# INCIDENTES DE CIBERSEGURIDAD

**Horas:** 120

**Profesora:** Esperanza Micó (emico@ieseljust.com) (me.micomendez@edu.gva.es)

## COMPETENCIAS

Las competencias asociadas al módulo Incidentes de Ciberseguridad son:

- Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
- Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.
- Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.
- Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.
- Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.
- Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.
- Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

## LÍNEAS DE ACTUACIÓN

Las líneas de actuación en el proceso de enseñanza aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

– La elaboración de planes de prevención y concienciación de ciberseguridad.
– La detección de incidentes mediante distintas herramientas de monitorización.
– La implantación de las medidas necesarias para responder a los incidentes detectados.
– Identificación de la normativa nacional e internacional aplicable en la organización.
– La notificación de incidentes tanto interna como externa, si procede, mediante los procedimientos adecuados.

# CONTENIDOS

Los contenidos y estándares de aprendizaje evaluables que se consideran como “imprescindibles o básicos” se indican en la siguiente tabla.

## Contenidos básicos:

### Desarrollo de planes de prevención y concienciación en ciberseguridad:

– Principios generales en materia de ciberseguridad.
– Normativa de protección del puesto del trabajo.
– Plan de formación y concienciación en materia de ciberseguridad.
– Materiales de formación y concienciación.
– Auditorías internas de cumplimiento en materia de prevención.

### Auditoría de incidentes de ciberseguridad:

– Taxonomía de incidentes de ciberseguridad.
– Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes: tipos y fuentes
– Controles, herramientas y mecanismos de detección e identificación de incidentes de seguridad física.
– Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT).
– Clasificación, valoración, documentación, seguimiento inicial de incidentes de ciberseguridad.

### Investigación de los incidentes de ciberseguridad:

– Recopilación de evidencias.
– Análisis de evidencias.
– Investigación del incidente
– Intercambio de información del incidente con proveedores u organismos competentes.
– Medidas de contención de incidentes.

### Implementación de medidas de ciberseguridad:

– Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes.
– Implantar capacidades de ciberresiliencia.
– Establecer flujos de toma de decisiones y escalado interno y/o externo adecuados.
– Tareas para restablecer los servicios afectados por incidentes.
– Documentación
– Seguimiento de incidentes para evitar una situación similar.

### Detección y documentación de incidentes de ciberseguridad:

– Desarrollar procedimientos de actuación para la notificación de incidentes.
– Notificación interna de incidentes.
– Notificación de incidentes a quienes corresponda.

**Los contenidos a tratar en el módulo se distribuyen en las siguientes Unidades Didácticas.**

UD 0- INTRODUCCIÓN A LA CIBERSEGURIDAD

- Introducción a la ciberseguridad
- Concepto de seguridad informática
- ¿Quienes son los objetivos de los ciberatacantes?
- ¿Quienes son los atacantes?
- ¿Qué esperan obtener los ciberatacantes?
- La seguridad del IoT
- El SOC (Security Operation Center)
- Niveles de seguridad

UD1- DESARROLLO DE PLANES DE PREVENCIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD

- Introducción
- Principios generales en materia de ciberseguridad
- Normativa de protección del puesto de trabajo
- Plan de formación y concienciación en materia de ciberseguridad
- Materiales de formación y concienciación
- Auditorías de Seguridad
- Auditorías internas de cumplimiento en materia de prevención
- Ingeniería social

UD2- AUDITORÍA DE INCIDENTES DE CIBERSEGURIDAD

- Introducción
- Fases de ataque informático
- Tipos de ataque
- Taxonomia de incidentes de seguridad
- Sistemas de detección de intrusos (IDS)
- Sistemas de prevención de intrusos (IPS)
- Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes

UD3- INVESTIGACIÓN DE LOS INCIDENTES DE CIBERSEGURIDAD

- Introducción
- Recopilación de evidencias
- Análisis de evidencias
- Investigación del incidente
- Intercambio de información del incidente con proveedores u organismos competentes
- Medidas de contención de incidentes

UD4- IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

- Introducción

- Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidencia
- Implantar capacidades de ciber-resiliencia
- Establecer flujos de tomas de decisiones y escalado interno/o externo adecuados
- Tareas para restablecer los servicios afectados por incidentes
- Documentación
- Seguimiento de incidentes para evitar una situación similar

UD5- DOCUMENTACIÓN DE INCIDENTES DE CIBERSEGURIDAD

- Detección de incidentes
- Informar/denunciar
- Documentar los incidentes de seguridad
- CCN-CERT – Lucia

*Las Unidades Didácticas se adaptaran para incluir los contenidos básicos del módulo y se secuenciaran de acuerdo a las características del alumnado y a la coordinación con el resto de módulos del curso de Especialización.*

## DISTRIBUCIÓN TEMPORAL DE CONTENIDOS

Este módulo se imparte durante 4 horas semanales distribuidas a lo largo de **dos evaluaciones**.

*Se impartirán 60 horas por evaluación (aproximadamente) completando las 120 anuales establecidas.*

| *1ª evaluación* | *2ª evaluación* |
|---|---|
| *Introducción*<br>*+ UD1, UD2, UD3*<br><br>Actividad de control de mínimos: 3h | *UD3*<br>*+ UD4, UD5*<br><br>Actividad de control de mínimos: 3h |

# EVALUACIÓN

Se utilizarán las siguientes ponderaciones para obtener la calificación del período:

- ✔ Media de las calificaciones **obtenidas en las pruebas objetivas** realizadas, en las cuales el alumno demuestra la correcta asimilación de las materias impartidas, mediante exámenes, prácticas o trabajos obligatorios. Si alguna de las pruebas tuviera una valoración distinta a las demás, se indicará al alumno previamente. **(50%)**
- ✔ **Trabajos prácticos voluntarios** de ampliación de contenidos; en caso de que en la evaluación no haya trabajos prácticos voluntarios, este porcentaje se añade al apartado siguiente. **(10%)**
- ✔ La valoración del profesor sobre las **prácticas y actividades obligatorias propuestas en el aula**, desarrolladas por el alumno bien en grupo o individualmente.**(40%).**

***Para poder realizar el cálculo de la calificación final de la evaluación, se debe estar APTO (nota >=5) en el 70% de las prácticas obligatorias propuestas y en la media de las pruebas objetivas.***

**La calificación final del período será de aprobado si se obtiene una nota >= 5 sobre 10.**

**Convocatoria ordinaria**

La calificación final del módulo será la **media aritmética** obtenida en las evaluaciones parciales, siempre que se obtenga al menos 5 puntos (sobre 10) en cada una.
En el caso de que en alguna de las evaluaciones no se obtenga una calificación de 5 puntos o superior, se realizará el **examen final**.

**Si finalmente, la calificación de cada evaluación es 5 o mayor, el alumno habrá superado el módulo, recogiéndose dicha calificación en la convocatoria Ordinaria (Final).**
**En caso contrario, deberá acudir al examen de la convocatoria extraordinaria.**

**Convocatoria extraordinaria**

Los alumnos que tengan que realizar el examen de la convocatoria extraordinaria se examinarán de ***todos los contenidos teórico-prácticos del módulo.***

# RECURSOS

La plataforma que utilizaremos es **AULES** de la 'Conselleria d'Educació'

https://aules.edu.gva.es/fp