ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Seguridad en la Nube y Microsoft 365 en Organismos Públicos: Configuración y Buenas Prácticas

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



Especialízate con este programa diseñado para profesionales que trabajan o desean incorporarse al ámbito de la ciberseguridad en las administraciones públicas. En ICUFOR comprendemos que la transformación digital del sector público requiere especialistas capaces de garantizar la protección de los sistemas de información y los datos de los ciudadanos. La migración a entornos cloud y la adopción de herramientas colaborativas como Microsoft 365 plantean desafíos de seguridad únicos que demandan conocimientos técnicos actualizados y alineados con el marco normativo vigente.

Duración
150 horas

Créditos
6 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos de la computación en la nube y sus modelos de despliegue y servicio, identificando las ventajas, riesgos y desafíos específicos de su adopción en organismos públicos.

Analizar la arquitectura de seguridad de Microsoft 365, describiendo sus componentes, capas de protección y el paradigma de confianza cero como base de la defensa en profundidad.

Implementar directivas de protección de dispositivos, correo electrónico e información sensible, utilizando Microsoft Intune, Defender for Office 365 y Microsoft Purview para prevenir amenazas y pérdida de datos.

Conocer el marco normativo y regulatorio aplicable a la seguridad en la nube en el sector público, diferenciando las obligaciones derivadas del ENS, el RGPD, la Directiva NIS2 y las guías del CCN.

Dominar la gestión de identidades y el control de acceso con Microsoft Entra ID, aplicando autenticación multifactor, directivas de acceso condicional y protección de cuentas privilegiadas en entornos gubernamentales.

Diseñar estrategias de gobernanza y configuración segura de las herramientas colaborativas, incorporando controles de compartición, acceso externo y etiquetado de confidencialidad en Teams, SharePoint Online y OneDrive.

Objetivos del curso

Desarrollar capacidades de monitorización, auditoría y respuesta a incidentes de seguridad en Microsoft 365, utilizando Microsoft Sentinel, Defender XDR y los registros de auditoría unificados conforme a los procedimientos de coordinación con el CCN-CERT.

Elaborar un plan integral de securización y bastionado de un tenant de Microsoft 365 para un organismo público, aplicando las guías CCN-STIC, las líneas base de seguridad y una metodología de mejora continua adaptada a cambios normativos y tecnológicos.

Temario

01 Fundamentos de la computación en la nube y su adopción en el sector público

1.1. Concepto, evolución histórica y principios básicos de la computación en la nube
1.2. Modelos de despliegue: nube pública, privada, híbrida y comunitaria en las administraciones públicas
1.3. Modelos de servicio y distribución de responsabilidades de seguridad
1.4. Ventajas, riesgos y desafíos específicos de la migración a la nube en el ámbito público
1.5. Panorama actual de la adopción de servicios en la nube por las administraciones públicas en España y Europa

Temario

02 Marco normativo, regulatorio y de referencia aplicable a la seguridad en la nube en organismos públicos

2.1. El Esquema Nacional de Seguridad (ENS) y su aplicación a los servicios en la nube
2.2. Reglamento General de Protección de Datos (RGPD) y Ley Orgánica de Protección de Datos (LOPDGDD) en entornos cloud
2.3. Normativa europea sobre ciberseguridad: Directiva NIS2 y Reglamento de Ciberseguridad (Cybersecurity Act)
2.4. Guías y recomendaciones del Centro Criptológico Nacional (CCN) para servicios cloud
2.5. Contratación pública de servicios en la nube: pliegos de condiciones y requisitos de seguridad
2.6. Marco de gobernanza de la información y políticas de seguridad corporativas en la administración pública
2.7. Marcos internacionales de referencia y estándares de seguridad en la nube: ISO 27017, ISO 27018 y CSA STAR

Temario

03 Arquitectura de seguridad del ecosistema Microsoft 365 y sus componentes fundamentales

3.1. Visión general del ecosistema Microsoft 365: componentes, servicios y planes de licenciamiento para el sector público
3.2. Infraestructura de centros de datos de Microsoft y garantías de residencia de datos para organismos europeos
3.3. Modelo de confianza cero (Zero Trust) como paradigma de seguridad en Microsoft 365
3.4. Arquitectura de seguridad multicapa de Microsoft 365: defensa en profundidad
3.5. Portales de administración y centros de seguridad de Microsoft 365

Temario

04 Gestión de identidades y control de acceso con Microsoft Entra ID en organismos públicos

4.1. Fundamentos de Microsoft Entra ID como servicio de identidad en la nube
4.2. Configuración de modelos de identidad híbrida: sincronización con directorios locales
4.3. Autenticación multifactor (MFA) y métodos de autenticación robusta
4.4. Directivas de acceso condicional: diseño, configuración y despliegue
4.5. Microsoft Entra ID Protection: detección y remediación de riesgos de identidad
4.6. Gestión de roles administrativos y protección de cuentas privilegiadas
4.7. Gestión del ciclo de vida de identidades externas y acceso de invitados (B2B)
4.8. Revisiones de acceso y gobernanza de identidades con Microsoft Entra ID Governance

Temario

05 Protección de dispositivos y puntos de acceso mediante Microsoft Intune y seguridad de endpoints

5.1. Estrategia de gestión unificada de endpoints en organismos públicos: fundamentos y planificación
5.2. Inscripción y registro de dispositivos en Microsoft Intune: escenarios gubernamentales
5.3. Directivas de cumplimiento de dispositivos y su integración con el acceso condicional
5.4. Perfiles de configuración de seguridad y líneas base de seguridad (security baselines)
5.5. Gestión de aplicaciones móviles (MAM) y protección de datos corporativos en dispositivos personales (BYOD)
5.6. Microsoft Defender for Endpoint: protección avanzada del punto de conexión

Temario

06 Seguridad del correo electrónico y protección contra amenazas avanzadas en Exchange Online

6.1. Panorama de amenazas dirigidas al correo electrónico en organismos públicos
6.2. Exchange Online Protection (EOP): configuración de la protección estándar del correo
6.3. Microsoft Defender for Office 365: protección avanzada frente a amenazas sofisticadas
6.4. Directivas de seguridad preestablecidas: perfiles estándar y estricto en entornos gubernamentales
6.5. Investigación y respuesta automatizada ante incidentes de correo electrónico
6.6. Simulación de ataques de phishing y concienciación de empleados públicos con Attack Simulation Training

Temario

07 Protección de la información sensible y prevención de pérdida de datos con Microsoft Purview

7.1. Clasificación de la información en organismos públicos: marco conceptual y requisitos normativos
7.2. Etiquetas de confidencialidad de Microsoft Purview Information Protection: diseño y despliegue
7.3. Tipos de información sensible y clasificadores entrenables para datos del sector público
7.4. Directivas de prevención de pérdida de datos (DLP) en Microsoft Purview
7.5. Cifrado de mensajes de Microsoft Purview (OME) para comunicaciones seguras con entidades externas
7.6. Azure Information Protection Unified Labeling y protección de documentos fuera de Microsoft 365
7.7. Supervisión y análisis del estado de protección de la información

Temario

08 Seguridad y gobernanza de herramientas colaborativas: Microsoft Teams, SharePoint Online y OneDrive

8.1. Análisis de riesgos de seguridad específicos en los entornos de colaboración de Microsoft 365
8.2. Configuración segura de Microsoft Teams en organismos públicos
8.3. Configuración segura de SharePoint Online y OneDrive for Business
8.4. Gobernanza del ciclo de vida de grupos de Microsoft 365 y equipos de Teams
8.5. Aplicación de etiquetas de confidencialidad a equipos de Teams, sitios de SharePoint y grupos de Microsoft 365
8.6. Microsoft Defender for Cloud Apps: visibilidad y control sobre el uso de aplicaciones SaaS

Temario

09 Cumplimiento normativo, retención de la información y gestión de riesgos internos con Microsoft Purview

9.1. Administrador de cumplimiento de Microsoft Purview: evaluación de la postura de cumplimiento del organismo público
9.2. Directivas de retención y eliminación de la información en Microsoft 365
9.3. Administración de registros con Microsoft Purview para la gestión documental del sector público
9.4. eDiscovery y búsqueda de contenido para investigaciones internas y requerimientos legales
9.5. Gestión de riesgos internos y controles de separación de la información

Temario

10 Monitorización, auditoría y respuesta a incidentes de seguridad en Microsoft 365

10.1. Registro de auditoría unificado de Microsoft 365: configuración, consulta y retención
10.2. Microsoft Sentinel como solución SIEM/SOAR para entornos Microsoft 365 en organismos públicos
10.3. Panel de incidentes de Microsoft Defender XDR: investigación y correlación de alertas
10.4. Microsoft Secure Score: evaluación continua y mejora de la postura de seguridad del tenant
10.5. Procedimiento de gestión de incidentes de seguridad en la nube adaptado a organismos públicos
10.6. Alertas de actividad y directivas de alerta en los portales de seguridad y cumplimiento
10.7. Informes de seguridad y cuadros de mando para la dirección del organismo público

Temario

11 Buenas prácticas de configuración segura y bastionado del tenant de Microsoft 365 para organismos públicos

11.1. Guías de referencia del CCN para la configuración segura de Microsoft 365
11.2. Líneas base de seguridad de Microsoft y marcos de configuración recomendada (CIS Benchmarks)
11.3. Configuración segura de la autenticación y el acceso a nivel de tenant
11.4. Bastionado de los servicios principales: Exchange Online, SharePoint Online, OneDrive y Teams
11.5. Gestión segura de la administración del tenant: segregación de funciones y protección de cuentas de administración
11.6. Proceso continuo de revisión de la configuración de seguridad y auditorías periódicas

Temario

12 Planificación, implantación y caso práctico integral de seguridad de Microsoft 365 en un organismo público

12.1. Metodología de planificación del proyecto de securización de Microsoft 365 en la administración pública
12.2. Estrategia de gestión del cambio y formación en ciberseguridad para empleados públicos
12.3. Desarrollo del caso práctico integral: configuración de seguridad de un tenant de Microsoft 365 para un organismo público tipo
12.4. Plan de mantenimiento, mejora continua y adaptación a cambios normativos y tecnológicos

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

