EXTRACO PROGRAMACIÓN DOCENTE

Principado de Asturias | Consejería de Educación

Centro Integrado de Formación Profesional

AVILÉS

Principado de Asturias

DEPARTAMENTO DE FAMILIA PROFESIONAL:

INFORMÁTICA Y COMUNICACIONES

CICLO FORMATIVO:

IFC401 – CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS TIC

MODULO FORMATIVO:

5021– INCIDENTES DE CIBERSEGURIDAD

DOCENTE:

JUAN CARLOS MARTINEZ FERNÁNDEZ

CURSO:

2026 – 2027

Identificación de la programación

Centro Educativo

Código	Centro	Año académico
33028684	**CIFP Avilés**	**2026/2027**

Ciclo formativo

Familia profesional	Ciclo formativo	Código	Curso
Informática y Comunicaciones	**Curso de Especialización en CIBERSEGURIDAD en ENTORNOS TIC**	**IFCE01**	**1º**
Regulación legal	- Ley Orgánica 2/2006, de 3 de mayo, de Educación. - Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la anterior. - Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo - Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la Formación Profesional.		

Módulo profesional

Código	**5021**
Nombre	**Incidentes de ciberseguridad**
Horas/curso	**180**
Horas/semana	**6**
Especialidad del profesorado	**Profesorado de Enseñanza Secundaria – Informática (0590 - 107)**

Índice

1. Resultados de aprendizaje 3

2. Contenidos y criterios 5

UT1: Introducción a la ciberseguridad 5

UT2: Prevención y concienciación en ciberseguridad. 6

UT3: Auditoría de incidentes de ciberseguridad 6

UT4: Investigación de los incidentes de ciberseguridad 7

UT5: Implementación de medidas de ciberseguridad 8

UT6: Detección y documentación de incidentes de ciberseguridad. 9

3. Evaluación 9

3.1. Criterios de evaluación 9

3.2. Procedimientos e instrumentos de evaluación 9

3.3. Criterios de calificación 11

3.4. Ponderación 13

4. Actividades de recuperación 13

4.1. Actividades de recuperación del primer cuatrimestre 13

4.2. Programas de recuperación de módulos no superados 14

5. Sistema extraordinario de evaluación para aquellos alumnos a los que, como consecuencia de sus faltas de asistencia, no se les puedan aplicar los criterios generales de evaluación ni la propia evaluación continua 14

6. Criterios de elaboración de pruebas extraordinarias 14

7. Mínimos exigibles 15

1. Resultados de aprendizaje

Los resultados de aprendizaje y los criterios de evaluación del módulo que se detallan a continuación son los mencionados en el *Real Decreto 479/2020* por el que se establece el título y las enseñanzas mínimas.

1) Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.

Criterios de evaluación:

a) Se han definido los principios generales de la organización en materia de ciberseguridad, que deben ser conocidos y apoyados por la dirección de la misma.
b) Se ha establecido una normativa de protección del puesto de trabajo.
c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.
d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.
e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.

2) Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.

Criterios de evaluación:

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).
e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.

3) Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.

Criterios de evaluación:

a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.
b) Se ha realizado un análisis de evidencias.
c) Se ha realizado la investigación de incidentes de ciberseguridad.
d) Se ha intercambiado información de incidentes, con proveedores y/u organismos competentes que podrían hacer aportaciones al respecto.
e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados.

4) Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.

Criterios de evaluación:

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.

5) Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.

Criterios de evaluación:

a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.
b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.

c) Se ha notificado el incidente de manera adecuada a las autoridades competentes en el ámbito de la gestión de incidentes de ciberseguridad en caso de ser necesario.
d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.
e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.

2. Contenidos y criterios

Los criterios de evaluación son los descritos en el apartado de anterior. Los contenidos se desarrollan en base a los dispuestos por el Real Decreto 479/2020. Se enumeran a continuación enmarcados en las unidades de trabajo que los comprenden.

UT1: Introducción a la ciberseguridad

Al tratarse de una unidad de trabajo introductoria, no se asocia exclusivamente con un resultado de aprendizaje concreto, sino que sirve de soporte para el resto de las unidades.

Criterios de evaluación

- Se ha definido la seguridad informática y definido los pilares en los que se basa.
- Se ha analizado los estándares europeos de la seguridad lógica.
- Se ha identificado los objetivos de los ciberdelincuentes
- Se ha analizado los perfiles de los ciberdelincuentes
- Se han identificado los roles del personal del centro de operaciones de seguridad (SOC)
- Se han identificado las etapas definidas en la ISO 27035.

Contenidos

- Seguridad Informática.
- Niveles en la seguridad informática
- Objetivos de los ciberdelincuentes
- Perfiles de los ciberdelincuentes
- Centro de operaciones de seguridad (SOC)
- Gestión de incidentes. ISO 27035

UT2: Prevención y concienciación en ciberseguridad.

Resultado de aprendizaje asociado**: RA1.** *Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.*

Criterios de evaluación:

a) Se han definido los principios generales de la organización en materia de ciberseguridad, que deben ser conocidos y apoyados por la dirección de la misma.
b) Se ha establecido una normativa de protección del puesto de trabajo.
c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.
d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.
e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.

Contenidos

- 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.
- Plan director de seguridad

UT3: Auditoría de incidentes de ciberseguridad

Resultado de aprendizaje asociado: **RA2.** *Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertar de seguridad.*

Criterios de evaluación:

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)
e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.

Contenidos

- 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.

UT4: Investigación de los incidentes de ciberseguridad

Resultado de aprendizaje asociado: **RA3.** *Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.*

Criterios de evaluación:

a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización
b) Se ha realizado un análisis de evidencias
c) Se ha realizado la investigación de incidentes de ciberseguridad
d) Se ha intercambiado información de incidentes con proveedores y/u organismos competentes que podrían hacer aportaciones al respecto.
e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causado.

Contenidos

- 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.

UT5: Implementación de medidas de ciberseguridad

Resultado de aprendizaje asociado: **RA4.** *Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando técnicas de protección adecuadas.*

Criterios de evaluación:

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.

Contenidos

- Cyber Kill Chain.
- Indicadores de Compromiso (IOC)
- 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 reestablecer los servicios afectados por incidentes.
  - Documentación.
  - Seguimiento de incidentes para evitar una situación similar.

UT6: Detección y documentación de incidentes de ciberseguridad.

Resultado de aprendizaje asociado: **RA5.** *Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.*

Criterios de evaluación:

a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.
b) Se ha modificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.
c) Se ha notificado el incidente de manera adecuada a las autoridades competentes en el ámbito de la gestión de incidentes de ciberseguridad en caso de ser necesario.
d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.
e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.

Contenidos

- 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
- Lecciones aprendidas

3. Evaluación

Los siguientes apartados recogen los distintos aspectos de la evaluación.

3.1. Criterios de evaluación

Son criterios de evaluación a tener en consideración todos los detallados previamente. Las capacidades personales y sociales podrán ser evaluadas como parte de otras actividades que integren los mencionados criterios.

3.2. Procedimientos e instrumentos de evaluación

Principios generales

El proceso de evaluación del aprendizaje debe atender a los siguientes puntos:

- En el desarrollo de las unidades de trabajo en que se divide el módulo, se realizará un proceso de **evaluación continua**.
- La evaluación continua, dentro de cada unidad de trabajo, se realiza valorando la participación del alumnado en la clase, los trabajos y actividades, tanto individuales como en grupo, y la resolución de ejercicios y cuestionarios que en cada caso se realicen.
- Los criterios de evaluación específicos de cada unidad de trabajo han sido mostrados previamente junto con la descripción de sus contenidos.

Métodos específicos

En cada una de las unidades de trabajo enumeradas en la programación se realizarán las siguientes actividades de evaluación:

- **Pruebas objetivas**:
  - ✓ Cuestionario tipo **test**: Se podrán realizar cuestionarios en las unidades de trabajo. La nota mínima para superar el cuestionario es de 5.
  - ✓ Pruebas **teórico-prácticas**: se podrán realizar pruebas teórico-prácticas en las unidades de trabajo, en la que se evaluará la comprensión de los diferentes conceptos y procedimientos. La nota mínima de superación de la prueba es de 5.
  - ✓ **Prácticas**: en las unidades de trabajo se podrán realizar trabajos prácticos, cuya nota mínima de superación es de 5.
- Entrega de informes de **actividades prácticas** en diferentes formatos.

Los trabajos y prácticas **deberán ser originales**, **se penalizará la copia entre el alumnado calificando con 0 puntos a cada persona implicada**, independientemente si ha copiado o se ha dejado copiar. En el caso de utilizar distintas fuentes para realizar las prácticas se deberá indicar en el informe las mismas a modo de **referencias bibliográficas**, así como el **uso de cualquier herramienta de IA** para la realización de las mismas. En caso de no hacerlo también se penalizará con una calificación de 0 puntos.

Con el fin de realizar una evaluación del alumnado lo más precisa y justa posible, y teniendo presente un carácter continuo de la evaluación, se van a utilizar los siguientes **instrumentos de evaluación**:

Procedimientos	Aspectos Considerados
Pruebas tipo test	- Conceptos - Procedimientos
Prácticas/Informes	- Conceptos - Procedimientos - Organización - Planteamiento correcto - Originalidad - Contenido
Observación sistemática del trabajo	- Capacidad organizativa - Comportamiento
Diálogo con el alumnado	- Conceptos - Procedimientos
Interpretación de datos	- Conceptos - Procedimientos

3.3. Criterios de calificación

Siguiendo el proceso de evaluación descrito, la calificación del alumnado para cada evaluación puede concretarse a través de la suma de tres componentes: **pruebas objetivas (30%), actividades prácticas (60%) y trabajo en el aula (10%).**

A continuación se especifica cómo se calificará cada uno de los tipos de pruebas que se realizarán a lo largo del curso:

a) **Pruebas objetivas:** Resolución de cuestionarios y pruebas individuales prácticas: Cada una de estas pruebas se valorará de 0 a 10 considerándose aprobada si el alumno obtiene una valoración igual o superior a 5.

b) **Actividades prácticas**: cada prueba se valorará de 0 a 10. Si a lo largo del periodo de evaluación se hubieran realizado varias de estas pruebas se calculará la media entre ellas, siempre y cuando el alumno haya superado los contenidos mínimos exigibles para aprobar cada una de ellas. Esta media será ponderada en función de la importancia dada a cada ejercicio.

Alternativamente, en las actividades prácticas también se utilizará la forma de calificación consistente en tres niveles de corrección:

- **No satisfactoria/presentada.** Equivale a una calificación de 0 puntos. Esto ocurre cuando no se ha procedido a la entrega de la tarea o no tiene contenido mínimo evaluable.
- **Satisfactoria.** Equivale a una calificación de 7 puntos. Se califica como tal cuando la tarea cumple unos mínimos, pero contiene fallos que suponen no llegar al máximo.
- **Supera lo esperado**. Equivale a una calificación de 10 puntos. Si la tarea cumple con todo lo pedido y además añade elementos que la enriquecen.

c) **Trabajo en el aula:** se valorarán las aportaciones realizadas en el aula, la actitud de trabajo y colaboración con los compañeros, cuestionarios gamificados que se realicen durante las clases, participación en los foros que se dispondrán en el Teams/aula virtual, etc.

Las entregas han de realizarse en el plazo marcado por el profesor para ello. **No se permite la entrega fuera de plazo**. En este caso, la puntuación de la práctica será de 0 puntos.

Para el alumnado que no supere el módulo profesional en la evaluación final ordinaria se realizará una **evaluación final extraordinaria**. Durante el periodo comprendido entre ambas evaluaciones finales se desarrollarán las actividades de refuerzo destinadas a superar el módulo en la evaluación extraordinaria. La docencia impartida entre la evaluación ordinaria y la extraordinaria estará dedicada a que el alumnado que no haya superado el módulo en la evaluación final ordinaria pueda afianzar sus conocimientos y afrontar con garantías de éxito la prueba o pruebas de la evaluación final extraordinaria.

3.4. Ponderación

UT	Ponderación
UT 1: Introducción a la ciberseguridad	5%
UT 2: Prevención y concienciación en ciberseguridad	15%
UT 3: Auditoría de incidentes de ciberseguridad	25%
UT 4: Investigación de los incidentes de ciberseguridad	20%
UT 5: Implementación de medidas de ciberseguridad	20%
UT 6: Detección y documentación de incidentes de ciberseguridad	15%

4. Actividades de recuperación

Los siguientes apartados detallan los distintos tipos de actividades de recuperación.

4.1. Actividades de recuperación del primer cuatrimestre

Este punto se refiere a las actividades que realizará el alumnado que obtenga calificación negativa en la evaluación parcial intermedia de febrero.

Al tratarse de un sistema de evaluación totalmente continua, en el cual al final del curso se emplean todos los contenidos que se han ido desarrollando durante el curso, no es necesaria la realización de actividades específicas de recuperación tras el primer cuatrimestre. El alumnado tendrá la oportunidad de recuperar en la segunda evaluación todas las evaluaciones con calificación negativa por medio de:

- Repetición de todas las pruebas objetivas con calificación negativa
- Realización de las prácticas no superadas

4.2. Programas de recuperación de módulos no superados

El alumnado que no haya superado el módulo a través del procedimiento de evaluación continua, ni mediante la prueba de recuperación anterior a la sesión de evaluación ordinaria, podrá recuperarlo en una o varias pruebas teórico-prácticas a desarrollar con anterioridad a la sesión de evaluación extraordinaria.

5. Sistema extraordinario de evaluación para aquellos alumnos a los que, como consecuencia de sus faltas de asistencia, no se les puedan aplicar los criterios generales de evaluación ni la propia evaluación continua

Para la planificación de este sistema extraordinario se siguen las directrices establecidas en el Proyecto Curricular de Ciclo Formativo.

Al alumnado a quien no se pueda aplicar los criterios de evaluación continua a causa de un elevado número de faltas de asistencia se les realizará **a final de cada evaluación** (febrero y junio) una **prueba extraordinaria** de evaluación teórico-práctica.

En dicha prueba se incluirán:

- cuestionarios de tipo test
- preguntas teóricas
- actividades prácticas

Así mismo, se deberán entregar todas las prácticas propuestas a lo largo del módulo, que se encontrarán en el Teams/aula virtual.

6. Criterios de elaboración de pruebas extraordinarias

En la prueba extraordinaria podrán incluirse ejercicios y cuestiones sobre todos los contenidos de las unidades de trabajo incluidas en esta programación, además de la presentación de los trabajos exigidos con carácter general para el resto del alumnado y/o trabajos específicos para el alumnado que se presente a la prueba extraordinaria.

Los criterios de calificación de estas pruebas son los mismos que se aplican durante el curso.

En las pruebas extraordinarias, las cuestiones planteadas se diseñarán de forma que el 50% de ellas versen sobre contenidos mínimos, de forma que si el alumnado resuelve satisfactoriamente dichas cuestiones sobre contenidos mínimos pueda ser evaluado con un 5.

En el caso de las **pruebas extraordinarias de junio**, siempre incluirá, **al menos**:

- Examen tipo test.
- Presentación y defensa de las prácticas asociadas del módulo.

7. Mínimos exigibles

Son mínimos exigibles todos los criterios de evaluación detallados en esta programación.