ANEXO XIII
MODELO DE PROGRAMACIÓN DE MÓDULOS PROFESIONAIS

1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
15021482	San Clemente	Santiago de Compostela	2024/2025

Ciclo formativo

Código da familia profesional	Familia profesional	Código do ciclo formativo	Ciclo formativo	Grao	Réxime
IFC	Informática e comunicacións	CE3IFC005000	Ciberseguridade en contornos das tecnoloxías da información	Ciclos formativos de grao superior	Réxime xeral-ordinario

Módulo profesional e unidades formativas de menor duración (*)

Código MP/UF	Nome	Curso	Sesións semanais	Horas anuais	Sesións anuais
MP5021	Incidentes de ciberseguridade	2024/2025	6	140	168

(*) No caso de que o módulo profesional estea organizado en unidades formativas de menor duración

Profesorado responsable

Profesorado asignado ao módulo	ISABEL GAMALLO GÓMEZ
Outro profesorado	

Estado: Pendente de supervisión departamento

2. Concreción do currículo en relación coa súa adecuación ás características do ámbito produtivo

O módulo Incidentes de Ciberseguridade forma parte do Curso de Especialización de Ciberseguridade en Contornos das Tecnoloxías da Información desenvolvido no Real Decreto 479/2020, do 7 de abril, que se toma como punto de partida da presente programación, con unha modificación respecto do número de horas do módulo establecido en 80 horas no RD e ampliado a 140 horas na nosa comunidade autónoma segundo se pode consultar en http://edu.xunta.gal/fp/ciclo/SIFC50 .

Este módulo profesional contén a formación necesaria para realizar a función de Analista de Incidentes, desenvolvese en 140horas/168 sesións e contribúe a acadar os obxectivos xerais a), b), c), d), q), r), s), t), u) y v) e as competencias a), b), k), l), m), n) ñ) do decreto curso de especialización .

O desenvolvemento curricular deste módulo profesional fíxose tomando como referencia o Centro educativo IES San Clemente que cumpre as condicións establecidas pola lexislación vixente en canto a espazos, instalacións, alumnado...
O IES San Clemente, está na cidade de Santiago de Compostela. Este módulo de está contextualizado para a contorna do centro., na que se atopan varias empresas de servizos informáticos, moitas delas dependentes das Administracións Públicas (Xunta, Concello e Universidade) onde é previsible que poidan desenvolver a súa carreira profesional.

3. Relación de unidades didácticas que a integran, que contribuirán ao desenvolvemento do módulo profesional, xunto coa secuencia e o tempo asignado para o desenvolvemento de cada unha

U.D.	Título	Descrición	Duración (sesións)	Peso (%)
1	Plans de prevención e concienciación en ciberseguridade	Conceptos básicos da resposta a incidentes: ciclo de vida, equipos, plans de resposta a incidentes, plans de formación e concienciación.	36	20
2	Auditoria de incidentes de ciberseguridade	Monitorización e detección de incidentes. Taxonomía e seguimento inicial.	48	25
3	Investigación dos incidentes de ciberseguridade	Análise de evidencias e intercambio de información con organismos competentes.	36	20
4	Implementación de medidas de ciberseguridade	Procedementos de actuación detallados, flulxos de toma de decisións, respostas ciberesilientes.	36	20
5	Detección e documentación de incidentes de ciberseguridade	Documentación e informes de incidentes, leccións aprendidas.	12	15

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Plans de prevención e concienciación en ciberseguridade	36

4.1.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA1 - Desenvolve plans de prevención e concienciación en ciberseguridade, e establece normas e medidas de protección	SI

4.1.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA1.1 Definíronse os principios xerais da organización en materia de ciberseguridade, que deben ser coñecidos e apoiados por esta
CA1.2 Estableceuse unha normativa de protección do posto de traballo
CA1.3 Definiuse un plan de concienciación de ciberseguridade dirixido aos/ás empregados/as
CA1.4 Desenvolveuse o material necesario para levar a cabo as accións de concienciación dirixidas aos/ás empregados/as
CA1.5 Realizouse unha auditoría para verificar o cumprimento do plan de prevención e concienciación da organización

4.1.e) Contidos

Contidos
Principios xerais en materia de ciberseguridade. Normativa de protección do posto do traballo. Plan de formación e concienciación en materia de ciberseguridade. Materiais de formación e concienciación.

Contidos
Auditorías internas de cumprimento en materia de prevención.

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Auditoria de incidentes de ciberseguridade	48

4.2.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA2 - Analiza incidentes de ciberseguridade utilizando ferramentas, mecanismos de detección e alertas de seguridade	SI

4.2.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA2.1 Clasificouse e definiuse a taxonomía de incidentes de ciberseguridade que poden afectar a organización
CA2.2 Establecéronse controis, ferramentas e mecanismos de monitorización, identificación, detección e alerta de incidentes
CA2.3 Establecéronse controis e mecanismos de detección e identificación de incidentes de seguridade física
CA2.4 Establecéronse controis, ferramentas e mecanismos de monitorización, identificación, detección e alerta de incidentes a través da investigación en fontes abertas OSINT (open source intelligence)
CA2.5 Realizouse a clasificación, a valoración, a documentación e o seguimento dos incidentes detectados dentro da organización

4.2.e) Contidos

Contidos
Taxonomía de incidentes de ciberseguridade. Controis, ferramentas e mecanismos de monitorización, identificación, detección e alerta de incidentes: tipos e fontes

Contidos
Controis, ferramentas e mecanismos de detección e identificación de incidentes de seguridade física.
Controis, ferramentas e mecanismos de monitorización, identificación, detección e alerta de incidentes a través da investigación en fontes abertas (OSINT).
Clasificación, valoración, documentación, seguimento inicial de incidentes de ciberseguridade.

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Investigación dos incidentes de ciberseguridade	36

4.3.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA3 - Investiga incidentes de ciberseguridade, analiza os riscos implicados e define as posibles medidas para adoptar	SI

4.3.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA3.1 Compiláronse e almacenáronse de xeito seguro evidencias de incidentes de ciberseguridade que afectan a organización
CA3.2 Realizouse unha análise de evidencias
CA3.3 Realizouse a investigación de incidentes de ciberseguridade
CA3.4 Intercambiouse información de incidentes con provedores e/ou organismos competentes que poderían facer achegas ao respecto
CA3.5 Iniciáronse as primeiras medidas de contención dos incidentes para limitar os posibles danos causados

4.3.e) Contidos

Contidos
Compilación de evidencias.

Contidos
Análise de evidencias.
Investigación do incidente.
Intercambio de información do incidente con provedores ou organismos competentes.
Medidas de contención de incidentes.

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Implementación de medidas de ciberseguridade	36

4.4.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA4 - Pon en práctica medidas de ciberseguridade en redes e sistemas, como resposta aos incidentes detectados, aplicando as técnicas de protección adecuadas	SI

4.4.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA4.1 Desenvolvéronse procedementos de actuación detallados para dar resposta, mitigar, eliminar ou conter os tipos de incidentes de ciberseguridade máis habituais
CA4.2 Preparáronse respostas ciberresilientes ante incidentes que permitan seguir prestando os servizos da organización e fortalecendo as capacidades de identificación, detección, prevención, contención, recuperación e cooperación con terceiros
CA4.3 Estableceuse un fluxo de toma de decisións e escalado de incidentes interno e/ou externo adecuados
CA4.4 Leváronse a cabo as tarefas de restablecemento dos servizos afectados por un incidente ata confirmar a volta á normalidade
CA4.5 Documentáronse as accións realizadas e as conclusións que permitan manter un rexistro de ?leccións aprendidas?
CA4.6 Realizouse un seguimento adecuado do incidente para evitar que unha situación similar se volva repetir

4.4.e) Contidos

Contidos
Desenvolver procedementos de actuación detallados para dar resposta, mitigar, eliminar ou conter os tipos de incidentes.
Implantar capacidades de ciberresiliencia.
Establecer fluxos de toma de decisións e escalado interno e/ou externo adecuados.
Tarefas para restablecer os servizos afectados por incidentes.
Documentación.
Seguimento de incidentes para evitar unha situación similar.

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Detección e documentación de incidentes de ciberseguridade	12

4.5.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA5 - Detecta e documenta incidentes de ciberseguridade seguindo procedementos de actuación establecidos	SI

4.5.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA5.1 Desenvolveuse un procedemento de actuación detallado para a notificación de incidentes de ciberseguridade nos tempos adecuados
CA5.2 Notificóuselle adecuadamente o incidente ao persoal interno da organización responsable da toma de decisións
CA5.3 Notificóuselles adecuadamente o incidente ás autoridades competentes no ámbito da xestión de incidentes de ciberseguridade, en caso de ser necesario
CA5.4 Notificóuselles formalmente o incidente, en caso de ser necesario, ás instancias afectadas: persoal interno, clientela, provedores, etc

Criterios de avaliación
CA5.5 Notificouse o incidente aos medios de comunicación, en caso de ser necesario

4.5.e) Contidos

Contidos
Desenvolver procedementos de actuación para a notificación de incidentes.
Notificación interna de incidentes.
Notificación de incidentes a quen corresponda.

5. Mínimos exixibles para alcanzar a avaliación positiva e os criterios de cualificación

Mínimos exixibles

Os mínimos exixibles son os correspondentes aos criterios de avaliación indicados no apartado 4c desta programación. Para aprobar o módulo é necesario obter unha cualificación mínima de 5 sobre 10 en todos e cada un dos CA indicados como mínimos e que se indican a continuación:

UD1 Plans de prevención e concienciación en ciberseguridade
- Estableceuse unha normativa de protección do posto de traballo
- Definiuse un plan de concienciación de ciberseguridade dirixido aos/ás empregados/as
- Desenvolveuse o material necesario para levar a cabo as accións de concienciación dirixidas aos/ás empregados/as
- Realizouse unha auditoría para verificar o cumprimento do plan de prevención e concienciación da organización

UD2- Auditoría de incidentes de ciberseguridade
- Establecéronse controis, ferramentas e mecanismos de monitorización, identificación, detección e alerta de incidentes.
- Establecéronse controis e mecanismos de detección e identificación de incidentes de seguridade física

- Establecéronse controis, ferramentas e mecanismos de monitorización, identificación, detección e alerta de incidentes a través da investigación en fontes abertas OSINT (Open Source Intelligence)
- Realizouse a clasificación, a valoración, a documentación e o seguimento dos incidentes detectados dentro da organización.

UD3. Investigación dos incidentes de ciberseguridade
- Compiláronse e almacenáronse de xeito seguro evidencias de incidentes de ciberseguridade que afectan a organización,
- Realizouse unha análise de evidencias.
- Realizouse a investigación de incidentes de ciberseguridade.
- Iniciáronse as primeiras medidas de contención dos incidentes para limitar os posibles danos causados.

UD4. Implementación de medidas de seguridade
- Desenvolvéronse procedementos de actuación detallados para dar resposta, mitigar, eliminar ou conter os tipos de incidentes de ciberseguridade máis habituais.
- Prepáraronse respostas ciberresilientes ante incidentes que permitan seguir prestando os servizos da organización e fortalecendo as capacidades de identificación, detección, prevención, contención, recuperación e cooperación con terceiros.
- Estableceuse un fluxo de toma de decisións e escalado de incidentes interno e/ou externo adecuados.
- Leváronse a cabo as tarefas de restablecemento dos servizos afectados por un incidente ata confirmar a volta á normalidade,
- Documentáronse as accións realizadas e as conclusións que permitan manter un rexistro de leccións aprendidas.
- Realizouse un seguimento adecuado do incidente para evitar que unha situación similar se volva repetir.

UD5. Detección e documentación de incidentes de ciberseguridade.
- Desenvolveuse un procedemento de actuación detallado para a notificación de incidentes de ciberseguridade nos tempos adecuados
- Notificóuselle adecuadamente o incidente ao persoal interno da organización responsable da toma de decisións.
- Notificóuselles adecuadamente o incidente ás autoridades competentes no ámbito da xestión de incidentes de ciberseguridade, en caso de ser necesario.
- Notificóuselles formalmente o incidente, en caso de ser necesario, ás instancias afectadas: persoal interno, clientela, provedores, etc

Criterios de cualificación

En cada avaliación realizarase como mínimo unha proba e unha tarefa ou traballo (individual e/ou en grupo)

- Realizaráse como mínimo unha proba teórico-práctica en cada avaliación correspondente ás unidades didacticas vistas durante ese período. Para aprobar o módulo será necesario obter unha cualificación positiva (5 sobre 10) .

-Algunhas tarefas sinalaránse como especiais e obrigatorias sendo preciso obter unha nota de 5 sobre 10 para aprobalas. En cada unha delas indicaráse a porcentaxe sobre a nota da avaliación que corresponda, sendo ésta, na maior parte dos casos o 10% da nota de avaliación.

No caso do alumnado que non supere a proba de avaliación ou traballo, a puntuación máxima que poderá asignarse será de catro puntos

A nota final do módulo será a media ponderada das notas das probas e tarefas, sendo necesario que todas teñan unha nota igual ou superior a 5 sobre 10, e que esta media sexa igual ou superior a 5/10 para aprobar o módulo.

Calquera modificación sobre a forma de avaliar que supoña unha adaptación e mellora no proceso de ensinanza-aprendizaxe do grupo, será comunicada con antelación ao alumnado e explicada detalladamente.

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

O alumnado deberá recuperar no caso de que en algunha das unidades non alcance unha cualificación positiva (igual ou superior a 5 sobre 10).

No mes de xuño para o alumnado con partes pendentes (non superadas):
- haberá unha proba final personalizada, onde poderá recuperar aquelas partes da asignatura que teña suspensas.
- no caso de traballos non superados, asignaráse ao alumnado unha serie de tarefas para entregar.

De superar esta proba/traballos, considerarase que superou o módulo.
No caso de non superar esta proba/traballos, considerase que non superou a asignatura.

Para aquel alumnado que supere o módulo nesta proba/traballos, a nota final será o promedio das notas das avaliacións xunto coa nota da proba final. Para o alumnado que non superou o módulo, a nota final reflictirá a nota da proba final. Nesta situación non se calculan medias coas notas recibidas en partes superadas

6.b) Procedemento para definir a proba de avaliación extraordinaria para o alumnado con perda de dereito a avaliación continua

Non aplica

7. Procedemento sobre o seguimento da programación e a avaliación da propia práctica docente

Esta programación irase adaptando e reaxustando ao longo do curso.
O departamento realizará un seguimento de cada módulo. e o profesorado do ciclo, coordinado por o titor proporá os cambios e axustes oportunos.
Realizaranse enquisas de cara a coñecer a opinión do alumando con respecto ao desenvolvimento do módulo.
Empregaráse a aplicación web de seguimento de programacións www.edu.xunta.gal/programacions..

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

Realizase unha sesión de avaliación inicial conxunta do equipo docente.
Como resultado desta avaliación e se fose necesario poránse as medidas de atención á diversidade que o alumnado precise.
Esta avaliación non implica unha cualificación para o alumnado.

8.b) Medidas de reforzo educativo para o alumnado que non responda globalmente aos obxectivos programados

Para o alumnado con dificultades realizaránse os cambios na metodoloxía e temporalidade axeitados para que o alumnado poida acadar os obxectivos do módulo.

9. Aspectos transversais

9.a) Programación da educación en valores

Nas actividades propostas a educación en valores estará presente (confidencialidade da información, respecto á propiedade intelectual, igualdade, medio ambiente, etc)

9.b) Actividades complementarias e extraescolares

Procuraremos charlas e talleres con profesionais do sector que poidan dar unha visión do seu traballo diario; participación en concursos e foros de ciberseguridade.