ICUFOR
Cursos de Formación Permanente Universitaria



Curso de Formación Permanente

Ciberseguridad para el Profesional Asistencial: Correo Fraudulento, Puesto Clínico Seguro y Actuación ante un Ciberataque

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



Curso de Formación Permanente en Ciberseguridad para el Profesional Asistencial: Correo Fraudulento, Puesto Clínico Seguro y Actuación ante un Ciberataque de ICUFOR te prepara para afrontar uno de los mayores desafíos actuales del sector sanitario. Los ciberataques contra instituciones de salud han aumentado exponencialmente, poniendo en riesgo tanto la continuidad asistencial como la seguridad de los pacientes. Como profesional sanitario, te conviertes en la primera línea de defensa frente a estas amenazas digitales.

A través de este programa, dominarás la identificación y gestión del correo electrónico fraudulento, reconociendo técnicas de phishing, spear phishing y suplantación de identidad específicamente dirigidas al personal clínico.

Duración
75 horas

Créditos
3 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Conocer los fundamentos de ciberseguridad aplicados al entorno sanitario asistencial, identificando las principales amenazas, vectores de ataque y vulnerabilidades del ecosistema tecnológico clínico.

Aplicar el procedimiento de actuación ante la recepción de un correo sospechoso, utilizando los canales de notificación y las herramientas de protección disponibles en el entorno clínico.

Conocer el marco normativo vigente en materia de protección de datos de salud y ciberseguridad, diferenciando las obligaciones y responsabilidades legales, éticas y disciplinarias del profesional asistencial.

Comprender los planes de continuidad asistencial y las fases de recuperación tras un ciberataque, incorporando las lecciones aprendidas en la actualización de protocolos y programas de formación.

Distinguir las diferentes tipologías de correo electrónico fraudulento dirigidas al profesional sanitario, analizando sus elementos constitutivos, indicadores lingüísticos y señales de alerta.

Dominar las prácticas de configuración y uso seguro del puesto clínico de trabajo, implementando una gestión adecuada de credenciales, dispositivos de almacenamiento externo y acceso remoto.

Describir el protocolo de respuesta inmediata ante un ciberataque en el entorno asistencial, identificando las señales de alerta temprana, las acciones críticas de aislamiento y la cadena de notificación interna.

Temario

01 Fundamentos de ciberseguridad aplicados al entorno sanitario asistencial

1.1. Contexto actual de la ciberseguridad en el sector salud y su relevancia para la práctica clínica
1.2. Conceptos esenciales de seguridad de la información aplicados al ámbito clínico
1.3. Principales tipos de amenazas y vectores de ataque en organizaciones sanitarias
1.4. Ecosistema tecnológico del entorno clínico: sistemas de información y dispositivos médicos conectados
1.5. El rol del profesional asistencial como primera línea de defensa frente a las ciberamenazas

02 Identificación y gestión del correo electrónico fraudulento en el ámbito sanitario

2.1. El correo electrónico como principal vector de ciberataques en organizaciones sanitarias
2.2. Tipología de ataques basados en el correo electrónico dirigidos al profesional sanitario
2.3. Anatomía de un correo fraudulento: elementos de identificación y señales de alerta
2.4. Análisis de casos reales de ataques por correo electrónico en instituciones sanitarias
2.5. Procedimiento de actuación ante la recepción de un correo electrónico sospechoso
2.6. Herramientas de protección y buenas prácticas en el uso del correo electrónico clínico

Temario

03 Configuración y uso seguro del puesto clínico de trabajo

3.1. Definición y componentes del puesto clínico de trabajo en el entorno sanitario actual
3.2. Gestión segura de credenciales y sistemas de autenticación en aplicaciones clínicas
3.3. Navegación segura y uso responsable de internet y redes Wi-Fi desde el puesto clínico
3.4. Gestión de actualizaciones, parches de seguridad y política de software autorizado
3.5. Seguridad física del puesto de trabajo y política de escritorio limpio
3.6. Uso seguro de dispositivos de almacenamiento externo y transferencia de archivos clínicos
3.7. Teletrabajo y acceso remoto seguro a sistemas de información sanitarios

Temario

04 Marco normativo, protección de datos de salud y responsabilidad del profesional sanitario en ciberseguridad

4.1. Marco legal y regulatorio de la ciberseguridad y la protección de datos en el sector sanitario
4.2. Protección de datos de salud como categoría especial de datos personales
4.3. Responsabilidad profesional e institucional ante brechas e incidentes de seguridad
4.4. Políticas de seguridad de la información y promoción de la cultura de ciberseguridad en organizaciones sanitarias

Temario

05 Protocolo de actuación ante un ciberataque en entornos asistenciales

5.1. Tipos de ciberataques con mayor incidencia e impacto en el entorno sanitario
5.2. Señales de alerta y detección temprana de un ciberataque desde el puesto clínico
5.3. Protocolo de respuesta inmediata del profesional asistencial ante un ciberincidente
5.4. Plan de continuidad asistencial durante un ciberataque activo
5.5. Fases de recuperación y vuelta a la normalidad operativa tras un ciberataque
5.6. Análisis post-incidente, lecciones aprendidas y mejora de los protocolos de seguridad
5.7. Simulacros y ejercicios de preparación ante ciberataques en instituciones sanitarias
5.8. Recursos y organismos de referencia para la gestión de ciberincidentes en el sector salud

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.



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

