UNIDA



DIPLOMADO EN

Ciberseguridad Aplicada a Entornos Corporativos

Becas otorgadas con el **financiamiento del MITIC**

GOBIERNO DEL PARAGUAY | MITIC

AGENDA DIGITAL



Fundamentación del Programa

La ciberseguridad se ha convertido en un pilar fundamental para la continuidad operativa, la protección de datos y la resiliencia digital de las organizaciones públicas y privadas. Ante el incremento de los ciberataques, la transformación digital y las exigencias normativas internacionales, este diplomado ofrece una formación integral orientada al desarrollo de competencias técnicas, estratégicas y normativas para la gestión de la seguridad de la información. El programa prepara profesionales capaces de implementar controles basados en marcos internacionales como ISO 27001, NIST Cybersecurity Framework y CIS Controls v8, alineados con las mejores prácticas en monitoreo, respuesta a incidentes, gestión de vulnerabilidades y cultura de ciberseguridad.

Desde una perspectiva de desarrollo sostenible, este curso se alinea con varios Objetivos de Desarrollo Sostenible (ODS):

- ODS 4 (Educación de Calidad): fomenta la capacitación en competencias digitales avanzadas mediante una formación virtual inclusiva.
- ODS 8 (Trabajo Decente y Crecimiento Económico): impulsa la empleabilidad en el sector tecnológico de alta demanda.
- ODS 9 (Industria, Innovación e Infraestructura): promueve la adopción de tecnologías emergentes para modernizar la infraestructura de las TIC.
- ODS 10 (Reducción de las Desigualdades): facilita el acceso equitativo a la educación tecnológica mediante la modalidad virtual, reduciendo las brechas territoriales y socioeconómicas.

En el contexto paraguayo, la pertinencia de esta formación es estratégica. El país se encuentra en un proceso de consolidación de su ecosistema digital y científico-tecnológico, impulsado por iniciativas de innovación, el fortalecimiento del capital humano y la transformación de los servicios públicos. Sin embargo, persisten desafíos en materia de infraestructura tecnológica, de talento digital y de la adopción de soluciones basadas en IA en instituciones públicas y privadas. Este curso responde a dichas necesidades, ofreciendo un espacio de formación que articula teoría, práctica y aplicación contextualizada, orientado a fortalecer las capacidades profesionales en tecnologías inteligentes y en computación en la nube.

En suma, este curso contribuye al desarrollo de talento humano altamente calificado, promueve la competitividad tecnológica y apoya los esfuerzos nacionales y regionales por consolidar una sociedad del conocimiento inclusiva, innovadora y sostenible.



Áreas abarcadas

Inteligencia Artificial (IA)

Es el eje central del diplomado, ya que todos los módulos abordan conceptos, técnicas y herramientas para diseñar, entrenar y desplegar modelos inteligentes (aprendizaje automático, redes neuronales, modelos de lenguaje, servicios de IA gestionados, MLOps, etc.).

Computación en la nube

Es la segunda área directamente relacionada, porque el programa se enfoca en el uso de plataformas cloud (AWS, Azure, Google Cloud) para crear, orquestar y escalar soluciones de IA, utilizando contenedores, servicios administrados y recursos virtualizados para el despliegue de modelos.



Áreas abarcadas



Infraestructura tecnológica

De forma complementaria, el diplomado se vincula con esta área en la medida en que enseña a planificar y utilizar infraestructuras robustas, virtualizadas y escalables (contenedores, Kubernetes, almacenamiento y redes) que soporten de manera segura y eficiente las cargas de trabajo de IA en la nube, garantizando su disponibilidad y rendimiento.

Objetivos del Programa

Objetivo General

Formar profesionales capaces de diseñar, implementar y gestionar estrategias de ciberseguridad en entornos corporativos, aplicando estándares internacionales y herramientas prácticas de defensa, monitoreo y respuesta ante incidentes.

Objetivos Específicos

Comprender los marcos de referencia y normas internacionales de seguridad.
Identificar, evaluar y mitigar riesgos y vulnerabilidades.
Configurar entornos seguros en redes, sistemas y servicios cloud.
Operar herramientas de monitoreo y SIEM en un entorno SOC.
Fomentar la cultura de ciberseguridad y cumplimiento normativo institucional.
Integrar conocimientos mediante el desarrollo de un proyecto final aplicable.





Programa Académico

Módulo 1 - Introducción, Gobernanza y Gestión de Riesgos

Conceptos básicos de ciberseguridad y riesgo; marcos ISO 27001/NIST; gestión y matriz de riesgos.

Metodología: Clases expositivas breves, análisis de casos y ejercicio de matriz de riesgos.

Competencias específicas: Comprende el rol estratégico de la ciberseguridad y aplica nociones básicas de gestión de riesgos.

Horas: 10 h

Módulo 2 - Redes, Protocolos y Seguridad Perimetral

Fundamentos de redes y protocolos; perímetro, segmentación, firewalls e IDS/IPS.

Metodología: Demostraciones con diagramas, laboratorio guiado y casos de arquitectura segura.

Competencias específicas: Reconoce componentes de red y propone configuraciones perimetrales más seguras.

Horas: 12 h

Módulo 3 - Sistemas Operativos y Hardening (Windows / Linux)

Seguridad en Windows/Linux; usuarios y permisos; hardening y gestión de parches.

Metodología: Laboratorios en máquinas virtuales con checklists de hardening.

Competencias específicas: Administra y refuerza la seguridad básica de servidores y estaciones de trabajo.

Horas: 12 h

Módulo 4 - SOC, SIEM y Monitorización de Seguridad

SOC y SIEM; monitoreo, correlación de eventos e incidentes de seguridad.

Metodología: Demostraciones de flujos, laboratorio en SIEM simulado y role-play de respuesta a incidentes.

Competencias específicas: Interpreta eventos de seguridad y participa en la respuesta a incidentes.

Horas: 12 h



Programa Académico

Módulo 5 – Gestión de Vulnerabilidades y Pentesting Básico

Gestión de vulnerabilidades; escaneo, priorización por riesgo e introducción al pentesting ético.

Metodología: Laboratorios de escaneo, análisis de reportes y mini-informe de vulnerabilidades.

Competencias específicas: Identifica, prioriza y propone remediación básica de vulnerabilidades.

Horas: 10 h

Módulo 6 – Gestión de Identidades y Accesos (IAM)

Identidad digital, IAM, directorios, modelos de control de acceso y MFA/SSO.

Metodología: Clases con diagramas, demostraciones de políticas de acceso y ejercicios de diseño de roles.

Competencias específicas: Aplica el principio de mínimo privilegio y configura accesos básicos basados en roles.

Horas: 8 h

Módulo 7 – Seguridad en la Nube y Enfoque DevSecOps

Modelos de nube, responsabilidades compartidas, riesgos cloud y enfoque DevSecOps.

Metodología: Ejemplos de arquitecturas cloud, laboratorio de configuración segura y análisis de pipeline CI/CD.

Competencias específicas: Reconoce riesgos en cloud y plantea controles y puntos de seguridad en el ciclo DevOps.

Horas: 10 h



Programa Académico

Módulo 8 – Seguridad de Aplicaciones y Desarrollo Seguro

Seguridad en el SDLC, OWASP Top 10 y pautas de codificación segura.

Metodología: Análisis de ejemplos de código, taller de identificación de vulnerabilidades y mitigación.

Competencias específicas: Identifica vulnerabilidades típicas y sugiere mejoras de desarrollo seguro.

Horas: 8 h

Módulo 9 – Cumplimiento Legal y Privacidad de la Información

Marco legal de protección de datos, privacidad y políticas internas de seguridad.

Metodología: Clases con casos de incumplimiento, debates éticos y revisión de políticas modelo.

Competencias específicas: Reconoce obligaciones legales básicas y contribuye al ajuste de políticas de seguridad y privacidad.

Horas: 8 h

Módulo 10 – Proyecto Final Integrador y Evaluación

Proyecto integrador: diagnóstico, propuesta de controles e informe ejecutivo/técnico

Metodología: Tutorías, trabajo autónomo y presentación/defensa del proyecto final.

Competencias específicas: Integra lo aprendido en un proyecto aplicable y lo comunica de forma clara y fundamentada.

Horas: 10 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 60 % del puntaje total.
- Cumplir el 80 % de las actividades prácticas.
- Presentar y aprobar el Trabajo Final Integrador.



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