

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
MP5024	Análise forense informática	2024/2025	5	120	144

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

Profesorado responsable

Profesorado asignado ao módulo	MARIANO SÁNCHEZ MARTÍN
Outro profesorado	

Estado: Pendente de supervisión departamento

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

O desenvolvemento curricular deste módulo profesional fíxose tomando como referencia o Centro educativo IES San Clemente que cumpre as condicións establecidas pola normativa vixente en canto a espazos, instalacións, alumnado, etc.

O módulo Análise Forense Informática forma parte do Curso de Especialización de Ciberseguridade en contornos das tecnoloxías da información, que ten unha duración de 720 horas ao longo de un curso académico, que permite obter coa súa superación a correspondente certificación académica con validez en todo o territorio nacional.

O desenvolvemento curricular de este módulo ten como referencia de partida o Real Decreto 479/2020, de 7 de abril, polo que se establece o Curso de especialización en ciberseguridade en entornos das tecnoloxías da información e se fixan os aspectos básicos do currículo.

O centro atópase situado na cidade de Santiago de Compostela. Na contorna do Centro poden atoparse varias empresas de servizos informáticos onde é previsible que poidan desenvolver a súa carreira profesional nun futuro.

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	Análise forense en sistemas Windows	Análise forense en sistemas Windows	57	50
2	Análise forense en dispositivos móbiles	Análise forense en dispositivos móbiles	27	15
3	Análise forense en sistemas Linux	Análise forense en sistemas Linux	40	25
4	Análise forense en dispositivos IoT e a nube	Análise forense en dispositivos IoT e a nube	20	10

4. Por cada unidade didáctica
4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Análise forense en sistemas Windows	57

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Aplica metodoloxías de análise forense e caracteriza as fases de preservación, adquisición, análise e documentación	SI
RA5 - Documenta análises forenses elaborando informes que inclúan a normativa aplicable	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 Identifícaronse os dispositivos que cómpre analizar para garantir a preservación de evidencias
CA1.2 Utilizáronse as ferramentas e os mecanismos adecuados para a adquisición e a extracción das evidencias
CA1.3 Asegúrouse a escena e consérvouse a cadea de custodia
CA1.4 Documentouse metodicamente o proceso realizado
CA1.5 Considerouse a liña temporal das evidencias
CA1.6 Elaborouse un informe de conclusións a niveis técnico e executivo
CA1.7 Presentáronse e expuxéronse as conclusións da análise forense realizada
CA5.1 Definiuse o obxectivo do informe pericial e a súa xustificación
CA5.2 Definiuse o ámbito de aplicación do informe pericial
CA5.3 Documentáronse os antecedentes
CA5.4 Compiláronse as normas legais e os regulamentos cumpridos na análise forense realizada
CA5.5 Recolléronse os requisitos establecidos polo/a cliente/a
CA5.6 Incluíronse as conclusións e a súa xustificación

4.1.e) Contidos

Contidos
<p>Identificación dos dispositivos para analizar.</p> <p>Colleita de evidencias (traballar un escenario).</p> <p>Análise da liña de tempo (TimeStamp).</p> <p>Análise de volatilidade e extracción de información (Volatility).</p> <p>Análise de logs (ferramentas máis usadas).</p> <p>Folla de identificación: título, razón social, nome e apelidos, e sinatura.</p> <p>0Anexos.</p> <p>Índice da memoria.</p> <p>Obxecto: obxectivo do informe pericial e a súa xustificación).</p> <p>Alcance: ámbito de aplicación do informe pericial; resumo executivo para unha supervisión rápida do contido e dos resultados.</p> <p>Antecedentes: aspectos necesarios para a comprensión das alternativas estudadas e das conclusións finais.</p> <p>Normas e referencias; documentos e normas legais e regulamentos citados nos apartados.</p> <p>Definicións e abreviaturas: definicións, abreviaturas e expresións técnicas que se utilizaron ao longo do informe.</p> <p>Requisitos: bases e datos de partida establecidos polo/a cliente/a; lexislación, regulamentación e normativa aplicables.</p> <p>Análise de solucións: resumo de conclusións do informe pericial (alternativas estudadas e camiños seguidos para chegar a elas; vantaxes e inconvenientes de cada unha e solución finalmente elixida e a súa xustificación).</p>

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Análise forense en dispositivos móbiles	27

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Aplica metodoloxías de análise forense e caracteriza as fases de preservación, adquisición, análise e documentación	SI
RA2 - Realiza análises forenses en dispositivos móbiles, aplicando metodoloxías establecidas, actualizadas e recoñecidas	SI
RA5 - Documenta análises forenses elaborando informes que inclúan a normativa aplicable	SI

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

Criterios de avaliación
CA1.1 Identifícanse os dispositivos que cómpre analizar para garantir a preservación de evidencias
CA1.2 Utilizáronse as ferramentas e os mecanismos adecuados para a adquisición e a extracción das evidencias
CA1.3 Asegurouse a escena e conservouse a cadea de custodia
CA1.4 Documentouse metodicamente o proceso realizado
CA1.5 Considerouse a liña temporal das evidencias
CA1.6 Elaborouse un informe de conclusións a niveis técnico e executivo
CA1.7 Presentáronse e expuxéronse as conclusións da análise forense realizada
CA2.1 Realizouse o proceso de toma de evidencias nun dispositivo móbil
CA2.2 Extraéronse, descodificáronse e analizáronse as probas, e conservouse a cadea de custodia
CA2.3 Xeráronse informes de datos móbiles cumprindo os requisitos da industria forense de telefonía móbil
CA2.4 Presentáronse e expuxéronse a quen proceda as conclusións da análise forense realizada
CA5.1 Definiuse o obxectivo do informe pericial e a súa xustificación

Criterios de avaliación
CA5.2 Definiuse o ámbito de aplicación do informe pericial
CA5.3 Documentáronse os antecedentes
CA5.4 Compiláronse as normas legais e os regulamentos cumpridos na análise forense realizada
CA5.5 Recolléronse os requisitos establecidos polo/a cliente/a
CA5.6 Incluíronse as conclusións e a súa xustificación

4.2.e) Contidos

Contidos
<p>Identificación dos dispositivos para analizar.</p> <p>Colleita de evidencias (traballar un escenario).</p> <p>Análise da liña de tempo (TimeStamp).</p> <p>Análise de logs (ferramentas máis usadas).</p> <p>Métodos para a extracción de evidencias.</p> <p>Ferramentas de mercado máis comúns.</p> <p>Folla de identificación: título, razón social, nome e apelidos, e sinatura.</p> <p>0Anexos.</p> <p>Índice da memoria.</p> <p>Obxecto: obxectivo do informe pericial e a súa xustificación).</p> <p>Alcance: ámbito de aplicación do informe pericial; resumo executivo para unha supervisión rápida do contido e dos resultados.</p> <p>Antecedentes: aspectos necesarios para a comprensión das alternativas estudadas e das conclusións finais.</p> <p>Normas e referencias; documentos e normas legais e regulamentos citados nos apartados.</p> <p>Definicións e abreviaturas: definicións, abreviaturas e expresións técnicas que se utilizaron ao longo do informe.</p>

Contidos
Requisitos: bases e datos de partida establecidos polo/a cliente/a; lexislación, regulamentación e normativa aplicables.
Análise de solucións: resumo de conclusións do informe pericial (alternativas estudadas e camiños seguidos para chegar a elas; vantaxes e inconvenientes de cada unha e solución finalmente elixida e a súa xustificación).

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Análise forense en sistemas Linux	40

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Aplica metodoloxías de análise forense e caracteriza as fases de preservación, adquisición, análise e documentación	SI
RA5 - Documenta análises forenses elaborando informes que inclúan a normativa aplicable	SI

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

Criterios de avaliación
CA1.1 Identifícaronse os dispositivos que cómpre analizar para garantir a preservación de evidencias
CA1.2 Utilizáronse as ferramentas e os mecanismos adecuados para a adquisición e a extracción das evidencias
CA1.3 Asegurouse a escena e conservouse a cadea de custodia
CA1.4 Documentouse metodicamente o proceso realizado
CA1.5 Considerouse a liña temporal das evidencias
CA1.6 Elaborouse un informe de conclusións a niveis técnico e executivo
CA1.7 Presentáronse e expuxéronse as conclusións da análise forense realizada

Criterios de avaliación
CA5.1 Definiuse o obxectivo do informe pericial e a súa xustificación
CA5.2 Definiuse o ámbito de aplicación do informe pericial
CA5.3 Documentáronse os antecedentes
CA5.4 Compiláronse as normas legais e os regulamentos cumpridos na análise forense realizada
CA5.5 Recolléronse os requisitos establecidos polo/a cliente/a
CA5.6 Incluíronse as conclusións e a súa xustificación

4.3.e) Contidos

Contidos
<p>Identificación dos dispositivos para analizar.</p> <p>Colleita de evidencias (traballar un escenario).</p> <p>Análise da liña de tempo (TimeStamp).</p> <p>Análise de volatilidade e extracción de información (Volatility).</p> <p>Análise de logs (ferramentas máis usadas).</p> <p>Folla de identificación: título, razón social, nome e apelidos, e sinatura.</p> <p>0Anexos.</p> <p>Índice da memoria.</p> <p>Obxecto: obxectivo do informe pericial e a súa xustificación).</p> <p>Alcance: ámbito de aplicación do informe pericial; resumo executivo para unha supervisión rápida do contido e dos resultados.</p> <p>Antecedentes: aspectos necesarios para a comprensión das alternativas estudadas e das conclusións finais.</p> <p>Normas e referencias; documentos e normas legais e regulamentos citados nos apartados.</p>

Contidos
Definicións e abreviaturas: definicións, abreviaturas e expresións técnicas que se utilizaron ao longo do informe.
Requisitos: bases e datos de partida establecidos polo/a cliente/a; lexislación, regulamentación e normativa aplicables.
Análise de solucións: resumo de conclusións do informe pericial (alternativas estudadas e camiños seguidos para chegar a elas; vantaxes e inconvenientes de cada unha e solución finalmente elixida e a súa xustificación).

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Análise forense en dispositivos IoT e a nube	20

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Aplica metodoloxías de análise forense e caracteriza as fases de preservación, adquisición, análise e documentación	SI
RA3 - Realiza análises forenses en Cloude, aplicando metodoloxías establecidas, actualizadas e recoñecidas	SI
RA4 - Realiza análise forense en dispositivos do IoT, aplicando metodoloxías establecidas, actualizadas e recoñecidas	SI
RA5 - Documenta análises forenses elaborando informes que inclúan a normativa aplicable	SI

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

Criterios de avaliación
CA1.1 Identifícanse os dispositivos que cómpre analizar para garantir a preservación de evidencias
CA1.2 Utilizáronse as ferramentas e os mecanismos adecuados para a adquisición e a extracción das evidencias
CA1.3 Asegurouse a escena e conservouse a cadea de custodia
CA1.4 Documentouse metodicamente o proceso realizado
CA1.5 Considerouse a liña temporal das evidencias

Criterios de avaliación
CA1.6 Elaborouse un informe de conclusións a niveis técnico e executivo
CA1.7 Presentáronse e expuxéronse as conclusións da análise forense realizada
CA3.1 Desenvolveuse unha estratexia de análise forense en Cloude, asegurando a dispoñibilidade das capacidades e dos recursos necesarios, logo de ocorrer o accidente
CA3.2 Conseguiuse identificar as causas e o alcance do accidente, e seu impacto real causado por el
CA3.3 Realizáronse as fases da análise forense en Cloude
CA3.4 Identificáronse as características intrínsecas da nube (elasticidade, ubicuidade, abstracción, volatilidade e compartición de recursos)
CA3.5 Cumpríronse os requisitos legais en vigor: regulamento xeral de protección de datos (RXPDP) e directiva da UE sobre seguridade de redes e sistemas de información (directiva NIS), ou os que eventualmente puidesen substituílos
CA3.6 Presentáronse e expuxéronse as conclusións da análise forense realizada
CA4.1 Identificáronse os dispositivos para analizar garantindo a preservación das evidencias
CA4.2 Utilizáronse mecanismos e ferramentas adecuadas para a adquisición e a extracción de evidencias
CA4.3 Garantiuse a autenticidade, a completitude, a fiabilidade e a legalidade das evidencias extraídas
CA4.4 Realizáronse análises de evidencias de xeito manual e mediante ferramentas
CA4.5 Documentouse o proceso de maneira metódica e detallada
CA4.6 Considerouse a liña temporal das evidencias
CA4.7 Mantívose a cadea de custodia
CA4.8 Elaborouse un informe de conclusións a niveis técnico e executivo
CA4.9 Presentáronse e expuxéronse as conclusións da análise forense realizada
CA5.1 Definiuse o obxectivo do informe pericial e a súa xustificación

Criterios de avaliación

CA5.2 Definiuse o ámbito de aplicación do informe pericial

CA5.3 Documentáronse os antecedentes

CA5.4 Compiláronse as normas legais e os regulamentos cumpridos na análise forense realizada

CA5.5 Recolléronse os requisitos establecidos polo/a cliente/a

CA5.6 Incluíronse as conclusións e a súa xustificación

4.4.e) Contidos**Contidos**

Identificación dos dispositivos para analizar.

Colleita de evidencias (traballar un escenario).

Análise da liña de tempo (TimeStamp).

Análise de logs (ferramentas máis usadas).

Nube privada e nube pública ou híbrida.

Retos legais, organizativos e técnicos particulares dunha análise en Cloude.

Estratexias de análise forense en Cloude.

Fases salientables da análise forense en Cloude.

Ferramentas de análise en Cloude (Cellebrite UFEDE Cloude Analyzer, Cloude Trail, Frost, OWADE, ?).

Identificación dos dispositivos para analizar.

Adquisición e extracción das evidencias.

Análise as evidencias de xeito manual e automático.

Documentación do proceso realizado.

Establecemento da liña temporal.

Contidos

Mantemento da cadea de custodia.

Elaboración das conclusións.

Presentación e exposición das conclusións.

Folla de identificación: título, razón social, nome e apelidos, e sinatura.

0Anexos.

Índice da memoria.

Obxecto: obxectivo do informe pericial e a súa xustificación).

Alcance: ámbito de aplicación do informe pericial; resumo executivo para unha supervisión rápida do contido e dos resultados.

Antecedentes: aspectos necesarios para a comprensión das alternativas estudadas e das conclusións finais.

Normas e referencias; documentos e normas legais e regulamentos citados nos apartados.

Definicións e abreviaturas: definicións, abreviaturas e expresións técnicas que se utilizaron ao longo do informe.

Requisitos: bases e datos de partida establecidos polo/a cliente/a; lexislación, regulamentación e normativa aplicables.

Análise de solucións: resumo de conclusións do informe pericial (alternativas estudadas e camiños seguidos para chegar a elas; vantaxes e inconvenientes de cada unha e solución finalmente elixida e a súa xustificación).

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

PARA CADA AVALIACIÓN:

A cualificación final calcularase da seguinte forma:

* 1ª parte: 40% - Prácticas, traballos, presentacións, e actividades en clase.

* 2ª parte: 60% - Proba escrita final de trimestre.

* Realizarase unha proba escrita final de trimestre cuxo contido abarcará todo o trimestre e na que se deberá obter unha cualificación igual ou maior que 5 sobre 10 para aprobala.

* A proba final poderá ter que ser presentada en clase.

* Para obter unha cualificación positiva no módulo é necesario obter un mínimo de 5 puntos sobre 10 nas dúas partes.

* A cualificación final do trimestre será unha media aritmética entre as notas obtidas nas dúas partes.

* No caso do alumnado que non obteña un mínimo de 5 puntos nas dúas partes, a puntuación máxima final que poderá asignarse será de 4 puntos.

* As probas poden realizarse en ordenador empregando máquinas virtuais, na plataforma de educación (Moodle), en papel, no taller ou na elaboración e presentación dun informe forense.

PARA A AVALIACIÓN FINAL:

A efectos de superar a avaliación final consideraranse os seguintes criterios:

* A nota final será a media aritmética das dúas avaliacións.

* Para superar o módulo é preciso ter, polo menos, un 5 en cada avaliación.

* O alumnado que non teña superada algunha das avaliacións terá que recuperar a parte correspondente na avaliación final.

* No caso do alumnado que non supere todas as avaliacións, a puntuación máxima final que poderá asignarse será de 4 puntos.

* A avaliación final poderá consistir nunha proba presencial que conterà exercicios de índole práctica e teórica ou na elaboración e presentación dun proxecto final.

PARA TODAS AS AVALIACIÓNS:

Se se detecta que o alumno ou alumna copiou parcial ou totalmente nas actividades ou en calquera das partes da proba a puntuación será de 0 puntos (aparecendo coma 1 en XADE).

Un mal uso intencional do material posto a disposición do alumnado pode implicar, aparte das medidas disciplinarias que correspondan, a non superación do módulo, cualificándose neste caso coma 0 (e aparecendo coma 1 en XADE).

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

Para aqueles estudantes que non acaden os mínimos requiridos, propóranse actividades complementarias de recuperación e reforzo consistentes na realización de exercicios prácticos, teóricos e explicacións relativas ás unidades didácticas das avaliacións non superadas.

Realizarase unha proba para valorar a recuperación deses mínimos seguindo os criterios propostos para a avaliación final no punto 5. "Criterios de cualificación".

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

A perda do dereito a avaliación continua non será de aplicación ao alumnado de cursos de especialización, polo que non se pode aplicar a este módulo.

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

O departamento realizará o seguimento das programacións de cada módulo, o cal reflectirá o grao de cumprimento con respecto á programación e a xustificación razoada no caso de desviacións. A programación será revisada ao inicio de cada curso académico á vista da experiencia do curso anterior e outras circunstancias. O referido seguimento e revisión constará nas correspondentes actas do departamento ou, de ser o caso, do equipo docente do curso de especialización.

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

Ao comezo de cada curso o profesor do módulo realizará un procedemento propio a tal fin, co seguinte esquema:

- * Reunir información das circunstancias persoais de cada alumna/o (formación previa, intereses, motivacións, recursos dispoñibles, experiencias previas, expectativas, etc.) e analizar as respostas obtidas.
- * Realizar unha sesión de avaliación inicial (preceptiva) á luz da devandita información e calquera outra que xurda ao longo dese tempo.

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

Cada profesor terá en conta as necesidades educativas específicas ou, simplemente, dificultades de aprendizaxe que algún alumno do seu grupo poida ter elaborando unha programación flexible e aberta que favoreza os cambios que o profesor debe introducir para dar resposta ás diferenzas individuais en estilos de aprendizaxe, motivacións, intereses ou dificultades de aprendizaxe. As medidas para estudantes con necesidades especiais serán facilitarlle as directrices especiais dacordo cas instrucións da orientadora do centro e adaptarle a metodoloxía didáctica.

9. Aspectos transversais

9.a) Programación da educación en valores

Tendo en conta que unha das nosas metas e a formación integral dos alumnos/as, terase en conta a transversalidade dos valores. Estes concíbense como o conxunto de contidos pertencentes a campos do coñecemento moi diversos, que deben ser abordados cun enfoque interdisciplinario e que se aprecian de maneira integrada tanto nos obxectivos como nos contidos de tódolos módulos que conforman o currículo.

- * Educación ambiental: evitar proxectos empresariais non respectuosos co medio ambiente e o perigo de determinados residuos informáticos.
- * Educación moral e cívica: axustarse a lexislación todo o relacionado, por exemplo, o respecto da propiedade intelectual do software, o uso adecuado da Internet...
- * Educación para a paz e a convivencia: promoverase como principio fundamental o respecto mutuo e o respecto a regras de convivencia no día a día da aula.
- * Educación do consumidor: hai diversidade de empresas comerciais e diversidade de produtos. O consumidor ten a posibilidade de elixir de acordo a uns criterios. A posibilidade de elección entre software libre e propietario. Esixir unha documentación correcta e adecuada as empresas subministradoras. Aprendizaxe para a toma de decisións.

9.b) Actividades complementarias e extraescolares

Tendo en conta a alta especialización destas ensinanzas e que a formación recibida e as competencias adquiridas polo alumnado deberán estar intimamente ligadas aos sectores produtivos de Galicia, tentarase contar coa participación puntual, activa e directa, de persoas expertas de empresas, institucións, institutos de investigación etc., sinaladamente do contorno galego.