Programa completo de las Microcredenciales Universitarias especializadas en ciberseguridad de la Universidad de Oviedo (2025-2026)

Contenido

Introducción a la construcción de sistemas seguros y rol del CISO

- **Introducción: La ciberseguridad, hoy**
- **La labor multidisciplinar de un CISO**
  - ¿Qué es un CISO?
  - Construyendo un CISO.
  - Determinando el rol de un CISO de manera adecuada.
  - Perfiles de un CISO.
  - Fases de diseño de un programa de ciberseguridad.
  - Estructura de la seguridad de una empresa.
  - Elaboración de presupuestos para ciberseguridad.
  - Planteamiento de casos de negocio.
  - Construyendo un equipo de seguridad.
- **Especialidad en infraestructuras**
  - *Protección de perímetro*.
    - Firewalls y conceptos de red necesarios.
    - Construcción de infraestructuras seguras.
    - Monitorización de activos.
    - Captura de intrusos.
  - *Monitorización de plataforma*.
    - Monitorización en tiempo de ejecución.
    - La necesidad de una LAN de administración aislada.
    - La utilidad del *Threat Intelligence* y *Threat Hunting*.
- **Especialidad en Defensa de Aplicaciones**
  - Introducción.
  - Seguridad a nivel de requisitos.
  - Seguridad a nivel de diseño.
  - Seguridad a nivel de implementación.
  - Herramientas de *Application Security Testing*.
  - La importancia de la detección de incidentes.
- **Especialidad en Tecnologías de la Información**
  - La importancia de la protección de *endpoints* y la defensa en profundidad.
  - Fase 1: Evitando la recepción de amenazas.
  - Fase 2: Identificando y rechazando amenazas.
  - Fase 3: Técnicas de acceso seguro a la información.
  - Fase 4: Técnicas de seguridad cuando la información debe procesarse localmente.
  - Cuando todo falla: La importancia de los planes de gestión de incidencias.
- **Especialidad en *Compliance***
  - Conociendo el entorno a asegurar: Inventarios.
  - Sistemas de Gestión de la Seguridad de la Información.
  - La norma internacional ISO 27001:2022/27002:2022.
  - *Hardening* automatizado.

Fundamentos de ciberseguridad (*CCNA CyberOPS* Parte I)

- **Módulo 1. El Peligro**
- **Módulo 2. Combatientes en la guerra contra la ciberdelincuencia**
  - Examen de punto de control. Atacantes y defensores de amenazas
- **Módulo 3. Sistema operativo Windows**
- **Módulo 4. Descripción general de Linux**
  - Examen de punto de control. Sistemas operativos
- **Módulo 5. Protocolos de red**
- **Módulo 6. Protocolo de Internet (IP) y Ethernet**
- **Módulo 7. Verificación de la conectividad.**
- **Módulo 8. Protocolo de resolución de direcciones**
- **Módulo 9. Capa de transporte**
- **Módulo 10. Servicios de red**
  - Examen de punto de control. Examen del grupo, Fundamentos de la red
- **Módulo 11. Dispositivos de comunicación por redes**
- **Módulo 12. Infraestructura de seguridad de la red**
  - Examen de punto de control. Examen del grupo, Seguridad de la infraestructura de red
- **Módulo 13. Los atacantes y sus herramientas**
- **Módulo 14. Amenazas y ataques comunes**
- **Módulo 15. Monitoreo de red y sus herramientas**
- **Módulo 16. Ataque a los fundamentos**
- **Módulo 17. Atacando lo que hacemos**
  - Examen de punto de control. Tipos de ataques

Fundamentos de ciberseguridad (*CCNA CyberOPS* Parte II)

- **Módulo 18. Comprendiendo qué es defensa**
- **Módulo 19. Control de acceso**
- **Módulo 20. Inteligencia contra amenazas**
  - Examen de punto de control. Defensa de la red
- **Módulo 21. Criptografía**
- **Módulo 22. Protección de terminales**
- **Módulo 23. Evaluación de vulnerabilidades en terminales**
  - Examen de punto de control. Criptografía y protección de terminales
- **Módulo 24. Tecnologías y protocolos**
- **Módulo 25. Datos de seguridad de la red**
  - Examen de punto de control. Protocolos y archivos de registro
- **Módulo 26. Evaluación de alertas**
- **Módulo 27. Trabajo con datos de seguridad de la red**
- **Módulo 28. Análisis y respuesta de incidentes e informática forense digital**
  - Examen de punto de control. Análisis de datos de seguridad

Gestión de activos para la ciberseguridad (CyberITAM)

- **Introducción a la ciberseguridad.**
  - Concepto de ciberseguridad y su importancia en entornos corporativos.
  - Objetivos del control de infraestructura.
  - Vulnerabilidades comunes en activos TI.
  - Normativas y marcos de referencia: ENS, ISO 27001.
- **Introducción a *Proactivanet*.**
  - Acceso a la herramienta.
  - Consola de técnicos: panel inicial, alertas y eventos.
  - Recursos de ayuda.
- **Uso de *Proactivanet discovery* & gestión de activos.**
  - Consulta y explotación básica de datos: árboles, formularios.
  - Consulta de activos (PCs, servidores, dispositivos).
  - Clasificación, localización y estado de activos. Campos personalizados y registro adicional.
  - *Dashboards* y *reporting*: informes y listados.
  - Roles y perfiles de acceso.
- **Administración de la herramienta**.
  - Despliegue de agentes auditores.
  - Creación de jerarquías de localización y clasificación automática de HW y SW.
  - Control de licencias de software (SAM).
  - Operaciones masivas: asignación, eliminación, modificación de activos.
  - Importación de datos.
  - Gestión de accesos por criterios de localización y clasificación.
- **Administración de dispositivos SNMP y móviles (MDM).**
  - Inventario y reglas de tipificación de SNMP.
  - OIDs favoritos.
  - Gestión de dispositivos móviles corporativos.
  - Monitorización y Distribución de Software.
- **Monitorización del rendimiento y uso real de HW y SW.**
  - Gestión de alertas y eventos.
  - Distribución automática de software, actualizaciones y parches.
  - Configuración de repositorios y lanzamientos.
- **Seguridad de la Información con *Proactivanet*.**
  - Control de accesos a unidades compartidas y locales sensibles.
  - Auditoría de permisos.
- **Control de la Ciberseguridad desde *Proactivanet*.**
  - Detección de equipos desconocidos en red.
  - Gestión y estado de antivirus.
  - Control de firewalls, VPNs y cifrado de discos.
  - Gestión automática de actualizaciones de Windows y software de terceros.

Desarrollo seguro en entornos (*DevSecOps*)

- **Módulo 1. Introducción a DevOps y Cultura Colaborativa**
  - ¿Qué es *DevOps*/*DevSecOps*?
  - Principios de *DevOps*/*DevSecOps*
  - Beneficios y desafíos de la implementación de *DevOps*/*DevSecOps*
- **Módulo 2. Ciclo de Vida y Puesta en Producción DevOps**
  - *Ciclo de Vida DevOps*.
    - Planificación.
    - Desarrollo.
    - Integración.
    - Pruebas.
    - Despliegue.
    - Operaciones.
  - *Puesta en Producción*.
    - Estrategias de despliegue.
    - Gestión de configuraciones.
    - Orquestación de contenedores.
    - Plan de contingencia
- **Módulo 3. *DevSecOps*: Seguridad integrada en *DevSecOps***
  - Conceptos fundamentales
  - *Mejores prácticas*.
    - Planificación.
    - Desarrollo.
    - Integración.
    - Pruebas.
    - Despliegue.
    - Operaciones
  - Herramientas de seguridad automatizadas
- **Módulo 4. Otros conceptos**
  - *FinOps*, *GreenOps* y la Sostenibilidad en *DevOps*

Análisis forense digital en sistemas *Windows*, *Linux* y *Android*

- **Módulo 1. Introducción al análisis forense informático**
  - Definición y objeto del análisis forense
  - El informe pericial en el proceso judicial
  - Fases del análisis forense
- **Módulo 2: Análisis forense en sistemas Windows**
  - Adquisición y preservación de evidencias
  - Artefactos Windows
  - Análisis de dispositivos de almacenamientos: discos/pendrives
  - Análisis de memoria
- **Módulo 3: Análisis forense en sistemas Linux**
  - Adquisición y preservación de evidencias
  - Artefactos Linux
  - Análisis de dispositivos de almacenamientos: discos/pendrives
  - Análisis de memoria
- **Módulo 4: Análisis forense en dispositivos móviles Android**
  - Adquisición lógica y física
  - Artefactos Android
  - Análisis de los datos de las aplicaciones

Pentesting y seguridad ofensiva

- **Módulo 1. Introducción al *pentesting***
  - Definición y objetivos del *pentesting*.
  - Diferencias entre *pentesting*, hacking ético y auditoría de seguridad.
- **Módulo 2. *Pentesting* en aplicaciones web**
  - Fundamentos de seguridad en aplicaciones web.
  - Principios de seguridad en el desarrollo de software.
  - OWASP Top 10.
  - Análisis detallado de las vulnerabilidades más críticas.
  - WSTG (*Web Security Testing Guide*).
  - Metodología y técnicas de pruebas de seguridad.
  - Herramientas de pentesting web. Introducción a herramientas como *Burp Suite*, OWASP ZAP, etc.
  - Laboratorios prácticos. Ejercicios prácticos de pentesting en aplicaciones web.
- **Módulo 3. *Pentesting* en aplicaciones móviles**
  - Fundamentos de seguridad en aplicaciones móviles.
  - Diferencias entre aplicaciones nativas, híbridas y web.
  - OWASP *Mobile Top 10*.
  - Análisis de las vulnerabilidades más comunes en aplicaciones móviles.
  - MSTG (*Mobile Security Testing Guide*). Metodología y técnicas de pruebas de seguridad en móviles.
  - Herramientas de pentesting móvil. Introducción a herramientas como MobSF, Frida, etc.
  - Laboratorios prácticos (Android). Ejercicios prácticos de pentesting en aplicaciones móviles.
- **Módulo 4. Generación de informes**
  - Estructura y contenido de un informe de *pentesting*.
  - Mejores prácticas para la presentación de resultados.

Ciberseguridad en entornos industriales y críticos

- **Módulo 1. Introducción, definiciones y normativas aplicables**
  - Introducción
  - Definiciones
  - Normativas aplicables.
- **Módulo 2. Análisis y gestión de riesgos industriales**
  - Análisis de riesgos industriales
  - Gestión de riesgos industriales.
- **Módulo 3. Auditorías en entornos industriales y riesgos inherentes a cada una de ellas**
  - Auditorías en entornos industriales
  - Riesgos inherentes a cada tipo de auditoría.
- **Módulo 4. Medidas activas, dirigidas a prevenir**
  - Inventario de activos
  - Modelado de amenazas
  - Seguridad física
  - Segmentación de la red
  - Control de accesos y privilegios
  - Monitorización activa.
- **Módulo 5. Medidas pasivas, dirigidas a mitigar impacto**
  - El ciclo de gestión de incidentes
  - Copias de seguridad
  - Simulacros y ciberejercicios
  - Equipo de respuesta y comité de crisis

Gestión y respuesta ante ciberincidentes

- **Módulo 1. Introducción a los ciberincidentes**
  - Incidencia, Incidente o Crisis.
  - Contexto histórico.
  - Taxonomía de amenazas.
  - *Kill Chain*.
  - Taxonomía de incidentes.
  - Normativas de referencia.
- **Módulo 2. Gestión de incidentes**
  - Ciclo de gestión.
  - Triaje y DFIR.
  - Tareas post-incidente.
  - Informes y presentación de resultados.
- **Módulo 3. Respuesta a incidentes**
  - Primera respuesta.
  - Contención, Erradicación y Recuperación.
  - Aspectos logísticos y organizativos.
  - Aspectos legales.
  - Plan de comunicación.
- **Módulo 4. Preparación**
  - Gobernanza de la gestión de incidentes.
  - Aspectos organizativos.
  - Inteligencia de amenazas e intercambio de información.
  - Simulacros y ciberejercicios.
- **Monitorización de seguridad.**

Implantación y verificación del ENS

- **Módulo 1. Introducción y objetivos del curso.**
  - Objetivo del curso.
  - Obtención de la conformidad con el ENS.
  - Conformidad en el perfil de requisitos esenciales.
- **Módulo 2. Fundamentos del Esquema Nacional de Seguridad (ENS).**
  - Introducción al ENS.
  - Requisitos mínimos.
  - Desarrollo del ENS.
- **Módulo 3. Plan de adecuación al ENS.**
  - Política de seguridad.
  - Categorización de los sistemas.
  - Valoración de servicios e información.
  - Declaración de aplicabilidad provisional.
  - Análisis de riesgos.
  - Declaración de aplicabilidad definitiva.
  - Perfil de cumplimiento específico.
  - Plan de mejora de la seguridad (hoja de ruta).
- **Módulo 4. Medidas de seguridad del ENS (Anexo II).**
  - Marco organizativo [org].
  - Marco operacional [op].
  - Medidas de protección [mp].
- **Módulo 5. Otras medidas de seguridad.**
  - Medidas adicionales a las del Anexo II.
- **Módulo 6. Perfil de requisitos fundamentales de seguridad (PCE Requisitos Esenciales).**
  - Introducción. ¿Qué es el PCE Requisitos Esenciales?
  - Entidades u organizaciones que pueden beneficiarse del PCE.
  - Guías para la adecuación al PCE Requisitos Esenciales.
  - La plataforma de gobernanza.
- **Módulo 7. Pasos para la adecuación al PCE Requisitos Esenciales.**
  - Diagnóstico de cumplimiento.
  - Gobierno.
  - Plan de adecuación.
  - Implantación.
  - Articulado.
  - Perfil de cumplimiento.
  - Registros de seguridad.
  - Normativa de uso de medios electrónicos.
  - Implantación de medidas.
  - Evidencias de cumplimiento.
- **Módulo 8. Proceso de verificación de la conformidad.**
  - Fase 1: Solicitud de auditoría.
  - Fase 2: Evaluación documental y de evidencias.
  - Fase 3: Expedición de la conformidad con el ENS. Ciclo de mejora continua.

Protección de datos personales y seguridad de la información

- **Módulo 1. Fundamentos normativos de la protección de datos**
  - Normativa de protección de datos.
  - Agencia Española de Protección de Datos.
- **Módulo 2. Datos personales y tratamiento**
  - Dato de carácter personal.
  - Tratamiento de datos.
  - Principios de la protección de datos.
  - Licitud en el tratamiento.
- **Módulo 3. Derechos y deberes en materia de protección de datos**
  - El deber de información.
  - Derechos de las personas.
  - Datos de menores.
- **Módulo 4. Responsabilidades y medidas organizativas**
  - Tratamientos por cuenta de terceros.
  - Medidas de seguridad.
  - El Delegado de Protección de Datos (DPD).
- **Módulo 5. Gestión de incidentes**
  - Violaciones y brechas de seguridad.

Directiva NIS2 y cumplimiento normativo en ciberseguridad

- **Módulo 1. Marco legal europeo en ciberseguridad: Directiva NIS2**
  - Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión.
  - Modificaciones normativas introducidas y derogación de la Directiva (UE) 2016/1148.
- **Módulo 2. Anteproyecto de ley español y gobernanza nacional**
  - Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.
  - Principales implicaciones jurídicas y organizativas a nivel estatal y autonómico.
- **Módulo 3. Reglamentos y anexos sectoriales de la Directiva NIS2**
  - Reglamento de ejecución y anexos aplicables a sectores específicos.
  - Obligaciones diferenciadas según el tipo de entidad y criticidad del servicio.
- **Módulo 4. Relación entre la Directiva NIS2 y el Esquema Nacional de Seguridad (ENS)**
  - Interacción normativa entre NIS2 y ENS.
  - Complementariedad y procesos comunes en planes de cumplimiento y verificación.
- **Módulo 5. Perfil de cumplimiento específico de NIS2**
  - Perfil de cumplimiento propuesto para facilitar la aplicación práctica de NIS2 en entidades públicas y privadas.

Ciberseguridad y gestión del riesgo

- **Módulo I. Procedimientos de gestión del riesgo**
  - Introducción
  - Auditoría de activos
  - Evaluación del riesgo
  - Declaración de aplicabilidad (SOA)
  - Identificación y evaluación del riesgo
  - Objetivos definidos y transparentes de las políticas de seguridad
  - Compromiso de la dirección y del personal
  - *Procedimientos*
    - Instrucciones técnicas
    - Manuales
    - Contratos de confidencialidad (NDA) con proveedores, clientes y trabajadores.
  - *Funciones*
    - Grado de responsabilidad: CISO, responsables de dirección, responsables técnicos y propietarios del activo.
- **Módulo II. Metodologías activas de control del riesgo**
  - *Control activo del riesgo*
    - Control de contraseñas, evaluación de compromiso o exposición
    - Exposición de sitios, IPs y dominios, redes sociales, accesos al entorno
    - Seguridad perimetral física y virtual
    - Teletrabajo y accesos externos (personal propio y externo).
    - Políticas de antivirus y antimalware.
    - Monitorización.
  - *Gestión y comunicación de incidentes (interna y externa)*
    - Monitorización de tráfico y control de evidencias. SIEM. SOC
    - Software: desarrollo propio, propietario, *open source*.
    - Controles y políticas de actualización.
    - *Snapshots*.
    - Correo electrónico: gestión de listas, trazabilidad, agentes externos. Autenticación y políticas (DKIM, DMARC, SPF, *Lookup*).
    - Móviles y tablets: exposición y control de dispositivos.
- **Módulo III. Normativa y recomendaciones**
  - Normativa ISO (27001, 22301, 25000)
  - Esquema Nacional de Seguridad (ENS)
  - Directiva NIS2
  - Guías de seguridad CCN-STIC
  - Instituciones activas en ciberseguridad.
- **Módulo IV. Y después**
  - Continuidad de negocio
  - Informática forense.
- **Módulo V. Herramientas de gestión del riesgo**
  - Importancia de una herramienta de gestión de riesgos
  - Requisitos funcionales y beneficios
  - Referencias de NIS2 sobre la gestión del riesgo
  - Demostración de *Trend Micro Vision One ASRM*.