UNIVERSIDAD DE Belgrano
BUENOS AIRES - ARGENTINA

DEPARTAMENTO ESTUDIOS DE DE POSGRADO Y EDUCACIÓN CONTINUA

FACULTAD DE INGENIERÍA Y TECNOLOGÍA INFORMÁTICA

EDUCACIÓN CONTINUA

CICLO 2020

DIPLOMATURA EN CERTIFIED CYBER DEFENSE OFFICER (CCDO) - CYBERDEFENSA

BREVE INTRODUCCIÓN

La era de la Información y de las tecnologías en las que vivimos inmersos necesitan un nuevo soporte y paradigma. Ello requiere de especialistas altamente calificados para poder prevenir ataques cibernéticos que afecten las infraestructuras críticas de un Estado, de un Gobierno o de una Organización.
En EE.UU, en los países del Este y en Asia, y en OTAN es requerida esta certificación que hoy la Universidad de Belgrano la ha desarrollado para brindarla a quienes estén interesados.

Este programa está orientado a todas aquellas personas que deseen profundizar los conocimientos sobre el tratamiento de la Cyber-Defense y Certificar para asumir el rol de Manager en la especialidad. Esta disciplina, cada día más vigente y necesaria, requiere de expertos en diversas áreas públicas o privadas, que prevean y mitiguen posibles amenazas que interfieran en las operaciones diarias de trabajo y eviten –entre otras acciones no deseadas- fugas de Información. Wikileaks, Snowden, Vaticano-leaks, Fifa Gate, Panamá Papers, son sólo algunas de las secuelas de una débil administración de los datos, con imponderables consecuencias.

OBJETIVOS

Formar especialistas en Cyber-Defense a fin de brindarles una especialidad concreta de manera dinámica en este área, además de un conocimiento y de un lenguaje particular que les permita acceder a trabajar con las más altas autoridades a fin de procurar una hegemonía sólida que asegure la protección de los activos y que facilite la prosecución de los fines estratégicos de cualquier Organización, Estado o Gobierno.

PERFIL DEL ESTUDIANTE

Directores y decisores de las áreas de Auditoría, Control Interno, Gerentes de áreas críticas: Legales, Recursos Humanos, Seguridad de la Información, Compliance, Consultores y toda persona con funciones de contralor de la Industria Financiera, de la Salud, Gobierno o Corporación. Asimismo será de utilidad para los CEOs, CIOs, CFOs, y demás Gerentes de áreas críticas que deseen conocer las amenazas a los que enfrenta una Organización ante las tecnologías emergentes y las bandas cada vez más sofisticadas de delincuentes.

CARACTERÍSTICAS DEL CURSO Y METODOLOGÍA

Presencial con prácticas informáticas. Trabajos en grupo para evaluación final.

PROGRAMA DE ESTUDIO

MÓDULO 1: GOBIERNO, GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN

Marco y Gestión de la Seguridad de la Información. Maniobras en el Ciberespacio. Modelando el ciberespacio para su Comprensión. Clasificación de Información.

MÓDULO 2: ESTRATEGIA DE CIBER-SEGURIDAD – ROLES Y FUNCIONES

La estrategia de Cyber seguridad, no trata únicamente los aspectos tecnológicos, sino que también abarca el tema económico, político y de Factor Humano. Su comprensión y comunicación, la integración de equipos de tareas y definir Roles y funciones de cada uno de ellos.

MÓDULO 3: GESTIÓN Y EVALUACIÓN DE RIESGOS

Una efectiva práctica de administración de riesgos incluye aspectos de administración de sistemas, seguridad en red, seguridad de aplicaciones, administración de accesos, protección de datos, criptografía y Análisis de Impacto entre otros.

MÓDULO 4: AMENAZAS Y ANÁLISIS DE VULNERABILIDADES

El ciberespacio es un medio para la materialización de nuevos riesgos y amenazas. Su fácil accesibilidad hace que cada vez sean más comunes y preocupantes las intromisiones en este ámbito. Los ciberataques, en sus diversas modalidades de ciberdelito, ciberterrorismo, ciberespionaje o activismo en la red, se han convertido en un potente instrumento de agresión contra particulares e instituciones públicas y privadas.

MÓDULO 5: C-SIRT

El equipo de respuesta a Incidentes es clave para garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a Incientes como así también se debe desarrollar y mantener actualizadas las instrucciones de prevención y detección, incluyendo procedimientos de respuesta frente a situaciones de crisis y planes de contingencia específicos ante esta situación

MÓDULO 6: ANÁLISIS FORENSE Y AUDITORÍA

La evaluación de una correcta implementación de seguridad requiere monitoreo y auditorías permanentes. Los procesos, las tecnologías y las personas están presentes en el proceso de control como así también, las herramientas Forenses necesarias para establecer patrones de comportamientos sobre ataques nuestras estructuras críticas o activos de información.

MÓDULO 7: LEGISLACIONES, REGULACIONES Y CUMPLIMIENTO NORMATIVO

¿Para que una civilización funcione debe contar con normas para que se haga un uso adecuado y funcione sin afectar nuestros derechos, permitiendo la convivencia segura. Para ello se trabaja dinámicamente en leyes, regulaciones y normativas que aseguren este ámbito tan vertiginoso y cambiante que es el Cyber espacio.

MÓDULO 8: EJERCICIOS PRÁCTICOS (CDX - TALLER) “EL PROFESOR VIVE ENSEÑANDO Y EL MAESTRO ENSEÑA VIVIENDO”

Estos ejercicios proveerán una dinámica y conocimientos mínimos necesarios basados en simulaciones de ataques e intentos de penetración de la vida real.

DIRECTOR ACADÉMICO

LIC. GABRIEL BARBEITO

Director de Defense Technointelligence Office, Past Country Chief Information Security Officer de Citibank y Subsidiarias.
Ha trabajado como Auditor en el Corporate Audit - 111 Wall Street, NY y colaborado en el desarrollo de la Oficina de Emergencias y Respuesta ante Fraudes y Ataques a las bases de datos del conglomerado financiero del grupo. Junto con el cuerpo de Corporate Audit ha implementado soluciones y estrategias a fin de preservar los activos financieros de la Compañía y sus Subsidiarias.
Líder de Proyecto de Seguridad y Control Asian-Pacific Region, con sede en Bankok, Thailandia y LATAM.
Líder del programa “Entrenando a Entrenadores” para Latinoamérica.
Líder Regional del Security Incident Response Team.
A través de Citigroup ha realizado los cursos de Harvard sobre Liderazgo, Ciencias Políticas y People Management y Business to Business, Darden, USA.
Representó las legislaciones americanas en la comunidad de Interbanking, con sede local y alcance para la totalidad de la comunidad bancaria del país. Asimismo, ha

contribuido con varias entidades bancarias de LATAM y otras regiones del extranjero, en el alineamiento para implementar las mejores prácticas de la industria.
Profesor de posgrado en la Universidad de Buenos Aires en la cátedra “Auditoría Forense”.
Profesor titular de Posgrado en la Universidad del Salvador, Director de Posgrado de Management en las Funciones de Control y Auditoría en la Universidad CAECE, Argentina. Ha sido expositor en importantes congresos de USA, LATAM y Argentina Congreso Internacional de Auditoría, FELABAN (Federación Latam de Bancos), FLAI (Federación Latam de Auditores Internos), IIA, CLAI (Congreso Latinoamericano de Auditoría Interna), ABA (Asociación de Bancos de la República Argentina), Escuela Superior de Guerra, Escuela Superior del Ejército, CXO Community (Jornadas sobre Cyber-terrorismo), Cumbre Anti Fraude, (Lima), etc.
Licenciado en Sistemas de la Información, Analista de Inteligencia Estratégica (Escuela Superior de Guerra), Posgrado en Marketing Estratégico y certificado en USA como CISM, (Certified Information Security Officer), CGEIT (Global Enterprice Information Technology) y CIFI (Certified Information Forensic Investigator).
Distinguido en el año 2012 por AFCEA (Armed Forces Communication Electronic Association) en reconocimiento por haber coordinado los primeros juegos de defensa Cibernética fuera de los EEUU.
Miembro de EDP Auditor Association, USA.

PROFESORES INVITADOS COMO EXPOSITORES CICLO 2018

EDUARDO MARTINO

Jefe de Gabinete de Asesores - Secretaría de País Digital - Ministerio de Modernización

CARLOS FEDERICO AMAYA

Ingeniero - Investigador en UNDEF

PABLO LÁZARO

Ingeniero – Ministerio de Seguridad de la R.A.

DEREK WONG

Agregado Económico de la U.S.Embassy, Argentina

GABRIEL SAKATA

CISCO - Gerente General

MARCELO TRIVIÑO

IBM – Especialista en Cyber-security

PROFESORES TITULARES CICLO 2018/2019:

JUAN BOSOMS

Consultor e instructor en Seguridad de la Información.
Tiene 36 años de experiencia en varias empresas nacionales e internacionales. Desempeñó varias jefaturas en distintas gerencias de sistemas de las cuales la mayoría son específicamente en Gerencias de Seguridad de la Información. Actualmente se desempeña como Jefe del CSIRT de un importante banco Nacional de capitales privados y como consultor e instructor en arquitecturas de seguridad, Ethical Hacking y Pentesting.

OSCAR MAIOLA

Contador Público Nacional - Doctor en Ciencias Económicas de la UBA - Certificaciones internacionales: CIA – CFE – CRMA – QAR
Profesional en gestión de riesgos y fraude. Desempeñándose en el Grupo Shell, donde ocupó diversos puestos a nivel local y regional relativos a su especialidad. Fue síndico y auditor externo de Sociedades Anónimas.

EDUARDO ROSENDE

Especialista en Derecho Penal por la Facultad de Derecho de la Universidad Nacional de Buenos Aires y actualmente doctorando en Derecho por la primera institución citada. Se ha desempeñado desde el año 1999 en el Ministerio Público Fiscal y, en el año 2015, fue designado fiscal titular de la Fiscalía Nacional en lo Criminal y Correccional de Instrucción n° 48 de la Capital Federal. Profesor de la Escuela de Capacitación del Ministerio Público Fiscal.

MATIAS SLIAFERTAS

Especialista con más de 10 años de experiencia en Information Security y Cybersecurity. Actualmente se desempeña como Vice President en el J.P. Morgan Chase, Cybersecurity & Technology Controls para la region LATAM&Canadá . Académicamente, se ha formado –entre otras Universidades- en USAL (University del Salvador), UAI (University Abierta Interamericana), University of Maryland y MIT (Massachusetts Intitute of Technology). Tambien cuenta con certificaciones como CISM y ISO27001 Lead Auditor.

Los módulos podrán ser dictados por todos o algunos de los docentes mencionados en forma indistinta. La Universidad se reserva el derecho de realizar cambios en el cuerpo docente que considere pertinentes.

CONSIDERACIONES GENERALES

INICIO

Mayo de 2020

FINALIZACIÓN

Diciembre de 2020

DURACIÓN

El curso completo tiene una duración de 105 horas reloj, desarrolladas de acuerdo a la siguiente modalidad:

- 7 materias de 12 h. Promedio cada una (84 h. De cursadas)
- Hora por examen de cada materia= 1 (total 7 h.)
- Ejercicio – taller = 14 h.

DÍAS Y HORARIOS

Una clase por semana de 3 h. (miércoles de 19 a 22 h.)

SEDE DE DICTADO

Departamento de Estudios de Posgrado y Educación Continua. Tucumán 1489, CABA.

ASISTENCIA MÍNIMA

75 % de las clases.

MATERIAL DIDÁCTICO

Se dará material de referencia en base a lo cursado y adicionalmente, recomendaciones para investigación.

APROBACIÓN

Examen Múltiple Choice y trabajo práctico.

CERTIFICACIÓN

La Universidad de Belgrano, extenderá el respectivo Certificado, a quienes aprueben el trabajo final y cumplan con la asistencia mínima requerida. A aquellos alumnos que posean título de grado se les otorgará certificado de aprobación de la Diplomatura; a aquellos alumnos que no cumplan con dicho requisito se les entregará certificado de aprobación de Curso de Actualización Profesional.

Todos nuestros programas deberán contar con un cupo mínimo de alumnos matriculados para su apertura. En caso de no reunir el número indicado al cierre de inscripción, la Universidad se reserva el derecho de posponer o suspender el inicio de la actividad.