# Tarea online IC0201.

**Título de la tarea: Clasificador Automático de 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.
    1. Monitorización, Identificación, Detección y Alerta de Incidentes: Tipos y Fuentes.
    2. Detección e Identificación de Incidentes de Seguridad Física.
        1. Áreas Seguras.
        2. Seguridad de los Equipos.
    3. Monitorización, Identificación, Detección y Alerta de Incidentes a través de la Investigación en Fuentes Abiertas.
    4. Herramientas OSINT.
    5. Autoevaluación.
3. Clasificación, Valoración, Documentación, Seguimiento Inicial de Incidentes de Ciberseguridad.
4. Bibliografía.

# 1.- Descripción de la tarea.

## El Clasificador Automático de Incidentes

Un Sistema de Alerta Temprana levanta alarmas cuando la información que recibe cualifica con alguna regla. No obstante, el hecho de cumplir con condiciones predefinidas no garantiza al 100% que el evento alertado constituya un Incidente de Ciberseguridad.

Aparte de esto, hay otra cuestión importante. Si un Sistema de Alerta Temprana detecta y notifica con celeridad un potencial incidente, pero el análisis de datos posterior se demora en exceso, se pierde la ventaja derivada de la anticipación y el posible incidente puede llegar a manifestarse en toda su dimensión y con gran impacto.

Así pues, el proceso de análisis de evidencias, alertas y datos contextuales que lleva a concluir que un evento es un incidente de seguridad es un proceso crítico que conviene automatizar, máxime cuando de él se derivan avisos, notificaciones oficiales y medidas urgentes de contención y/o mitigación (como veremos en unidades posteriores de este mismo módulo formativo).

En esta tarea haremos clasificación en la taxonomía de incidentes conocidos en diferentes empresas.

Y por último realizaremos propuestas de medidas de seguridad física de diferentes elementos de la empresa, clasificándolos, valorándolos y creando la documentación necesaria para el seguimiento de las incidencias.

Por último, se investigará con herramientas OSINT diferentes organizaciones para realizar una clasificación y valoración de incidentes de cibersegirodad.

## ¿Qué te pedimos que hagas?

- Apartado 1: Investigación de incidentes para su taxonomía.

  **Investiga incidentes ocurridos en el último año y clasifícalos en la taxonomía de ENISA indicando a qué categoría de la clasificación pertenecen y el tipo de técnica que se ha empleado.**

  - **Incluye al menos 3 incidentes.**
  - **Cada incidente debe pertenecer a una categoría diferentes.**
  - **Indica la fuente de la que has obtenido la información.**

- Apartado 2: Medidas de seguridad física y seguimiento.

  **Realiza una propuesta de medidas de seguridad física para proteger los siguientes elementos de una empresa:**

  - **Ordenadores del personal de recepción**
  - **Servidores del CPD.**
  - **Cableado de red de la sala de desarrolladores.**
  - **Impresoras**
  - **Cuadro eléctrico.**

  Indica qué riesgos cubre cada una de las medidas de seguridad propuestas.

- Apartado 3: Investigación OSINT

  **Desde la web de Shodan realiza las siguientes búsquedas:**
  - **Dispositivos que tengan abierto el puerto 3306 en España. ¿Para qué se usa habitualmente ese puerto?**
  - **Dispositivos que estén usando el protocolo RFB y cuya autenticación esté deshabilitada.**
  - **Cámaras de video conectadas a la red.**
  - **Sistemas pertenecientes a un sistema autónomo (AS) concreto.**

Recuerda que las búsquedas deben ser éticas, respetando la privacidad y los derechos de las personas y organizaciones.

# 2.- Información de interés.

## Recursos necesarios y recomendaciones

### Recursos necesarios

- **Se trata de un ejercicio teórico, por lo que sólo hará falta un ordenador personal con Sistema Operativo Windows y procesador de texto (Microsoft Word/Google Docs/LibreOffice Writer).**
- **Pueden ser necesarios recursos webs indicados en la unidad del aula virtual.**

### 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 y guardará en formato **pdf** siguiendo las siguientes pautas:

**Apellido1_Apellido2_Nombre_IC0201_Tarea.pdf**

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_IC0201_Tarea.pdf**

# 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.**
- **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*).**
- **e) 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

| | |
|---|---|
| **Presentación.** Se valorará la presentación del documento (portada, índice, bibliografía, redacción adecuada y faltas de ortografía). | 1 punto (obligatorio) |
| **Apartado 1.** Se valorará la originalidad en búsqueda de incidentes y su correcta clasificación. | 3 puntos (obligatorio) |
| **Apartado 2.** Se valorará la idoneidad de las medidas así como los riesgos que cubre. | 3 puntos (obligatorio) |
| **Apartado 3.** Se valorará la descripción paso a paso del proceso seguido para obtener toda la información solicitada. | 3 puntos (obligatorio) |

Se valorará especialmente en cada uno de los apartados:

- Que la respuesta sea personal y no copiada de internet o generada con IA. En ese caso, según la programación docente del módulo, **tendrá una calificación de 0 puntos y no se permitirá realizar un segundo envío**.
- Que sea coherente con el resto de respuestas y con la teoría de la unidad.
- Que muestre que se comprenden adecuadamente los conceptos tratados.