proceso de análisis de daños ocasionados. (Lecciones aprendidas)	1 punto (obligatorio)
Apartado 5: Hace referencia al proceso de mejora en el análisis.	0,5 puntos (obligatorio)
Apartado 5: Indica a los agentes internos y externos a notificar los resultados.	0,5 puntos (obligatorio)