ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Seguridad en Teletrabajo y Dispositivos Móviles para Empleados Públicos

6 ECTS | 150 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

Amplía tu formación con este programa especializado que responde a una necesidad crítica en la Administración Pública actual: garantizar la protección de la información y los sistemas en entornos de trabajo remoto. La transformación digital del sector público ha convertido la ciberseguridad en una competencia imprescindible para todo empleado que desempeñe sus funciones a distancia, siendo fundamental conocer los protocolos y herramientas que salvaguardan los datos institucionales y ciudadanos.



Duración
150 horas

Créditos
6 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender el marco conceptual del teletrabajo en la Administración Pública, identificando sus implicaciones en materia de seguridad digital y el papel del empleado público como agente clave en la protección de la información.

Analizar las ciberamenazas y los riesgos específicos del entorno de teletrabajo, aplicando metodologías de gestión de riesgos como MAGERIT para identificar vulnerabilidades y definir estrategias de tratamiento adecuadas.

Implementar buenas prácticas de configuración y protección de dispositivos móviles y comunicaciones, incorporando medidas de cifrado, segmentación de redes y uso seguro de herramientas colaborativas y servicios en la nube.

Conocer el marco normativo y regulatorio aplicable a la seguridad en el teletrabajo público, diferenciando las obligaciones derivadas del Esquema Nacional de Seguridad, la normativa de protección de datos y la legislación de trabajo a distancia.

Dominar los mecanismos de acceso remoto seguro a los sistemas de la Administración Pública, distinguiendo arquitecturas, tecnologías VPN, modelos de autenticación robusta y principios del enfoque Zero Trust.

Aplicar los principios de protección de datos personales y gestión segura de la información pública en el teletrabajo, utilizando técnicas de clasificación, cifrado y prevención de fugas de información conforme a las directrices del CCN-CERT.

Objetivos del curso

Identificar las técnicas de ingeniería social dirigidas a empleados públicos, desarrollando capacidades de detección y respuesta ante intentos de manipulación y contribuyendo a la construcción de una cultura organizacional de ciberseguridad.

Saber llevar a cabo la detección, notificación y contención de incidentes de seguridad en el entorno de teletrabajo, relacionando los procedimientos de respuesta con las políticas de auditoría, continuidad del servicio y mejora continua del organismo.

Temario

01 Marco conceptual del teletrabajo y la seguridad digital en la Administración Pública

1.1. Transformación digital y evolución del teletrabajo en el sector público
1.2. Conceptos fundamentales de seguridad de la información aplicados al teletrabajo
1.3. Diferencias entre el entorno presencial y el teletrabajo desde la perspectiva de la ciberseguridad
1.4. El papel del empleado público como eslabón clave en la cadena de seguridad
1.5. Principales organismos y referencias en materia de ciberseguridad para el sector público

02 Marco normativo y regulatorio de la seguridad en el teletrabajo para empleados públicos

2.1. El Esquema Nacional de Seguridad (ENS) y su aplicación al entorno de teletrabajo
2.2. Regulación del teletrabajo en la Administración Pública española
2.3. Reglamento General de Protección de Datos y Ley Orgánica de Protección de Datos Personales
2.4. Leyes 39/2015 y 40/2015 en el contexto de la administración electrónica y el teletrabajo
2.5. Guías y directrices del CCN-CERT aplicables al teletrabajo seguro en organismos públicos
2.6. Responsabilidades legales y disciplinarias del empleado público en materia de seguridad de la información

Temario

03 Análisis de amenazas y gestión de riesgos en entornos de teletrabajo

3.1. Panorama actual de ciberamenazas dirigidas al sector público
3.2. Amenazas específicas derivadas del entorno de teletrabajo
3.3. Fundamentos de la gestión de riesgos en seguridad de la información
3.4. Metodología MAGERIT aplicada al análisis de riesgos del teletrabajo
3.5. Estrategias de tratamiento del riesgo en el trabajo remoto
3.6. Monitorización continua del nivel de riesgo en entornos de teletrabajo
3.7. Casos prácticos de análisis de riesgos en escenarios de teletrabajo público

Temario

04 Seguridad en el acceso remoto a los sistemas de la Administración Pública

4.1. Arquitecturas de acceso remoto seguro para entornos del sector público
4.2. Redes privadas virtuales (VPN): configuración y buenas prácticas para el empleado público
4.3. Autenticación robusta y gestión de identidades digitales
4.4. El modelo de seguridad Zero Trust aplicado al teletrabajo en la Administración Pública
4.5. Control de acceso basado en roles y segregación de funciones en el entorno remoto
4.6. Registro, auditoría y trazabilidad de los accesos remotos a los sistemas corporativos

Temario

05 Seguridad en dispositivos móviles utilizados por empleados públicos

5.1. Tipología de dispositivos móviles en el entorno de trabajo del sector público
5.2. Amenazas y vulnerabilidades específicas de los dispositivos móviles
5.3. Configuración segura de dispositivos móviles para uso profesional en la Administración
5.4. Políticas de uso de dispositivos personales con fines profesionales (BYOD)
5.5. Sistemas de gestión de dispositivos móviles (MDM, EMM y UEM) en el sector público
5.6. Mecanismos de separación de entornos personal y profesional en el dispositivo
5.7. Procedimientos de actuación ante pérdida, robo o compromiso de un dispositivo móvil
5.8. Guías y recomendaciones del CCN-CERT para la seguridad de dispositivos móviles

Temario

06 Comunicaciones seguras y protección de las redes en el entorno de teletrabajo

6.1. Seguridad de la red doméstica del empleado público teletrabajador
6.2. Protección de las comunicaciones mediante correo electrónico institucional
6.3. Seguridad en herramientas de videoconferencia y comunicación en tiempo real
6.4. Cifrado de las comunicaciones extremo a extremo en el teletrabajo público
6.5. Uso seguro de redes Wi-Fi públicas y conexiones realizadas fuera del domicilio
6.6. Navegación segura y protección frente a amenazas procedentes de la web

07 Seguridad en servicios en la nube y herramientas colaborativas del sector público

7.1. Modelos de servicios en la nube utilizados por la Administración Pública
7.2. Riesgos de seguridad específicos de los entornos cloud para el teletrabajo
7.3. Uso seguro de plataformas colaborativas y de almacenamiento en la nube
7.4. Criterios de selección de proveedores cloud conformes con el Esquema Nacional de Seguridad
7.5. Copias de seguridad y planes de continuidad en entornos de servicios cloud

Temario

08 Protección de datos personales y gestión segura de la información pública en el teletrabajo

8.1. Principios de protección de datos aplicados al trabajo remoto del empleado público
8.2. Clasificación y etiquetado de la información en la Administración Pública
8.3. Cifrado de datos en reposo y en tránsito en el entorno de teletrabajo
8.4. Prevención de fugas de información (DLP) en el entorno remoto de trabajo
8.5. Gestión segura de documentación en papel en el domicilio del teletrabajador
8.6. Destrucción y eliminación segura de información sensible en soportes físicos y digitales
8.7. Transferencias internacionales de datos y sus implicaciones en el contexto del teletrabajo

Temario

09 Ingeniería social, concienciación y cultura de ciberseguridad en el entorno público

9.1. Fundamentos de la ingeniería social y su especial relevancia en el teletrabajo
9.2. Técnicas de ingeniería social más utilizadas contra empleados públicos
9.3. Identificación y respuesta ante intentos de ingeniería social
9.4. Programas de concienciación y formación continua en ciberseguridad para empleados públicos
9.5. Construcción de una cultura organizacional de ciberseguridad en la Administración

10 Gestión de incidentes de seguridad en entornos de teletrabajo

10.1. Concepto, tipología y clasificación de incidentes de seguridad en el teletrabajo
10.2. Marco de gestión de incidentes según el ENS y las guías del CCN-CERT
10.3. Detección y notificación de incidentes por parte del empleado público teletrabajador
10.4. Primeras acciones de contención al alcance del empleado público teletrabajador
10.5. Coordinación con los equipos de respuesta ante incidentes (CERT/CSIRT) del organismo
10.6. Lecciones aprendidas y mejora continua tras la resolución de un incidente

Temario

11 Políticas de seguridad, auditoría y mejora continua del teletrabajo en la Administración Pública

11.1. Diseño y estructura de las políticas de seguridad específicas para el teletrabajo
11.2. Auditoría y verificación del cumplimiento de las medidas de seguridad en el teletrabajo
11.3. Planificación de la continuidad del servicio público y recuperación ante desastres
11.4. Tendencias emergentes y retos futuros de la ciberseguridad en el teletrabajo público

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 6 créditos ECTS y 150 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

