ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Ciberseguridad Hospitalaria para Personal de Sistemas: Dispositivos Médicos Conectados, Incidentes y Continuidad Asistencial

3 ECTS | 75 horas | Online, a tu ritmo

Formación acreditada por
Universidad de Vitoria-Gasteiz EUNEIZ



Acerca de ICUFOR

ICUFOR es un centro privado de formación online, Centro Acreditado y Autorizado por la Universidad EUNEIZ de Vitoria-Gasteiz. Diseñamos e impartimos Cursos de Formación Permanente universitarios, pensados para la actualización y la especialización de profesionales en activo.

Nuestros cursos se estudian a tu ritmo en un campus virtual propio y terminan con el diploma de la Universidad EUNEIZ y con certificados de ICUFOR verificables.

Centro acreditado
Universidad EUNEIZ

100 % online
Campus virtual propio

Equipo docente
Disponible todo el curso



Metodología de estudio

Campus virtual propio
Estudias desde cualquier lugar y dispositivo, sin horarios.

Aprendizaje autónomo, pero acompañado
Tú marcas el ritmo y nuestro equipo de docentes resuelve tus dudas y orienta tu estudio.

Contenido del curso en PDF
El material principal, para estudiarlo a fondo, tema a tema.

Abstract de cada tema
Su síntesis, para situarte al empezar y repasar al final.

Presentación con los aspectos clave
Lo esencial de cada bloque, para jerarquizar y fijar.

Cuestionarios de evaluación
De respuesta múltiple, uno por tema.



Campus virtual

Mis cursos
Tu progreso y el siguiente tema por estudiar

Materiales
Contenido en PDF, Abstract y presentación con los aspectos clave

Cuestionarios de evaluación
Tu nota y la revisión de tus respuestas

Equipo docente
Consulta por escrito, chat y asesor de IA a cualquier hora

Secretaría
Certificados en PDF con código de verificación

Pagos y facturas
Descarga de facturas en PDF



Presentación del programa



Especialízate con este Curso de Formación Permanente en Ciberseguridad Hospitalaria que ICUFOR ha diseñado específicamente para profesionales de sistemas que trabajan en entornos sanitarios. En un contexto donde los ciberataques a hospitales se han multiplicado exponencialmente, la protección de infraestructuras críticas y datos clínicos se ha convertido en una prioridad estratégica que requiere conocimientos altamente especializados.

A través de nuestro programa formativo, abordarás desde los fundamentos normativos (RGPD, ENS, NIS2) hasta la gestión avanzada del ecosistema IoMT, incluyendo la seguridad de dispositivos médicos conectados y sus vulnerabilidades específicas. Profundizarás en arquitecturas de red hospitalarias, sistemas de información sanitarios como HIS y HCE, y estándares de interoperabilidad esenciales como HL7 y FHIR.

Duración
75 horas

Créditos
3 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos de la ciberseguridad sanitaria, contextualizando el marco normativo, los estándares de referencia y la gobernanza de seguridad aplicables al entorno hospitalario.

Identificar las vulnerabilidades del ecosistema de dispositivos médicos conectados (IoMT), clasificando los activos según su criticidad clínica, exposición y nivel de riesgo asociado.

Conocer las amenazas y vectores de ataque específicos del sector sanitario, utilizando técnicas de análisis de vulnerabilidades e inteligencia de amenazas para la evaluación y priorización de riesgos en infraestructuras hospitalarias.

Diseñar planes de continuidad asistencial y resiliencia operativa, elaborando estrategias de recuperación ante desastres, procedimientos de contingencia sin sistemas digitales y mecanismos de mejora continua.

Analizar la arquitectura tecnológica hospitalaria, diferenciando redes, sistemas de información clínicos y mecanismos de gestión de identidades y accesos en centros sanitarios.

Aplicar estrategias de protección y bastionado de dispositivos biomédicos, desarrollando procedimientos de segmentación, monitorización continua y gestión de actualizaciones en entornos sujetos a certificación regulatoria.

Dominar la gestión de incidentes de ciberseguridad en entornos hospitalarios, implementando protocolos de detección, contención, respuesta operativa, análisis forense y notificación a las autoridades competentes.

Temario

01 Fundamentos de ciberseguridad aplicados al entorno sanitario y hospitalario

1.1. Contextualización de la ciberseguridad en el sector salud y su relevancia estratégica
1.2. Marco normativo, regulatorio y estándares de referencia para la ciberseguridad sanitaria
1.3. Principios fundamentales de seguridad de la información en organizaciones de salud
1.4. Gobierno, políticas y cultura de ciberseguridad en organizaciones sanitarias

02 Arquitectura tecnológica, redes y sistemas de información en el entorno hospitalario

2.1. Topología y segmentación de redes en infraestructuras hospitalarias
2.2. Sistemas de información sanitarios, interoperabilidad y flujos de datos clínicos
2.3. Infraestructura de comunicaciones y conectividad en centros sanitarios
2.4. Servicios en la nube y virtualización en entornos sanitarios
2.5. Gestión de identidades, accesos y autenticación en sistemas clínicos
2.6. Monitorización y visibilidad integral de la infraestructura tecnológica hospitalaria

Temario

03 Seguridad de dispositivos médicos conectados y gestión del ecosistema IoMT

3.1. Caracterización del ecosistema de dispositivos médicos conectados (IoMT)
3.2. Vulnerabilidades específicas de los dispositivos médicos conectados
3.3. Inventario, descubrimiento y gestión de activos IoMT en redes clínicas
3.4. Estrategias de protección y bastionado de dispositivos médicos en entornos asistenciales
3.5. Evaluación de riesgos de ciberseguridad en dispositivos médicos conectados
3.6. Marco regulatorio específico para la ciberseguridad de productos sanitarios
3.7. Coordinación operativa entre servicios de ingeniería biomédica y departamentos de TI
3.8. Monitorización continua y detección de amenazas en el ecosistema IoMT

Temario

04 Amenazas, vulnerabilidades y vectores de ataque específicos de infraestructuras sanitarias

4.1. Panorama actualizado de amenazas dirigidas al sector sanitario
4.2. Vectores de ataque prevalentes en entornos hospitalarios
4.3. Superficie de ataque ampliada en escenarios de telemedicina y atención remota
4.4. Análisis de vulnerabilidades en infraestructuras sanitarias en producción
4.5. Inteligencia de amenazas aplicada al sector salud
4.6. Evaluación y priorización de riesgos en la infraestructura hospitalaria

Temario

05 Gestión de incidentes de ciberseguridad en entornos hospitalarios

5.1. Marco conceptual y fases de la gestión de incidentes adaptadas al contexto sanitario
5.2. Preparación organizativa y capacidad de detección ante ciberincidentes
5.3. Clasificación, triaje y priorización de incidentes según impacto asistencial
5.4. Procedimientos de respuesta operativa ante incidentes en hospitales
5.5. Análisis forense digital en entornos sanitarios
5.6. Obligaciones de comunicación y notificación de incidentes de ciberseguridad
5.7. Aprendizaje organizacional y mejora continua tras incidentes de ciberseguridad

Temario

06 Continuidad asistencial y resiliencia operativa ante ciberincidentes

6.1. Fundamentos de la continuidad de negocio aplicados al ámbito hospitalario
6.2. Análisis de impacto en el negocio (BIA) y planificación de la continuidad asistencial
6.3. Estrategias de copias de seguridad, recuperación ante desastres y resiliencia operativa
6.4. Gestión de la relación con proveedores tecnológicos y fabricantes de dispositivos en escenarios de crisis
6.5. Pruebas, mantenimiento y actualización periódica de los planes de continuidad

Titulación y certificados

Diploma de la Universidad EUNEIZ

Al aprobar todos los cuestionarios de evaluación recibes el **diploma en formato digital** de Curso de Formación Permanente, con sus 3 créditos ECTS y 75 horas.

Certificados de ICUFOR

Se descargan en PDF desde la Secretaría del campus, con un código único y QR para verificarlos.



Universidad de Vitoria-Gasteiz EUNEIZ

Proceso de matriculación

1 **Pulsa «Matricularme» en la ficha del curso**
Completa tus datos personales y de facturación.

2 **Elige la forma de pago**
Tarjeta, PayPal o transferencia bancaria.

3 **Entra en el campus y empieza**
Recibes por correo tus datos de acceso y, en cuanto se confirma el pago, tienes el temario completo. La matrícula está abierta todo el año.

Matricúlate | Más información



Métodos de pago

Pago único
El precio se abona una sola vez, sin cuotas ni renovaciones.

Seguridad
Pago online en la pasarela de Stripe o de PayPal.

Flexibilidad
Tarjeta de crédito o débito, PayPal o transferencia.

Acceso inmediato
Con tarjeta o PayPal, el campus se activa al momento.

Simplicidad
Matrícula y pago en dos pasos.

Facturación
Facturas en «Pagos y facturas» del campus.



¿Por qué elegir ICUFOR?

01

Formación accesible

Formación universitaria rigurosa y acreditada, íntegramente online y compatible con tu trabajo.

02

Calidad universitaria

Cada curso está acreditado por la Universidad EUNEIZ, con su memoria académica y sus créditos ECTS.

03

Impulso a tu carrera

Contenidos de utilidad práctica y una titulación que suma en méritos, concursos y bolsas de empleo.

04

Especialización

Cada curso trata una única temática a fondo: combínalos y construye tu propio itinerario.

05

Atención de calidad

Consultas al equipo docente por escrito o por chat, y un asesor de IA a cualquier hora.

¿Por qué elegir ICUFOR?

06

Contenidos actualizados

Los cursos se revisan periódicamente para incorporar las novedades de cada ámbito.

07

El curso, por escrito

Cada tema en tres formatos: contenido en PDF, Abstract y presentación con los aspectos clave.

08

Autónomo, pero acompañado

Tú decides tu ritmo y nuestro equipo de docentes resuelve tus dudas y orienta tu estudio.

09

Enseñanza adaptada

Sin horarios ni conexiones obligatorias: seis meses para terminar, ampliables si lo necesitas.

10

Estudio sencillo e intuitivo

Un campus virtual propio, sin instalar nada y accesible desde cualquier dispositivo.

¿Necesitas más información?

Te contamos cómo funciona el curso, los plazos y la titulación, sin compromiso.

www.icufor.com

info@icufor.com

+34 858 895 080

+34 746 044 519

Formación acreditada por Universidad de Vitoria-Gasteiz EUNEIZ

