



SERCA
INSTITUTO
DE ALTOS ESTUDIOS
ESPECIALIZADOS

CURSO ONLINE EN CIBERSEGURIDAD CON IA EN EL SECTOR SANITARIO: PROTECCIÓN DE DATOS CLÍNICOS



FORMACIÓN PERMANENTE



WWW.INSTITUTOSERCA.COM



Acerca de **Instituto Serca**

Instituto Serca es un centro especializado en Formación de Postgrado: Másteres, Dobles Títulos de Máster, Especialistas y Expertos Universitarios, así como Cursos Homologados por Universidades. Se caracteriza por no centrarse en la formación de expedientes, sino de personas, cuyo aprendizaje dará sentido a su experiencia.

Los Másteres, Especialistas, Expertos Universitarios y Cursos que impartimos desde Instituto SERCA, cuentan con todas las garantías y exigencias de calidad, lo que hace posible que la titulación obtenida por nuestros alumnos/as sean Títulos expedidos por prestigiosas universidades.



Metodología de Estudio

- ✓ **Campus Virtual Avanzado:** Experiencia de estudio individualizada, intuitiva e interactiva.
- ✓ **Tutorización Permanente:** Nuestro equipo docente estará a disposición del alumnado desde su matriculación hasta la finalización de todo el proceso formativo.
- ✓ **Clases en vídeo y en audio:** Cada programa formativo dispone de clases en vídeo y audios específicos por materia, para reforzar el contenido teórico.
- ✓ **Metodología E-Learning:** Modalidad 100% online adaptada a las necesidades del alumnado.
- ✓ **Evaluación:** Planteamiento de casos y actividades dirigidas a la valoración competencial del programa formativo.
- ✓ **Profesorado Especializado:** Contamos con un claustro de profesores especializado que realizará un seguimiento personalizado del aprendizaje.
- ✓ **Biblioteca Digital:** A través de nuestra innovadora plataforma digital, el alumnado podrá acceder a un amplio catálogo de libros, revistas, obras de investigación y tesis doctorales.
- ✓ **Descarga automática de certificados y actualización de notas permanente.**
- ✓ **Notificaciones en tiempo real sobre el estado y evolución del estudio.**





Campus **Virtual**

- ✓ Clases en vídeo de cada materia
- ✓ Tutorías de seguimiento en directo mensuales
- ✓ Herramientas de interacción y seguimiento: tutorización permanente, foro, emails, etc.
- ✓ Consulta directa del expediente académico
- ✓ Descarga de certificados
- ✓ ¡Y mucho más!...

Presentación del Programa

Especialízate con el Curso de Ciberseguridad con IA en el Sector Sanitario: Protección de Datos Clínicos de Instituto Serca, una formación diseñada para profesionales que desean liderar la defensa digital en uno de los sectores más sensibles y expuestos a ciberamenazas.

A lo largo del programa, abordarás desde los fundamentos de ciberseguridad aplicada al entorno clínico y el marco normativo vigente (RGPD, LOPDGDD, Directiva NIS2) hasta técnicas avanzadas de inteligencia artificial para la detección de amenazas, protección de historiales electrónicos, gestión de identidades y seguridad en dispositivos médicos conectados (IoMT).

Además, profundizarás en respuesta a incidentes, continuidad asistencial, gobernanza, auditoría y tendencias emergentes como la arquitectura Zero Trust o la IA adversarial, analizando casos reales de ciberataques a instituciones sanitarias. Al finalizar, contarás con las competencias necesarias para diseñar estrategias integrales de ciberseguridad sanitaria, potenciando un perfil profesional altamente demandado en el mercado actual.



Duración: 150 horas



Créditos: 6 Créditos ECTS



Metodología: Online



Matriculación: Permanente

Programa Académico

- ✓ Comprender los fundamentos de ciberseguridad sanitaria, identificando sus principios y particularidades sectoriales.
- ✓ Conocer el marco normativo de protección de datos clínicos, diferenciando las regulaciones aplicables.
- ✓ Analizar la arquitectura de sistemas de información sanitarios, identificando superficies de ataque y vulnerabilidades.
- ✓ Dominar los fundamentos de inteligencia artificial, relacionándolos con la detección de ciberamenazas sanitarias.
- ✓ Aplicar técnicas de cifrado y protección de datos clínicos, distinguiendo métodos según su finalidad.
- ✓ Implementar estrategias de gestión de identidades y seguridad en dispositivos médicos conectados, incorporando soluciones adaptadas.
- ✓ Elaborar planes de respuesta a incidentes, garantizando la continuidad asistencial ante ciberataques.
- ✓ Fundamentar la gobernanza de ciberseguridad sanitaria, evaluando tendencias emergentes y casos reales documentados.



1: FUNDAMENTOS DE CIBERSEGURIDAD APLICADA AL ENTORNO SANITARIO

- 1.1. Conceptos esenciales de ciberseguridad y su relevancia en el sector salud
- 1.2. Evolución histórica de las amenazas cibernéticas en organizaciones sanitarias
- 1.3. Principios de la tríada CIA (confidencialidad, integridad y disponibilidad) en datos clínicos
- 1.4. Ecosistema digital sanitario: actores, infraestructuras y flujos de información clínica
- 1.5. Diferencias entre la ciberseguridad genérica y la ciberseguridad específica del sector salud
- 1.6. Cultura organizacional de seguridad y concienciación del personal sanitario

2: MARCO NORMATIVO Y REGULATORIO DE LA PROTECCIÓN DE DATOS CLÍNICOS

- 2.1. Reglamento General de Protección de Datos (RGPD) aplicado al ámbito sanitario
- 2.2. Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)
- 2.3. Normativa sectorial sanitaria y su interrelación con la protección de datos personales
- 2.4. Directiva NIS2 y su impacto en la catalogación de infraestructuras sanitarias como críticas
- 2.5. Estándares internacionales de seguridad de la información aplicados a la salud
- 2.6. Evaluaciones de impacto en protección de datos (EIPD) en proyectos sanitarios digitales
- 2.7. Regulación europea de la inteligencia artificial y sus implicaciones específicas para el sector salud



3: ARQUITECTURA DE SISTEMAS DE INFORMACIÓN SANITARIOS Y SUPERFICIES DE ATAQUE

- 3.1. Componentes principales de la infraestructura tecnológica en organizaciones sanitarias
- 3.2. Estándares de interoperabilidad y protocolos de comunicación de datos clínicos
- 3.3. Arquitecturas de red en entornos hospitalarios y centros ambulatorios
- 3.4. Identificación y análisis de la superficie de ataque en el ecosistema digital sanitario
- 3.5. Integración de servicios en la nube en entornos sanitarios regulados
- 3.6. Flujos de datos entre sistemas sanitarios y puntos críticos de exposición de información

4: AMENAZAS Y VULNERABILIDADES ESPECÍFICAS DEL ENTORNO SANITARIO

- 4.1. Panorama actual de ciberamenazas dirigidas específicamente al sector salud
- 4.2. Ransomware en hospitales: vectores de entrada, propagación e impacto asistencial
- 4.3. Phishing e ingeniería social dirigida al personal sanitario y administrativo
- 4.4. Amenazas internas y accesos no autorizados a datos sensibles de pacientes
- 4.5. Ataques dirigidos a la cadena de suministro tecnológico del sector sanitario
- 4.6. Exfiltración y comercialización de datos clínicos en mercados de la dark web
- 4.7. Vulnerabilidades en software médico heredado y sistemas operativos desactualizados
- 4.8. Amenazas emergentes: deepfakes médicos, manipulación de datos diagnósticos y falsificación de resultados



5: FUNDAMENTOS DE INTELIGENCIA ARTIFICIAL APLICADA A LA CIBERSEGURIDAD

- 5.1. Conceptos fundamentales de inteligencia artificial y aprendizaje automático en seguridad
- 5.2. Procesamiento de lenguaje natural (NLP) para el análisis automatizado de logs y alertas de seguridad
- 5.3. Modelos de detección de anomalías basados en técnicas de inteligencia artificial
- 5.4. Estrategias de integración de sistemas de IA en arquitecturas de seguridad preexistentes
- 5.5. Limitaciones, sesgos y riesgos inherentes a la aplicación de IA en ciberseguridad
- 5.6. IA generativa y su doble dimensión como herramienta defensiva y como vector de amenaza

6: TÉCNICAS DE IA PARA LA DETECCIÓN Y PREVENCIÓN DE AMENAZAS EN ENTORNOS CLÍNICOS

- 6.1. Sistemas de detección y prevención de intrusiones (IDS/IPS) potenciados con inteligencia artificial
- 6.2. Análisis comportamental de usuarios y entidades (UEBA) en organizaciones de salud
- 6.3. Automatización de la respuesta a incidentes mediante plataformas SOAR con capacidades de IA
- 6.4. Threat intelligence y análisis predictivo de amenazas dirigidas al sector salud
- 6.5. Aplicaciones de IA en la identificación proactiva de vulnerabilidades y pentesting automatizado
- 6.6. Evaluación de la eficacia y rendimiento de las soluciones de IA defensiva en entornos sanitarios reales



7: PROTECCIÓN Y CIFRADO DE DATOS CLÍNICOS E HISTORIALES ELECTRÓNICOS DE SALUD

- 7.1. Clasificación y categorización de datos clínicos según su nivel de sensibilidad y criticidad
- 7.2. Técnicas de cifrado aplicadas a la protección de información sanitaria
- 7.3. Anonimización y seudonimización de datos clínicos para investigación y analítica sanitaria
- 7.4. Gestión del ciclo de vida completo de los datos clínicos y procedimientos de destrucción segura
- 7.5. Protección de datos en sistemas de historia clínica electrónica
- 7.6. Privacidad diferencial y aprendizaje federado como técnicas avanzadas para la investigación clínica con IA

8: GESTIÓN DE IDENTIDADES, ACCESOS Y AUTENTICACIÓN EN SISTEMAS SANITARIOS

- 8.1. Principios de gestión de identidades y accesos (IAM) adaptados al entorno sanitario
- 8.2. Modelos de control de acceso aplicados a organizaciones de salud
- 8.3. Autenticación multifactor (MFA) en entornos clínicos de alta exigencia y disponibilidad
- 8.4. Gestión de accesos privilegiados (PAM) para administradores de sistemas e infraestructuras sanitarias
- 8.5. Single Sign-On (SSO) y gestión eficiente de sesiones en estaciones clínicas compartidas
- 8.6. Aplicación de inteligencia artificial en la detección de anomalías en patrones de acceso
- 8.7. Gestión de identidades de dispositivos médicos conectados y sistemas automatizados



9: SEGURIDAD EN DISPOSITIVOS MÉDICOS CONECTADOS E INTERNET DE LAS COSAS MÉDICAS (IOMT)

- 9.1. Panorama del Internet de las Cosas Médicas y su expansión en la práctica clínica contemporánea
- 9.2. Vulnerabilidades y riesgos de seguridad específicos de dispositivos médicos conectados
- 9.3. Marcos regulatorios y estándares de seguridad aplicables a dispositivos médicos conectados
- 9.4. Estrategias de segmentación y aislamiento de redes dedicadas a dispositivos médicos
- 9.5. Monitorización y detección de amenazas en entornos IoMT mediante inteligencia artificial
- 9.6. Gestión de parches y actualizaciones de seguridad en dispositivos médicos con restricciones operativas
- 9.7. Seguridad en wearables clínicos y plataformas de monitorización remota de pacientes

10: RESPUESTA A INCIDENTES Y CONTINUIDAD ASISTENCIAL ANTE CIBERATAQUES

- 10.1. Planificación y diseño del plan de respuesta a incidentes de ciberseguridad sanitaria
- 10.2. Fases de la respuesta a incidentes de ciberseguridad en entornos hospitalarios
- 10.3. Planes de continuidad de negocio y recuperación ante desastres (BCP/DRP) en el ámbito sanitario
- 10.4. Notificación de brechas de seguridad a autoridades competentes y pacientes afectados
- 10.5. Simulacros y ejercicios de ciberresiliencia en organizaciones sanitarias
- 10.6. Aplicación de inteligencia artificial en la automatización y aceleración de la respuesta a incidentes



11: GOBERNANZA, AUDITORÍA Y CUMPLIMIENTO EN CIBERSEGURIDAD SANITARIA

- 11.1. Marcos de gobernanza de ciberseguridad aplicados al sector sanitario
- 11.2. Funciones del delegado de protección de datos (DPO) y del CISO en entidades sanitarias
- 11.3. Gestión de riesgos de ciberseguridad en el entorno clínico y asistencial
- 11.4. Auditoría de seguridad de sistemas de información sanitarios
- 11.5. Definición y seguimiento de indicadores clave de rendimiento (KPI) en ciberseguridad sanitaria
- 11.6. Gestión de proveedores y terceros con acceso a datos clínicos y sistemas sanitarios

12: TENDENCIAS EMERGENTES Y CASOS PRÁCTICOS DE CIBERSEGURIDAD CON IA EN EL SECTOR SANITARIO

- 12.1. Evolución tecnológica de la IA aplicada a la ciberseguridad sanitaria: horizonte a medio y largo plazo
- 12.2. Arquitectura Zero Trust como modelo de seguridad integral para organizaciones sanitarias
- 12.3. IA adversarial: ataques sofisticados contra los propios sistemas de IA defensiva en sanidad
- 12.4. Ciberseguridad en telemedicina, plataformas de salud digital y aplicaciones de salud móvil (mHealth)
- 12.5. Análisis de casos reales de ciberataques a instituciones sanitarias a nivel global
- 12.6. Diseño de una estrategia integral de ciberseguridad sanitaria basada en inteligencia artificial
- 12.7. Retos éticos y sociales derivados de la aplicación de IA a la ciberseguridad en el ámbito de la salud



Titulación y Certificaciones



El alumno/a recibirá un **Certificado universitario** emitido por la **Universidad EUNEIZ**.



Descarga de certificados expedidos por Instituto Serca desde la Secretaría Virtual de nuestro Campus.



Proceso de **Matriculación**



Formalización de la matrícula:

- Completar y enviar el formulario de matriculación. Tras recibirlo, automáticamente le enviaremos sus claves de acceso a pagos/facturas.
- Una vez abonado el importe completo del Programa Formativo, el alumno/a recibirá los accesos al Campus Virtual y podrá iniciar su estudio.

Matricúlate

Más información



Métodos y facilidad de Pagos

- ✓ **Facilidad de pago:** Opciones de pago fraccionado sin intereses.
- ✓ **Seguridad:** Plataforma de pago online segura y encriptada.
- ✓ **Flexibilidad:** Varias opciones de pago como tarjeta de crédito, débito, transferencia bancaria y PayPal.
- ✓ **Descuentos:** Ofrecemos descuentos directos aplicados automáticamente al realizar la matrícula en nuestra web.
- ✓ **Simplicidad:** Proceso de pago simple e intuitivo en pocos pasos.
- ✓ **Facturación:** Descarga de facturas en el área de pagos.



¿Por qué elegir **Instituto Serca**?



Calidad en la enseñanza

Miles de alumnos/as de todo el mundo avalan nuestra **calidad** y nuestros **sistemas de enseñanza**, haciendo con Instituto Serca su especialización profesional.



Contenidos actualizados

Permanente actualización y mejora de contenidos. Instituto Serca está afiliado a las más prestigiosas instituciones de los ámbitos de **psicología, sanidad y educación**, para estar actualizados en las últimas innovaciones científicas y didácticas.



Profesionales de primer nivel

Nuestros programas formativos están diseñados por **profesionales de primer nivel** con amplia experiencia y siempre orientados al éxito profesional del alumnado.

¿Por qué elegir **Instituto Serca**?



A tu ritmo

Nos adaptamos al **ritmo de aprendizaje** de cada alumno/a. Nuestra metodología permite adaptarnos a las necesidades formativas individuales, garantizando así nuestra atención individualizada.



Tutorización

En Instituto Serca los alumnos/as disponen de un **tutor/a** a su disposición desde el momento de su matriculación, siendo prioritaria la resolución de dudas en el mínimo plazo.



Clases en vídeo

Clases en vídeo por materia para reforzar el contenido teórico. Además dispondrá de manera sistemática de un webinar de resolución de dudas.



SERCA

INSTITUTO
DE ALTOS ESTUDIOS
ESPECIALIZADOS



¿Necesita más **información**?

 www.institutoserca.com

 info@institutoserca.com

 +34 958 372 363 / 660 880 416

