UNIDA



DIPLOMADO EN

Desarrollo de Software Seguro

Becas otorgadas con el **financiamiento del MITIC**

GOBIERNO DEL PARAGUAY | MITIC

AGENDA DIGITAL



Fundamentación del Programa

El gran aumento del número de aplicaciones implementadas en el mercado a nivel mundial no ha hecho más que reforzar la necesidad de establecer un enfoque sólido para desarrollar aplicaciones y proteger datos: antes de iniciar la etapa de desarrollo, durante el desarrollo e incluso después de la publicación del software. Con este diplomado se busca contribuir a las personas y organizaciones a innovar de forma responsable, brindando un marco de conocimientos para la toma de decisiones que consideren los riesgos de ciberseguridad y equilibrar la velocidad y agilidad de la innovación con la seguridad y la resiliencia.

Este programa de capacitación abordará los desafíos y tendencias de la industria del desarrollo de software en lo que se refiere a la gestión de riesgos de seguridad. Se centrará principalmente en APIs y seguridad web. Se tomarán como referencia los recursos del Proyecto OWASP (WSTG, ASVS, Top Ten, Development Guide), organización referente a nivel mundial en desarrollo seguro.



Áreas abarcadas

Ciberseguridad

Es el eje principal del diplomado. Todo el programa gira en torno a la identificación, evaluación y mitigación de riesgos de seguridad en aplicaciones, tomando como referencia estándares y marcos como NIST SSDF, OWASP (WSTG, ASVS, Top Ten, Development Guide) y mejores prácticas de la industria. Se trabaja seguridad en APIs y aplicaciones web, gestión de vulnerabilidades y marcos normativos específicos de seguridad de la información.

Quality Assurance (QA) en TI:

Está estrechamente vinculado, ya que varios módulos abordan pruebas de seguridad en el SDLC (SAST, DAST, SCA), laboratorios prácticos y estudios de caso orientados a asegurar la calidad del software desde el punto de vista de la seguridad. El diplomado incorpora técnicas de testing, criterios de aceptación y prácticas de validación que forman parte del aseguramiento de calidad en TI.



Áreas abarcadas

Computación en la nube

De forma directa pero más focalizada en los contextos de despliegue, porque muchas de las aplicaciones y APIs que se analizan en el curso se ejecutan en entornos web y cloud. El enfoque en seguridad de aplicaciones web y gestión de riesgos resulta clave para proteger servicios expuestos en la nube, integrando buenas prácticas de configuración segura y protección de datos en estos entornos.

Infraestructura tecnológica

Se relaciona de manera complementaria, dado que el software seguro requiere una infraestructura robusta, correctamente configurada y monitoreada para mantener la confidencialidad, integridad y disponibilidad de la información. La gestión de riesgos, la cadena de suministro de software y la seguridad en el ciclo de vida implican necesariamente coordinar con la infraestructura subyacente.

Objetivos del Programa

Objetivo General

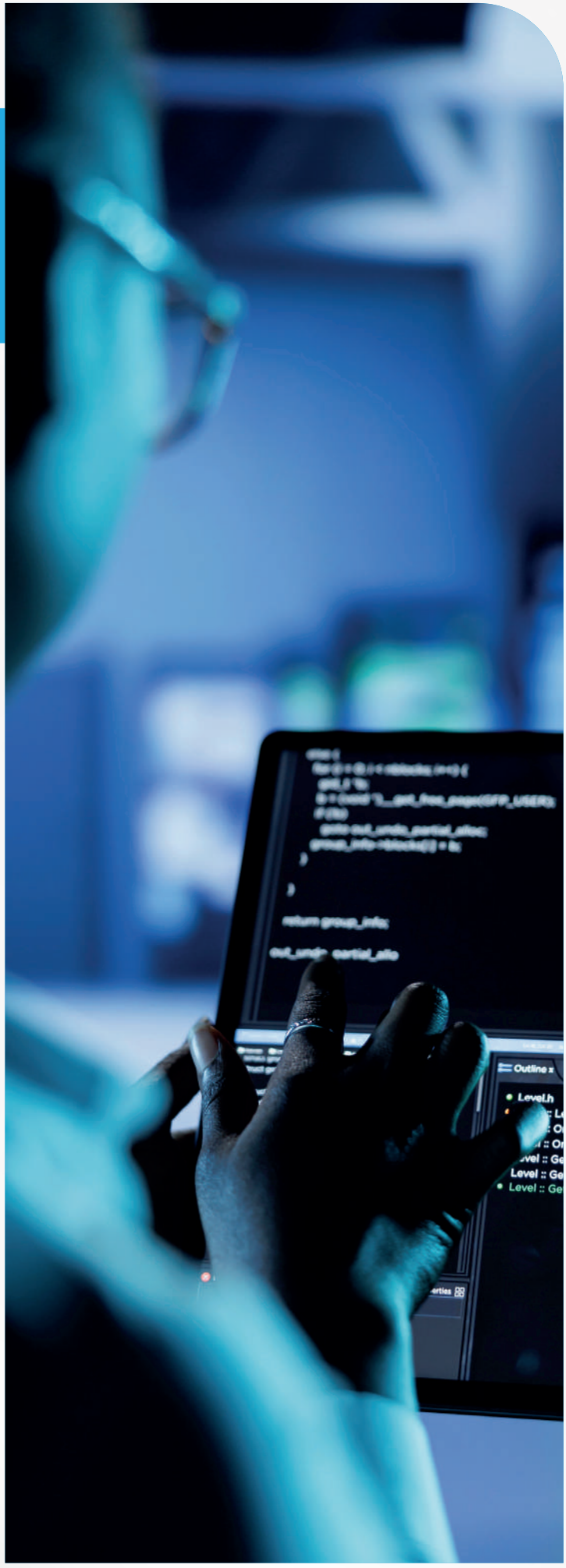
Desarrollar las competencias estratégicas y técnicas para diseñar, construir y gestionar software seguro, mediante la integración de la seguridad como un pilar fundamental en todo el ciclo de vida del desarrollo de software (SDLC) y el estudio de las prácticas técnicas y los marcos normativos de la industria con un enfoque proactivo de gestión de riesgos.

Objetivos Específicos

Adquirir conocimientos relacionados con marcos normativos, estándares principales y mejores prácticas de seguridad de aplicaciones y desarrollo de software seguro.

Vincular el análisis técnico de las vulnerabilidades más comunes con las metodologías formales de gestión de riesgos para su mitigación.

Comprender el papel de las herramientas de análisis de seguridad en el ciclo de vida del desarrollo de software (SAST, DAST, SCA).





Programa Académico

Módulo 1 - Desafíos de la Industria y Gestión de Riesgos

Estado del arte Risk Management | Mejores prácticas de la industria (NIST SSDF, SafeCode, OWASP)

Metodología: Clases Teóricas y Prácticas

Competencias específicas: Procesos estructurados de gestión de riesgos para evaluar, priorizar y comunicar riesgos de manera efectiva

Horas: 12 h

Módulo 2 - Security Testing (Web y API)

Vulnerabilidades más conocidas: escenarios de ataque, cómo prevenir

Metodología: Quiz inicial | Clases Teóricas y Prácticas

Competencias específicas: Reconocimiento de las vulnerabilidades más conocidas en la capa de aplicaciones

Horas: 36 h

Módulo 3 - Seguridad en SDLC

Pruebas estáticas, Pruebas Dinámicas, Gestión de Cadena de Suministro

Metodología: Quiz inicial | Clases Teóricas y Prácticas

Competencias específicas: Conocimiento de cómo se realizan pruebas de seguridad en todo el ciclo de vida de desarrollo de software

Horas: 27 h

Prueba Final - Taller Exposición grupal

Prueba final del Diplomado

Metodología: Taller final

Competencias específicas: Tormenta de ideas de proyectos a ser implementados. Trabajo práctico final.

Horas: 8 h



Detalles del Diplomado

Modalidad
En linea

Duración
4 meses

Clases
Martes y Jueves
19:00 a 21:00 h

Dirigido a: Estudiantes, Egresados y público interesado

Requisitos de Aprobación

- Alcanzar al menos el 70 % del puntaje total.
- Cumplir el 80 % de las actividades prácticas.
- Presentar y aprobar el Trabajo Final Integrador.
- Asistencia mínima del 70%.



Becas otorgadas con el financiamiento del **Ministerio de Tecnología de la Información y Comunicación (MITIC)**, en el marco del Programa de Apoyo a la Agenda Digital.

Inscríbete escaneando el QR

GOBIERNO DEL PARAGUAY | MITIC

AGENDA DIGITAL