

8ª EDICIÓN • ONLINE

Duración 6 meses

DIPLOMATURA *en* **Ciberseguridad**

INICIO: ABRIL 2026

✉ EDUCONTINUA@UBP.EDU.AR ☎ +54 9 351 3 881138

Evalúa escenarios de riesgo cibernético y mantén protegidas las organizaciones.

Fundamentos

El cibercrimen organizado representa un negocio rentable y estructurado, a niveles que difícilmente podamos creer.

En este entorno, las empresas, gobiernos y la sociedad misma, deben trabajar en conjunto no sólo en el desarrollo y adopción de tecnologías más seguras, sino también en la concientización del riesgo

en la población y en la creación de normas que redefinan una convivencia segura en los años por venir.

Hoy es necesario contar con profesionales con conocimientos avanzados en ciberseguridad que entiendan este escenario y que cuenten con las habilidades para proteger sus organizaciones.



CERTIFICACIÓN DIGITAL CON
TECNOLOGÍA BLOCKCHAIN

LA DIPLOMATURA CUENTA CON CERTIFICACIÓN DIGITAL A TRAVÉS DE LA TECNOLOGÍA BLOCKCHAIN MEDIANTE EL FORMATO NFTS. ESTOS SON IMPOSIBLES DE FALSIFICAR O MODIFICAR, FÁCILES DE COMPARTIR Y VERIFICAR; ECOLÓGICOS Y MANTIENEN LA PRIVACIDAD DE LOS DATOS DEL RECEPTOR.

Objetivos

- Comprender el comportamiento de las amenazas y de los ciberdelincuentes, desarrollando competencias para asistir y asesorar sobre cómo definir, desarrollar y mantener un escenario seguro.
- Obtener una sólida formación en los conceptos fundamentales de la Ciberseguridad, y la capacidad de aplicarlos en su ámbito profesional, independientemente de los productos o tecnologías informáticas con que se encuentren en sus roles profesionales ahora y en el futuro.
- Reconocer los elementos instrumentales y metodológicos para comprender la Norma ISO 27001 de Seguridad de la Información.
- Entender las diferencias y campos de aplicación de Seguridad Informática, Seguridad de la Información y Ciberseguridad, reconociendo escenarios con problemas de Ciberseguridad y aplicando el modelo de Defensa en Profundidad para mitigar sus fallos.
- Definir la arquitectura de escenarios seguros en la nube y on-premises; confeccionar y llevar a la práctica un Gap Analysis de Ciberseguridad de organizaciones, aprendiendo a tratar la información generada por diferentes fuentes de datos y protegerla, además de obtener información en situaciones críticas.
- Saber cómo reaccionar ante una infección de Ransomware y mitigar el problema.



Dirigida a:

- Alumnos avanzados y egresados de carreras de informática, telecomunicaciones, desarrollo de software, programación.
- Personas con responsabilidades en seguridad de la información tales como: ciosCIO, cisosCISO, Gerentes de IT. Responsables de áreas de Seguridad Informática, Seguridad de la Información y personas que tomen decisiones en aspectos de Ciberseguridad en las organizaciones.

Modalidad ONLINE



Programa · Módulos

1

INTRODUCCIÓN A LA CIBERSEGURIDAD - MARCO NORMATIVO

Introducción a la Seguridad Informática. Conceptos y objetivos de la Seguridad de la Información. Conceptos de información, riesgo, amenaza, vulnerabilidades, impacto, intrusos, objetivos y alcances.

Situación actual en las empresas. Organización de la Norma iso 27001. Objetivos de control.

Repaso de los diferentes dominios. Acceso a la información por parte de terceros.

¿Quién es pii? Definición – Preocupación mundial del dato del tercero. Aspectos legales en la protección de datos personales. Ej gdpr. Parámetros de contratos de trabajo. nda.

2

HACIA UNA CIBERSEGURIDAD PROACTIVA

La Ciberseguridad en tres dimensiones. Conceptos y de definiciones de Seguridad y Ciberseguridad.,Cifrado, Backups y Clasificación. Ciberinteligencia. Evolución de la Inteligencia. Ciberamenazas, ciberinteligencia de la amenaza y contra ciberinteligencia. Ciberdefensa en pocas palabras. Ciberdefensa Proactiva. Por aire, tierra y mar: Ahora en el Ciberespacio. Ciberamenazas. Panorama actual de amenazas y principales vectores de ataque. Decálogo de Recomendaciones de Ciberseguridad.

3

DEFENSA EN PROFUNDIDAD

Modelos de Defensa en Profundidad y Confianza Cero. Ingeniería social. Técnicas y herramientas de Inteligencia: OSINT. Introducción a análisis forense. Peritaje informático forense. Modelo NIST como soporte en asesoría. Práctica en el armado de tableros de control.

4

CIBERSEGURIDAD EN LA NUBE

¿Seguridad en la Nube, nuevo paradigma? Revisión de conceptos de tipo de nube. Implementación de seguridad en la nube. Cloud Security Alliance (csa). Aspectos de seguridad a tener en cuenta en la nube.Modelo de Defensa en Profundidad en la Nube. Exigencias de cumplimiento en la nube: rgdp, pci, hipaa, otros. Estrategias nacionales de ciberseguridad. Otras leyes u Organismos. (nist, oea, incibie, etc.)



ACREDITA
200 H



6 MÓDULOS

Programa · Módulos

5

LA INTELIGENCIA EN LA CIBERSEGURIDAD

Concepto de CERT y de CSIRT.

El Análisis de Inteligencia Técnicas de organización de la información adquirida. Metodologías de Análisis. Inteligencia Artificial brindando valor agregado a la Ciberseguridad.

Presentación de los Resultados de la Inteligencia. Gobierno de la Seguridad de la Información
Objetivos de control. KPI.

Definición del Plan Estratégico. Valor de la información. Activos de la organización. Entender las necesidades de los procesos de negocio. Protección de Activos de Información.

Implementar un Gap Analysis de Ciberseguridad.

6

CIBERRESILIENCIA

Evaluación esporádica de la infraestructura y datos. Equipos de Red Team y Blue Team. Conformando equipos de Red y Blue Team. Trabajo interdisciplinario. Aspectos de implementación. Concientizar a la Dirección. Concientizar a los usuarios. Ransomware, el peor enemigo. Buenas prácticas para prevenir ataques de Ransomware. Respondiendo a incidentes de Ransomware. Forensia.



Cuerpo docente



ESTEBAN PRÓSPERO • Director

Mgter. Ejecutivo en Administración de Empresas (EMBA, IAE BUSINESS SCHOOL) • Ing. Electrónico (UBA) • Ejecutivo de tecnología con 25 años de experiencia en el desarrollo de productos de software para el mercado global • Se desempeñó en puestos de liderazgo en empresas multinacionales de los sectores de las telecomunicaciones, las tecnologías de la información y la ciberseguridad • Responsable de liderar la ingeniería de productos de ciberseguridad para empresas Global 2000 • Asesor y consejero de empresas en ciberseguridad y estrategia de producto y organizacional



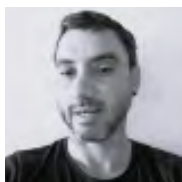
DANIEL BAQUER

Ingeniero en Sistemas (UCC) • Perito Informático, ESAPI (CPCIPC) • Diplomado en Ciberseguridad (UBP) y Derecho y Tecnología (UBP) • Es Jefe Infraestructura y Seguridad de la Información en V-N Global y Partner CIO en Austral Technology • Se desempeñó como CISO en Grupo Libertad, IT Manager en Conci Carpinella y en Universidad Siglo 21.



PABLO MASJOAN

Ingeniero en Sistemas de Información (UTN) • Diplomado en Gestión de Ciberseguridad (UCEMA) • Más de 20 años de trayectoria en empresas de infraestructura crítica, telecomunicaciones, y tecnología • Fue CISO en la Fábrica Argentina de Aviones. Actualmente lidera la Jefatura de Cumplimiento y Gestión de Seguridad en Claro Argentina, Uruguay y Paraguay.



MAXIMILIANO LUZURIAGA VIVOT

Especialista en Gestión de Seguridad de la información con experiencia en implementación y mantenimiento de Sistemas de Gestión de Seguridad de la Información (SGSI) asegurando el cumplimiento de estándares internacionales (ISO 27001, PCI DSS,) en la protección de activos críticos • Con sólida trayectoria en la coordinación de equipos de trabajo interdisciplinarios, para alcanzar objetivos estratégicos de seguridad, eficiencia y continuidad operativa • Actualmente es parte del equipo de Data Privacy and AI engineering en NaranjaX.



LEONARDO FRITTELLI

Mgter. en Ingeniería de Software e Ingeniería del Conocimiento (UPM MADRID) • Lic. en Informática (UBP) • Es Arquitecto de Software para MuleSoft (Salesforce) • Ha desarrollado softwares en diversas industrias y empresas como Motorola, Globant, eBookers/Orbitz, Bank of America, e Intel/McAfee, en desarrollo de soluciones para grandes clientes corporativos y también consumidores finales • Participó en la concepción técnica e implementación de software de ciberseguridad corporativa para clientes de la compañía McAfee.



JUAN CARLOS CASALE

Máster Dirección Estratégica en Tecnología de la Información, Dirección Estratégica y TIC; Dirección Estratégica y Empresas de Software / Telecomunicaciones (UNIVERSIDAD EUROPEA MIGUEL DE CERVANTES) • Analista de Sistemas de Computación-Informática (IES) • Esp. en Seguridad, Auditoría y Peritaje Informático (CPCIPC Córdoba) • Gerente de Innovación en Vertical S.A • Se desempeña como Profesor de Hardware, Programación, Recursos Informáticos en Colegio Universitario IES.



MARCELO CUADRADO

Ingeniero en Software (UNICEN) • MBA con especialización en startups y emprendimientos (UCEMA) • Gerente de tecnología con más de 20 años de experiencia liderando equipos de ingeniería y desarrollo de productos de software para mercados globales • Ha ocupado posiciones de liderazgo en empresas multinacionales de los sectores de ciberseguridad e inteligencia artificial • Fue responsable de productos críticos como soluciones de protección, detección y respuesta para endpoints (EDR), seguridad en correos electrónicos, y orquestación en la nube • Actualmente lidera equipos de desarrollo de productos de seguridad en Proofpoint, protegiendo a empresas globales frente a amenazas avanzadas.





Impulsá tu formación

Realizá tu inscripción

Completá tus datos y aboná la matrícula en pocos pasos

Aranceles y formas de pago

Beneficios

**ESTUDIANTES Y
GRADUADOS/AS UBP**

→ 20% OFF

**2 O MÁS PERSONAS
DE UNA ORGANIZACIÓN**

→ 15% OFF

NOTAS

- Los beneficios especiales **no se acumulan**, el destinatario puede elegir el de mayor conveniencia. Sobre los aranceles a pagar, el estudiante puede optar por las diferentes formas de pago, algunas de las cuales tienen **descuentos adicionales**.
- Los beneficios se consideran **sobre los aranceles** (excluyendo la matrícula).
- Según corresponda, los interesados deben **presentar la documentación respaldatoria**, por ejemplo: certificado laboral, constancia matrícula, nota de la institución/empresa a la que pertenece, etc.



Saber y Saber Hacer

Desde 1990, la Universidad Blas Pascal acompaña a profesionales en su desarrollo personal y laboral, combinando conocimientos sólidos con habilidades prácticas. Con **35 años de trayectoria** y **25 años en educación a distancia**, ofrece formación académica a estudiantes de todo el país. Cuenta con **170 centros de educación a distancia**, garantizando acceso amplio y de calidad.

La Universidad forma profesionales capaces de aplicar lo aprendido de manera ética, creativa e innovadora, generando valor en sus organizaciones y en la sociedad. Desde 2009, muchas de sus áreas cuentan con certificación **ISO 9001**, asegurando calidad y rigor académico.

Además, a través de la **Córdoba Management School**, la **Digital Skills Academy** y la **Soft Skills Academy**, la UBP brinda programas especializados que desarrollan competencias técnicas, digitales y humanas, acompañando al profesional en cada etapa de su crecimiento.

En la UBP, la educación continua está pensada para acompañar a cada profesional a aprender, crecer y transformar su entorno.

Educación Continua

70 DIPLOMATURAS

3500 ALUMNOS ANUALES

+20 CAPACITACIONES INCOMPANY CADA AÑO

MODALIDAD VIRTUAL ASINCRÓNICA, FLEXIBLE Y PENSADA PARA PROFESIONALES





UNIVERSIDAD Blas Pascal



Saber y Saber Hacer

INFORMES

WHATSAPP +54 9 351 3 881138

0054 0810 1 22 33 827

Opción 2

educontinua@ubp.edu.ar

REDES

www.ubp.edu.ar

📍 Educación ContinuaUBP

📧 ubp.educacioncontinua

📍 Cordoba-Management-School

CAMPUS

Av. Donato Álvarez 380

CPA X5147ERG

Córdoba, Argentina