PROGRAMACIÓN DOCENTE

Principado de Asturias | Consejería de Educación

CIFP

Centro Integrado de Formación Profesional

AVILÉS

Principado de Asturias

DEPARTAMENTO DE FAMILIA PROFESIONAL:

INFORMÁTICA Y COMUNICACIONES

CICLO FORMATIVO:

IFC401 – CURSO DE EXPERTO EN CIBERSEGURIDAD EN ENTORNOS TIC

MODULO FORMATIVO:

5026 – NORMATIVA DE CIBERSEGURIDAD

DOCENTE:

LUIS MIGUEL LESTÓN LÓPEZ
CLAUDIA DE BENITO RIMADA

Índice de contenidos

ÍNDICE

Índice de contenidos 2

1. Introducción 3

2. Contenidos y criterios de evaluación 3

3. Evaluación 5

3.1. Criterios de evaluación 5

3.2. Procedimientos e instrumentos de evaluación 5

3.3. Criterios de calificación y ponderación 6

4. Actividades de recuperación 7

5. Procedimiento extraordinario de evaluación en caso de absentismo escolar 7

6. Criterios de elaboración de pruebas extraordinarias 7

1. Introducción

El presente documento muestra el extracto de la programación docente correspondiente al módulo Normativa de Ciberseguridad (5026) del curso de experto en ciberseguridad en entornos TIC.

2. Contenidos y criterios de evaluación

RA 1: Identifica los puntos principales de aplicación para asegurar el cumplimiento normativo reconociendo funciones y responsabilidades.

- Criterios de evaluación:

a. Se han identificado las bases del cumplimiento normativo a tener en cuenta en las organizaciones.
b. Se han descrito y aplicado los principios de un buen gobierno y su relación con la ética profesional.
c. Se han definido las políticas y procedimientos, así como la estructura organizativa que establezca la cultura del cumplimiento normativo dentro de las organizaciones.
d. Se han descrito las funciones o competencias del responsable del cumplimiento normativo dentro de las organizaciones.
e. Se han establecido las relaciones con terceros para un correcto cumplimiento normativo.

RA 2: Diseña sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación.

- Criterios de evaluación:

a. Se han recogido las principales normativas que afectan a los diferentes tipos de organizaciones.
b. Se han establecido las recomendaciones válidas para diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 19.600 entre otras).
c. Se han realizado análisis y evaluaciones de los riesgos de diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 31.000 entre otras).
d. Se ha documentado el sistema de cumplimiento normativo diseñado.

RA 3: Relaciona la normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos, recopilando y aplicando las normas vigentes.

- Criterios de evaluación:

a. Se han identificado los riesgos penales aplicables a diferentes organizaciones.
b. Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados.
c. Se ha establecido un sistema de gestión de cumplimiento normativo penal de acuerdo con la legislación y normativa vigente (Código Penal y UNE 19.601, entre otros).
d. Se han determinado los principios básicos dentro de las organizaciones para combatir el soborno y promover una cultura empresarial ética de acuerdo con la legislación y normativa vigente (ISO 37.001 entre otros).

RA 4: Aplica la legislación nacional de protección de datos de carácter personal, relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia.

- Criterios de evaluación:

a. Se han reconocido las fuentes del Derecho de acuerdo con el ordenamiento jurídico en materia de protección de datos de carácter personal.
b. Se han aplicado los principios relacionados con la protección de datos de carácter personal tanto a nivel nacional como internacional.
c. Se han establecido los requisitos necesarios para afrontar la privacidad desde las bases del diseño.
d. Se han configurado las herramientas corporativas contemplando el cumplimiento normativo por defecto.
e. Se ha realizado un análisis de riesgos para el tratamiento de los derechos a la protección de datos.
f. Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados en la protección de datos.

g. Se han descrito las funciones o competencias del delegado de protección de datos dentro de las organizaciones.

RA 5: Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.

- Criterios de evaluación:

a. Se ha establecido el plan de revisiones de la normativa, jurisprudencia, notificaciones, etc. jurídicas que puedan afectar a la organización.
b. Se ha detectado nueva normativa consultando las bases de datos jurídicas siguiendo el plan de revisiones establecido.
c. Se ha analizado la nueva normativa para determinar si aplica a la actividad de la organización.
d. Se ha incluido en el plan de revisiones las modificaciones necesarias, sobre la nueva normativa aplicable a la organización, para un correcto cumplimiento normativo.
e. Se han determinado e implementado los controles necesarios para garantizar el correcto cumplimiento normativo de las nuevas normativas. incluidas en el plan de revisiones.

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 en el apartado 3.

3.2. Procedimientos e instrumentos de evaluación

El nivel de conocimientos del alumnado sobre las unidades temáticas se evaluará mediante prueba objetiva teórica junto con la realización de supuestos prácticos obligatorios a nivel individual.

Para superar una unidad didáctica será necesario demostrar unos conocimientos

equivalentes, cuando menos, a los contenidos mínimos enunciados en esta programación.

3.3. Criterios de calificación y ponderación

Atendiendo a los criterios y procedimientos de evaluación descritos, la obtención de la calificación para cada alumno/a en cada evaluación se realizará teniendo en cuenta la siguiente ponderación:

1. Pruebas objetivas: 50%
2. Prácticas 50%

Las pruebas objetivas, epígrafe 1, serán realizadas evaluando los conocimientos de una o varias unidades. En el caso de las prácticas, el instrumento básico de evaluación será la calidad de sus contenidos y la entrega en plazo.

Para considerar superada la evaluación ha de obtenerse una nota de 5 puntos o superior en la nota resultante de los dos epígrafes. No se hará media si el alumno/a no se presenta a alguna de las partes (epígrafes 1 y 2), o su nota es inferior a 5 en alguna de las pruebas objetivas. Aquellas unidades cuyas pruebas objetivas no sean superadas habrán de ser recuperadas.

Se considerará como aprobado la nota de evaluación del alumnado si tras aplicar las ponderaciones descritas resulta una puntuación de 5 o mayor, teniendo en cuenta las restricciones de párrafos anteriores.

4. Actividades de recuperación

El alumnado que no supere el módulo en convocatoria ordinaria deberá presentarse a la convocatoria extraordinaria de junio.

Durante ese plazo se le proporcionarán actividades que versarán sobre los aprendizajes mínimos exigibles necesarios para obtener una evaluación positiva y que no hubiera alcanzado.

5. Procedimiento extraordinario de evaluación en caso de absentismo escolar

Se aplicará lo dispuesto en la concreción curricular del centro.

6. Criterios de elaboración de pruebas extraordinarias

El alumnado que no obtenga una calificación de 5 o superior en la evaluación final ordinaria podrá optar al procedimiento extraordinario que se celebrará en junio.

Dicho procedimiento será equivalente en modo y ponderación al procedimiento ordinario dispuesto en el apartado 6.3, constando de una prueba escrita más la entrega de las actividades prácticas propuestas por el profesor