Tarea online IC02.

Título de la tarea: Clasificación de riesgos y potenciales 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

- **RA2.** Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad..

Contenidos

1.- Taxonomía de Incidentes de Ciberseguridad.
2.- Controles, Herramientas y Mecanismos.
    2.1.- Monitorización, Identificación, Detección y Alerta de Incidentes: Tipos y Fuentes.
    2.2.- Detección e Identificación de Incidentes de Seguridad Física.
        2.2.1.- Áreas Seguras.
        2.2.2.- Seguridad de los Equipos.
    2.3.- Monitorización, Identificación, Detección y Alerta de Incidentes a través de la Investigación en Fuentes Abiertas.
    2.4.- Herramientas OSINT.
    2.5.- Autoevaluación.
3.- Clasificación, Valoración, Documentación, Seguimiento Inicial de Incidentes de Ciberseguridad.
4.- Bibliografía.

1.- Descripción de la tarea.

Clasificación de riesgos y potenciales incidentes.

INCIBE. *Riesgo* (CC0)

Un Sistema de Gestión de Seguridad de la Información debe disponer de un correcto sistema de gestión de riesgos.

Un proceso de gestión de riesgos de seguridad de la información trata de identificar, comprender, evaluar y mitigar los riesgos.

El concepto de riesgo se corresponde con la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. El riesgo depende entonces de los siguientes factores: la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto. El producto de estos factores representa el riesgo.

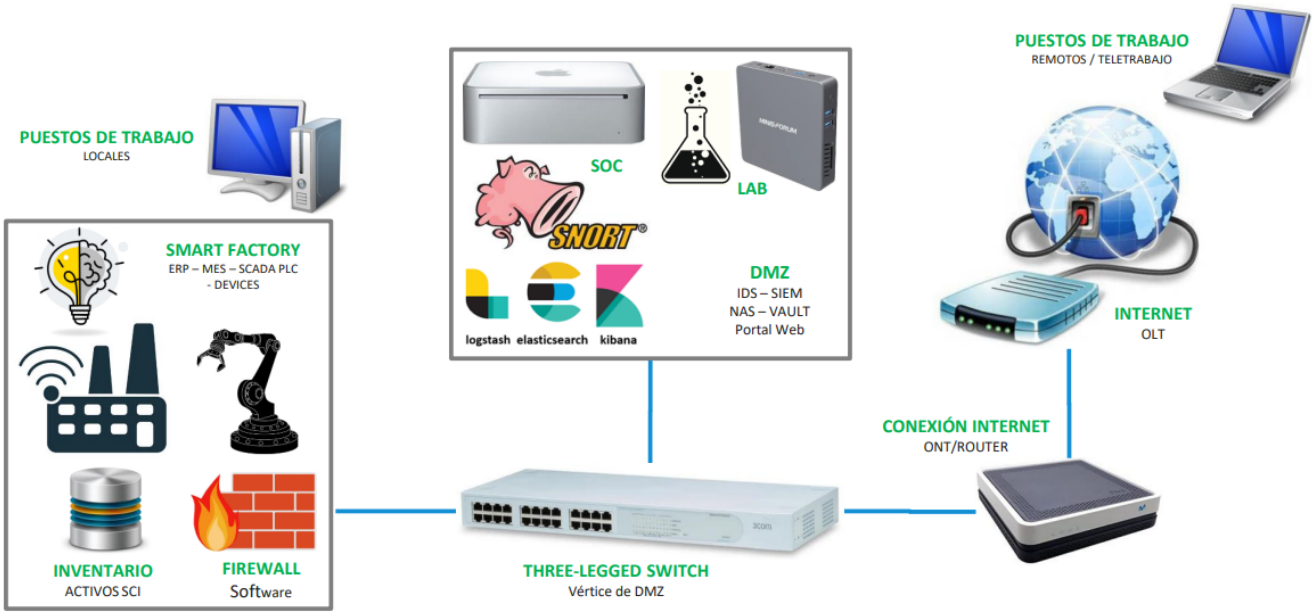
En esta tarea realizaremos un análisis y gestión de riesgos en la empresa ficticia de la unidad anterior para evitar o disminuir la probabilidad de que se produzcan diversos incidentes. Para este análisis seguiremos la metodología MAGERIT v.3 desarrollada por el gobierno español.

Además, haremos uso de la herramienta PILAR (versión Basic) que implementa la metodología MAGERIT que ha sido desarrollada por el Centro Criptológico Nacional (CCN). Este software es privativo y debe licenciarse, pero provee de una licencia de evaluación de 30 días, que es la que usaremos en este caso práctico.

¿Qué te pedimos que hagas?

- **Introducción: Diagrama de bloques y detalles de activos de la empresa.**

La empresa tiene el siguiente diagrama de bloques:



La empresa tiene los siguientes activos materiales principales:

Activo	Dirección IP	Sistema Operativo	Modelo Máquina	Función Empresa
Router	192.168.1.1	Askey SO	RTF3505VW	Router conexión Internet
Switch	192.168.1.11	3COM SO	SuperStack 3 3300XM	Three-Legged Switch
SOC	192.168.1.101	MacOS Ventura	Mac Mini M1	IDS/SIEM/NAS/VAULT
Labo_Server	192.168.1.102	Debian 11	MinisForum HM90	Servidor Laboratorio
ERP	192.168.1.25	Debian 11	ProLiant uServer Intel Xeon E	Servidor Gestor Empresarial
MES	192.168.1.24	Raspbian	Raspberry Pi 4B	Servidor Gestor Factoría
SCADA	192.168.1.23	Raspbian	Raspberry Pi 4B	Supervisión / Control / Firewall / Inventario
PLC	192.168.1.22	Raspbian	Raspberry Pi 4B	Controlador lógico
DEVICE	192.168.1.21	Raspbian	Raspberry Pi 4B	Dispositivo fabril
B.D. Inventario	192.168.1.25	MacOS Ventura	Mac Mini M1	Base de datos de Inventario
B.D. ECO/FIN	192.168.1.25	MacOS Ventura	Mac Mini M1	Base de datos ECO / FIN
Puestos trabajo	192.168.1.50-99	Windows 11 Pro	Lenovo ThinkCentre M720t	Puestos de trabajo
Maquetas, Prototipos	192.168.1.102	Debian 11	MinisForum HM90	Maquetas, prototipos, lanzaderas
Portal Web	192.168.1.102	Debian 11	MinisForum HM90	Portales web
Big Data, IA	192.168.1.50-99	Windows 11	Lenovo ThinkCentre M720t	Sistemas Big Data, IA

Nota: Todos los datos no proporcionados de la empresa deben ser definidos de forma autónoma y libre como si fueras parte de la dirección general de la empresa, justificando su elección. Por ejemplo: se puede decidir si los equipos actualmente disponen de una política de contraseñas seguras o si por el contrario no existen políticas al respecto. En cualquiera de los casos, debe exponerse en el documento de prácticas.

- **Apartado 1: Priorización y jerarquía de activos.**

Deberás efectuar la siguiente tarea:

- A partir de la lista de activos de la introducción, se deben priorizar y jerarquizar indicando los que crees que son esenciales para la empresa. Se ordenan desde el de más importancia al de menor, además se deben indicar aquellos que dependen de otros.
  De la anterior lista de activos, se debe seleccionar uno por cada uno de estos tipos indicados: activo esencial de información, activo esencial de servicio, activo de equipamiento informático y un activo de redes de comunicación.
  Con el uso de la herramienta PILAR se debe recoger la información de los cuatro activos anteriores.
  Estos activos deben definirse en su capa correcta y en un dominio de seguridad adecuado, por lo que habrá que crear los dominios de seguridad necesarios.
  Muestra la ventana detallada de información de estos cuatro activos.

- **Apartado 2: Valoración de los dominios de seguridad.**

  Deberás efectuar la siguiente tarea:

- Debes determinar el nivel de importancia que tienen los activos esenciales en sus diferentes dominios de seguridad definidos.
  Muestra una captura de pantalla con la valoración numérica de los activos en sus dominios de seguridad.
  Además, debes indicar, al menos, un par de factores atenuantes y/o agravantes por cada dominio de seguridad. Muestra una captura de estos factores.

- **Apartado 3: Determinación de las amenazas y sus salvaguardas dispuestas.**

  Deberás efectuar la siguiente tarea:

- Para cada uno de los cuatro activos seleccionados en el apartado uno, indica la lista de amenazas asociada a estos activos. Realiza una captura de cada activo con su lista de amenazas asociada.
  Además, para cada dominio de seguridad recoge las salvaguardas que te muestra la herramienta ordenadas de mayor a menor prioridad según la herramienta. Para cada una de estas salvaguardas debes indicar una acción concreta que se puede realizar para llevarla a cabo en cierto grado. Incluye también el estado actual y el estado objetivo de esta salvaguarda.
  Por último realiza una captura de pantalla en la que se ve muestren estas salvaguardas configuradas.

- **Apartado 4: Estimación del riesgo que tendría que considerar la empresa para su estudio y toma de decisiones.**

  Deberás efectuar la siguiente tarea:

- Para cada uno de los cuatro activos seleccionados en el apartado uno, indica la estimación del estado del riesgo a asumir por la empresa. Se debe indicar la estimación actual (current) y la estimación objetivo (target).
  Calcula la bajada que se produce en los riesgos en cada uno de los criterios de seguridad para cada activo.
  Además, muestra una captura de la gráfica de riesgos de tipo "Área" en la que se muestran los cuatro activos con sus valores actuales, objetivo y recomendados por PILAR.

- **Apartado 5: Taxonomía de incidentes.**

  Deberás efectuar la siguiente tarea:

- Para cada uno de los cuatro activos seleccionados en el apartado uno y tras el estudio de sus riesgos, determina un tipo de incidente que podría producirse en relación a sus riesgos. Para este tipo de incidente indica el grupo al que pertenece y realiza una pequeña explicación sobre este.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

- Se trata de un ejercicio teórico práctico, por lo que hará falta:
- Un ordenador personal con Sistema Operativo Windows y Suite Ofimática.
- Software PILAR Basic.

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_IC02_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 segunda unidad del MP de IC, debería nombrar esta tarea como...

sanchez_manas_begona_IC02_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicados

Criterios de evaluación RA2

- **a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización.**
- b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes
- c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física.
- d) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT: Open Source Intelligence).
- **d) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.**

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: Realiza una valoración correcta de los activos con su jerarquía y priorización. Define correctamente cada activo en su capa y dominio de seguridad con el uso de PILAR.	1 punto (obligatorio) 1 punto (obligatorio)
Apartado 2: Determina ambos activos esenciales en los criterios de seguridad que proceden. Define un par de factores atenuantes y/o agravantes para, al menos, dos dominios de seguridad.	1 punto (obligatorio) 1 punto (obligatorio)
Apartado 3: Muestra la lista de amenazas asociada a cada uno de los cuatro activos seleccionados. Recoge correctamente los valores solicitados de las salvaguardas para cada dominio de seguridad. Muestra una captura de pantalla con los valores configurados a las salvaguardas.	0,8 puntos (obligatorio) 1 punto (obligatorio) 0,2 puntos (obligatorio)
Apartado 4: Muestra la estimación del riesgo actual y la estimación objetivo, indicando la diferencia de valor entre sus criterios de seguridad. Refleja en un gráfico de tipo "Área" los cuatro activos con sus valores actuales, objetivo y recomendados por PILAR.	1,2 puntos (obligatorio) 0,8 puntos (obligatorio)
Apartado 5: Indica correctamente un tipo de incidente que puede producirse por cada activo y lo clasifica según la taxonomía de	2 puntos (obligatorio)

referencia.	
Redacción clara y correcta, sin errores ortográficos.	Se resta 0,1 puntos por cada error ortográfico o expresiones incorrectas.