ESIBE
ESCUELA IBEROAMERICANA DE POSTGRADO

Titulación expedida por Escuela Iberoamericana de Postgrado

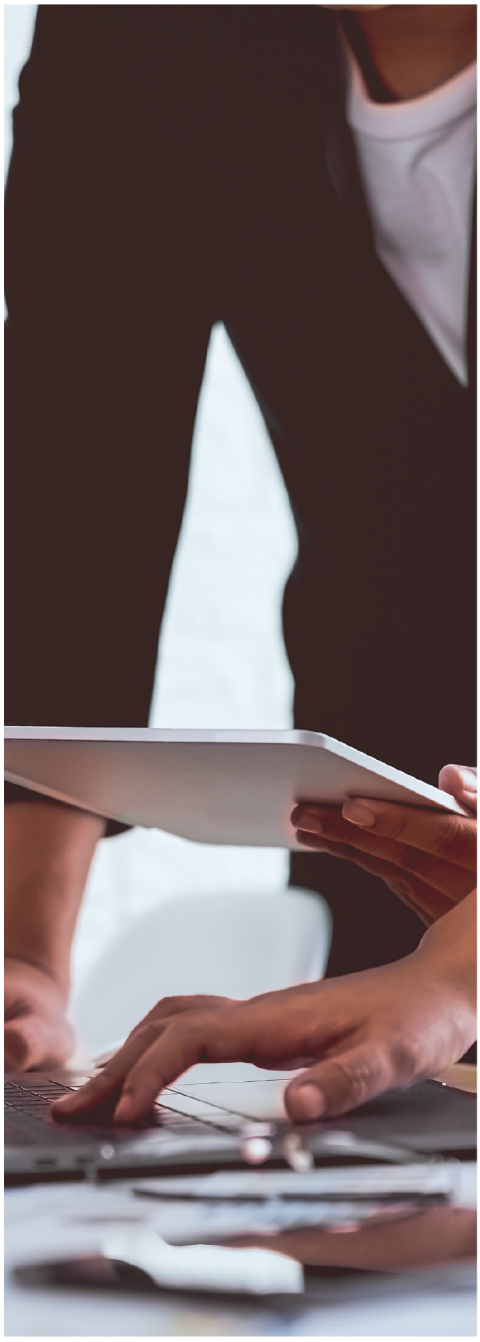
Maestría en Ciberseguridad

ALIANZA ESIBE Y UNIVERSIDAD DEL NORTE

ESIBE, Escuela Iberoamericana de Postgrado colabora estrechamente con la Universidad del Norte con el objetivo de **democratizar el acceso a la educación y apostar por la implementación de la tecnología en el sector educativo.** Para cumplir con esta misión, ambas entidades aúnan sus conocimientos y metodologías de enseñanza, logrando así una formación internacional y diferenciadora.

Esta suma de saberes hace que el proceso educativo se enriquezca y ofrezca al alumnado una oferta **variada, plural y de alta calidad.** La formación aborda materias desde un enfoque técnico y práctico, buscando contribuir al desarrollo de las capacidades y actitudes necesarias para el desempeño profesional.

ACREDITACIONES



Escuela Iberoamericana de Formación en línea.

ESIBE nace con la misión de crear un punto de encuentro entre Europa y América. Desde hace más de 18 años trabaja para cumplir con este reto, teniendo como finalidad potenciar el futuro empresarial de los profesionales de ambos continentes a través de programas de master, masters oficiales, master universitarios y maestrías.

ESIBE cuenta con Euroinnova e INESEM como entidades educativas de formación online colaboradoras, trabajando unidas para brindar nuevas oportunidades a sus estudiantes. Gracias al trabajo conjunto de estas instituciones, se ha conseguido llevar un modelo pedagógico único a miles de estudiantes y se han trazado alianzas estratégicas con diferentes universidades de prestigio.

ESIBE se sirve de la Metodología Active, una forma de adquirir conocimientos diferente que prima el aprendizaje personalizado atendiendo al contexto del estudiante, a sus objetivos y a su ritmo de aprendizaje. Para conseguir ofrecer esta forma particular de aprender, la entidad educativa se sirve de la Inteligencia Artificial y de los últimos avances tecnológicos.

ESIBE apuesta por ofrecer a su alumnado una formación de calidad sin barreras físicas, aprendiendo 100 % online, de forma flexible y adaptada a las necesidades e inquietudes del alumnado.

¡Aprende disfrutando de una experiencia que se adapta a ti!

VALORES

Los valores sobre los que se asienta Euroinnova son:

1

Accesibilidad
Somos cercanos y comprensivos, trabajamos para que todas las personas tengan oportunidad de seguir formándose.

2

Honestidad
Somos claros y transparentes, nuestras acciones tienen como último objetivo que el alumnado consiga sus objetivos, sin sorpresas.

3

Practicidad
Formación práctica que suponga un aprendizaje significativo. Nos esforzamos en ofrecer una metodología práctica.

4

Empatía
Somos inspiracionales y trabajamos para entender al alumno y brindarle así un servicio pensado por y para él.

A día de hoy, han pasado por nuestras aulas más de **300.000 alumnos** provenientes de los cinco continentes. Euroinnova es actualmente una de las empresas con mayor índice de crecimiento y proyección en el panorama internacional.

Nuestro portfolio se compone de cursos online, cursos homologados, baremables en oposiciones y formación superior de postgrado y máster.


Bolsa de empleo

METODOLOGÍA ACTIVE

Nuestra **Metodología Active** tiene en cuenta el perfil de cada estudiante y adapta el contenido a sus preferencias a través de la inteligencia artificial. Es una formación 100 % online, práctica y profesional.

1. Aprendizaje significativo y práctico

Los conocimientos se incorporan de forma sustantiva en la estructura cognitiva del alumnado. A través de sucesivas **prácticas** y de **ejercicios de reflexión**, se conduce al estudiante a relacionar los nuevos contenidos con los anteriormente adquiridos, conformando las bases de un aprendizaje sólido, útil y pragmático.

2. Flexibilidad

Aprendizaje a tu ritmo, a la hora que prefieras y desde cualquier lugar. **ESIBE se adapta a ti**, a tus circunstancias y a tu contexto. Tenemos en cuenta tus intereses y tu motivación y respondemos ofreciéndote un temario y un servicio acorde a tus preferencias y necesidades.

3. Acompañamiento docente

Contamos con **profesionales en activo**, con gran vocación y con dilatada experiencia para ofrecerte una formación de calidad y acorde a la realidad laboral. Además, contamos con un equipo de asesoramiento que te guiará durante todo el proceso de aprendizaje y te dará pautas para superar con éxito tu etapa educativa.

4. Innovación

Apostamos por la **implementación de la tecnología** y de los últimos **avances en e-learning.** Nos servimos de la IA para un aprendizaje inteligente, que tenga en cuenta tus metas y te permita desarrollarte profesionalmente en función de tus preferencias y potencial.

5. Desarrollo de competencias profesionales más demandadas

La metodología Active te prepara para el **desarrollo de las competencias más demandadas** del mercado. Conectamos el talento con la realidad laboral. Primamos el desarrollo de personas autónomas, críticas, con grandes dotes comunicativos y capaces de resolver casos reales.

6. ESIBE contigo

Te ofrecemos la oportunidad **de estar conectado** a distintos **temas de interés** gracias a nuestros **seminarios**. Profesionales de áreas especializadas nos cuentan de forma periódica los avances y novedades en los distintos campos, así como trucos y consejos.

7. Campus virtual

Aprende en un **entorno dinámico, avanzado e intuitivo.** Disfruta de un campus virtual diseñado por expertos y con múltiples funcionalidades para un aprendizaje óptimo.

8. Contenido de calidad

Temario actualizado, de calidad y acorde al contexto actual. Aprenderás con contenido elaborado específicamente para la formación en cuestión y con recursos didácticos que te permitirán una mejor comprensión. El temario está sometido a constantes cambios en función de la evolución del campo de especialización.

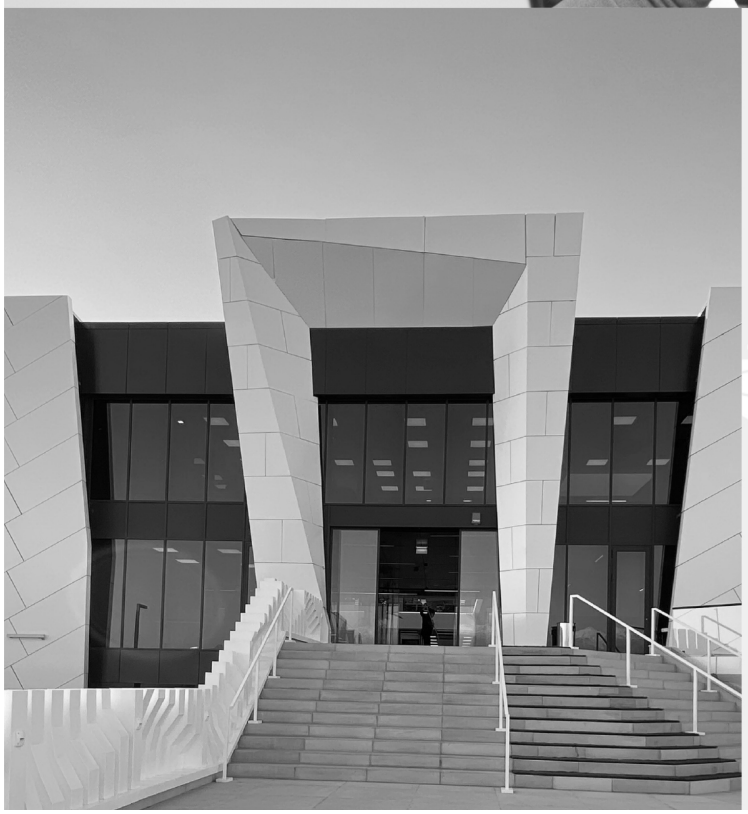
+200K Estudiantes formados

+18 Años de experiencia en el sector de la formación

5 Alumnado de los 5 continentes

98% de satisfacción

84% de los estudiantes repiten en ESIBE



Nuestras Sedes

España | Miami | México

ESIBE

Maestría en Ciberseguridad

DURACIÓN
1500 horas

MODALIDAD
Online

ACOMPAÑAMIENTO PERSONALIZADO

TITULACIÓN

Titulación de Maestría en Ciberseguridad con 1500 horas expedida por ESIBE (ESCUELA IBEROAMERICANA DE POSTGRADO).


ESIBE
Escuela Iberoamericana de Postgrado
NOMBRE DEL ALUMNO/A
Acción Formativa
Con un nivel de aprovechamiento [CALIFICACIÓN]

DESCRIPCIÓN

La ciberseguridad siempre ha sido importante, pero de un tiempo a esta parte se ha convertido en el eje central a seguir tanto para el mundo empresarial como en nuestro día a día. Con esta Maestría en Ciberseguridad podrás defenderte de ciberataques y aplicar estrategias para mejorar la ciberseguridad de sistemas, procesos o entornos. Conocerás la legislación y normativa que hay que cumplir. Utilizarás sistemas IDS/IPS, SIEM y herramientas OSINT como Shodan o Maltego. Aprenderás cómo funciona el hacking ético y entrenarás en plataformas como Hack the Box, Tryhackme o Vulnhub y por último desarrollarás webs de forma segura. Contarás con un equipo de profesionales especializados en la materia. Además, gracias a las prácticas garantizadas, podrás acceder a un mercado laboral en plena expansión.

OBJETIVOS

- Conocer la legislación y normativa aplicable para los Sistemas de Gestión de la Seguridad de la Información (SGSI).
- Utilizar herramientas OSINT como Google Dork, Shodan, Maltego, The Harvester o Foca.
- Saber cómo establecer comunicaciones seguras, cómo encriptar información e implantar sistemas IDS/IPS.
- Entender en qué consiste el hacking ético y como se aplica en diferentes entornos y ataques.
- Descubrir los principales aspectos y herramientas para llevar a cabo auditorías informáticas.
- Entrenar las técnicas de hacking en plataformas como Hack the Box (HTB), Tryhackme, Hacker101 o Vulnhub.
- Aprender a utilizar las guías OWASP para poder llevar a cabo desarrollos web seguros, testing y revisión de código.

A QUIÉN VA DIRIGIDO

La ciberseguridad es utilizada en todas las áreas, pero para su desarrollo los perfiles más adecuados para llevar a cabo esta Maestría en Ciberseguridad serían los de Ingenieros informáticos o estudiantes en Grados de informática que quieran especializarse en las principales técnicas y herramientas para garantizar la ciberseguridad siguiendo la legislación

y normativa vigente.

PARA QUÉ TE PREPARA

Con esta Maestría en Ciberseguridad podrás defenderte de ciberataques y aplicar estrategias para mejorar la ciberseguridad de sistemas, procesos o entornos. Conocerás la legislación y normativa que hay que cumplir. Utilizarás sistemas IDS/IPS, SIEM y herramientas OSINT como Shodan o Maltego. Aprenderás cómo funciona el hacking ético y entrenarás en plataformas como Hack the Box, Tryhackme o Vulnhub y por último desarrollarás webs de forma segura.

Programa Formativo

MÓDULO 1. LEGISLACIÓN, POLÍTICA DE SEGURIDAD Y CIBERINTELIGENCIA

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN Y CONCEPTOS BÁSICOS

1. La sociedad de la información
2. Diseño, desarrollo e implantación
3. Factores de éxito en la seguridad de la información

UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

1. Estándares y Normas Internacionales sobre los SGSI. ISO 27001
2. Legislación: Leyes aplicables a los SGSI (RGPD)

UNIDAD DIDÁCTICA 3. POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS

1. Plan de implantación del SGSI
2. Análisis de riesgos
3. Gestión de riesgos

UNIDAD DIDÁCTICA 4. CONTROL MALWARE

1. Sistemas de detección y contención de Malware
2. Herramientas de control de Malware
3. Criterios de seguridad para la configuración de las herramientas de protección frente a Malware
4. Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a Malware
5. Relación de los registros de auditoría de las herramientas de protección frente a Malware
6. Establecimiento de la monitorización y pruebas de las herramientas de protección frente a Malware
7. Análisis de Malware mediante desensambladores y entornos de ejecución controlada

UNIDAD DIDÁCTICA 5. INGENIERÍA SOCIAL, ATAQUES WEB Y PHISHING

1. Introducción a la ingeniería social
2. Recopilar información
3. Herramientas de ingeniería social
4. Técnicas de ataques
5. Prevención de ataques
6. Introducción al phishing

7. Phishing
8. Man in the middle

MÓDULO 2. HERRAMIENTAS DE CIBERSEGURIDAD OSINT

UNIDAD DIDÁCTICA 1. QUÉ SON LAS HERRAMIENTAS OSINT

1. Introducción

UNIDAD DIDÁCTICA 2. GOOGLE DORK

1. Qué es Google Dork
2. Uso y aplicación de Google Dork

UNIDAD DIDÁCTICA 3. SHODAN

1. Qué es Shodan
2. Uso y aplicación de Shodan

UNIDAD DIDÁCTICA 4. MALTEGO

1. Qué es Maltego
2. Uso y aplicación de Maltego

UNIDAD DIDÁCTICA 5. THE HARVESTER

1. Qué es The Harvester
2. Uso y aplicación de The Harvester

UNIDAD DIDÁCTICA 6. RECON-NG

1. Qué es Recon-ng
2. Uso y aplicación de Recon-ng

UNIDAD DIDÁCTICA 7. CREEPY

1. Qué es Creepy
2. Uso y aplicación de Creepy

UNIDAD DIDÁCTICA 8. FOCA

1. Qué es Foca
2. Uso y aplicación de Foca

MÓDULO 3. HERRAMIENTAS, TÉCNICAS DE CIBERSEGURIDAD Y

SISTEMAS SIEM

UNIDAD DIDÁCTICA 1. COMUNICACIONES SEGURAS: SEGURIDAD POR NIVELES

1. Seguridad a Nivel Físico
2. Seguridad a Nivel de Enlace
3. Seguridad a Nivel de Red
4. Seguridad a Nivel de Transporte
5. Seguridad a Nivel de Aplicación

UNIDAD DIDÁCTICA 2. CRIPTOGRAFÍA

1. Perspectiva histórica y objetivos de la criptografía
2. Teoría de la información
3. Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía
4. Criptografía de clave privada o simétrica
5. Criptografía de clave pública o asimétrica
6. Algoritmos criptográficos más utilizados
7. Funciones hash y los criterios para su utilización
8. Protocolos de intercambio de claves
9. Herramientas de cifrado

UNIDAD DIDÁCTICA 3. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

1. Identificación de los componentes de una PKI y sus modelos de relaciones
2. Autoridad de certificación y sus elementos
3. Política de certificado y declaración de prácticas de certificación (CPS)
4. Lista de certificados revocados (CRL)
5. Funcionamiento de las solicitudes de firma de certificados (CSR)
6. Infraestructuras de gestión de privilegios (PMI)
7. Campos de certificados de atributos
8. Aplicaciones que se apoyan en la existencia de una PKI

UNIDAD DIDÁCTICA 4. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1. Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
2. Identificación y caracterización de los datos de funcionamiento del sistema
3. Arquitecturas más frecuentes de los IDS
4. Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
5. Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

UNIDAD DIDÁCTICA 5. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

1. Análisis previo
2. Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3. Análisis de los eventos registrados por el IDS/IPS

4. Relación de los registros de auditoría del IDS/IPS
5. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 6. INTRODUCCIÓN A LOS SISTEMAS SIEM

1. ¿Qué es un SIEM?
2. Evolución de los sistemas SIEM: SIM, SEM y SIEM
3. Arquitectura de un sistema SIEM

UNIDAD DIDÁCTICA 7. CAPACIDADES DE LOS SISTEMAS SIEM

1. Problemas a solventar
2. Administración de logs
3. Regulaciones IT
4. Correlación de eventos
5. Soluciones SIEM en el mercado

MÓDULO 4. HACKING ÉTICO Y AUDITORÍA INFORMÁTICA

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN Y CONCEPTOS PREVIOS

1. ¿Qué es el hacking ético?
2. Aspectos legales del hacking ético
3. Perfiles del hacker ético

UNIDAD DIDÁCTICA 2. FASES DEL HACKING ÉTICO EN LOS ATAQUES A SISTEMAS Y REDES

1. Tipos de ataques
2. Herramientas de hacking ético
3. Tests de vulnerabilidades

UNIDAD DIDÁCTICA 3. FASES DEL HACKING ÉTICO EN LOS ATAQUES A REDES WIFI

1. Tipos de ataques
2. Herramientas de hacking ético
3. Tipos de seguridad WiFi
4. Sniffing

UNIDAD DIDÁCTICA 4. FASES DEL HACKING ÉTICO EN LOS ATAQUES WEB

1. Tipos de ataques
2. Herramientas de hacking ético
3. Tipos de seguridad web
4. Tipo de test de seguridad en entornos web

UNIDAD DIDÁCTICA 5. AUDITORÍA DE SEGURIDAD INFORMÁTICA

1. Criterios Generales
2. Aplicación de la normativa de protección de datos de carácter personal
3. Herramientas para la auditoría de sistemas
4. Descripción de los aspectos sobre cortafuego en auditorías de sistemas de información
5. Guías para la ejecución de las distintas fases de la auditoría de sistemas de información

MÓDULO 5. HACKING TRAINING PLATFORM

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A HACKING TRAINING PLATFORMS

1. ¿Qué es el hacking ético?
    1. - Diferencias entre hacker ético y malicioso
    2. - Tipos de hacking ético
    3. - Tipos de trabajos de hacking ético
2. Máquinas virtuales
    1. - Instalar VirtualBox
    2. - Instalar Kali Linux
3. Plataformas para practicar hacking ético

UNIDAD DIDÁCTICA 2. HACK THE BOX (HTB)

1. Introducción a Hack The Box
2. Crear una cuenta
3. Tutoriales

UNIDAD DIDÁCTICA 3. TRYHACKME

1. ¿Qué es TryHackMe?
2. Crear una cuenta
3. Interfaz de TryHackMe
4. Introducción a la ciberseguridad
5. Seguridad ofensiva
6. Ciencia forense digital

UNIDAD DIDÁCTICA 4. HACKER101

1. ¿Qué es Hacker101?
2. Hacker101 CTF
3. Tutoriales

UNIDAD DIDÁCTICA 5. VULNHUB

1. ¿Qué es Vulnhub?
    1. - Requisitos para utilizar Vulnhub
2. Interfaz de Vulnhub

3. Tutoriales
    1. - Ripper: 1 CTF, Vulnhub
    2. - Symfonos2 VulnHub
    3. - VulnHub - Zico 2 Walkthrough
    4. - DC-1:1 Vulnhub

UNIDAD DIDÁCTICA 6. HACK THIS SITE

1. ¿Qué es Hack This Suite?
2. Desafíos Hack This Site
    1. - Misiones básicas
    2. - Misiones realistas

UNIDAD DIDÁCTICA 7. GOOGLE XSS GAME

1. ¿Qué es Google XSS Game?
2. Niveles de Google XSS game
    1. - Nivel 1
    2. - Nivel 2
    3. - Nivel 3
    4. - Nivel 4
    5. - Nivel 5
    6. - Nivel 6

UNIDAD DIDÁCTICA 8. HACKTHIS

1. ¿Qué es HackThis?
    1. - Primer desafío
2. Tutorial HackThis
3. Basic+

MÓDULO 6. SEGURIDAD EN DESARROLLO WEB

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA SEGURIDAD WEB

1. ¿Qué es la seguridad web?
2. Amenazas para un sitio web
3. Consejos para mantener un sitio web seguro
4. Otros consejos de seguridad web
5. Proveedores de alojamiento web seguros

UNIDAD DIDÁCTICA 2. OWASP DEVELOPMENT

1. ¿Qué es OWASP? ¿Y OWASP Development?
2. ¿Qué es ASVS?
3. Uso del ASVS
4. Requisitos de arquitectura, diseño y modelado de amenazas

5. Requisitos de verificación de autenticación
6. Requisitos de verificación de gestión de sesión
7. Requisitos de verificación de control de acceso
8. Requisitos de validación, desinfección y verificación de la codificación
9. Requisitos de verificación de criptografía almacenados
10. Requisitos de manejo de verificaciones y registro de errores
11. Requisitos de verificación de protección de datos
12. Requisitos de verificación de comunicaciones
13. Requisitos de verificación de código malicioso
14. Requisitos de verificación de lógica de negocios
15. Requisitos de verificación de archivos y recursos
16. Requisitos de verificación de API y servicio web
17. Requisitos de verificación de configuración
18. Requisitos de verificación de Internet de las Cosas
19. Glosario de términos

UNIDAD DIDÁCTICA 3. OWASP TESTING GUIDE

1. Aspectos introductorios
2. La Guía de Pruebas de OWASP
3. El framework de pruebas de OWASP
4. Pruebas de seguridad de aplicaciones web
5. Reportes de las pruebas

UNIDAD DIDÁCTICA 4. OWASP CODE REVIEW

1. Aspectos introductorios
2. Revisión de código seguro
3. Metodología

UNIDAD DIDÁCTICA 5. OWASP TOP TEN

1. A1:2017 Inyección
2. A2:2017 Autenticación rota
3. A3:2017 Exposición de datos sensibles
4. A4:2017 Entidades externas XML (XXE)
5. A5:2017 Control de acceso roto
6. A6:2017 Mala configuración de seguridad
7. A7:2017 Cross-Site Scripting (XSS)
8. A8:2017 Deserialización insegura
9. A9:2017 Uso de componentes con vulnerabilidades conocidas
10. A10:2017 Insuficiente registro y monitoreo