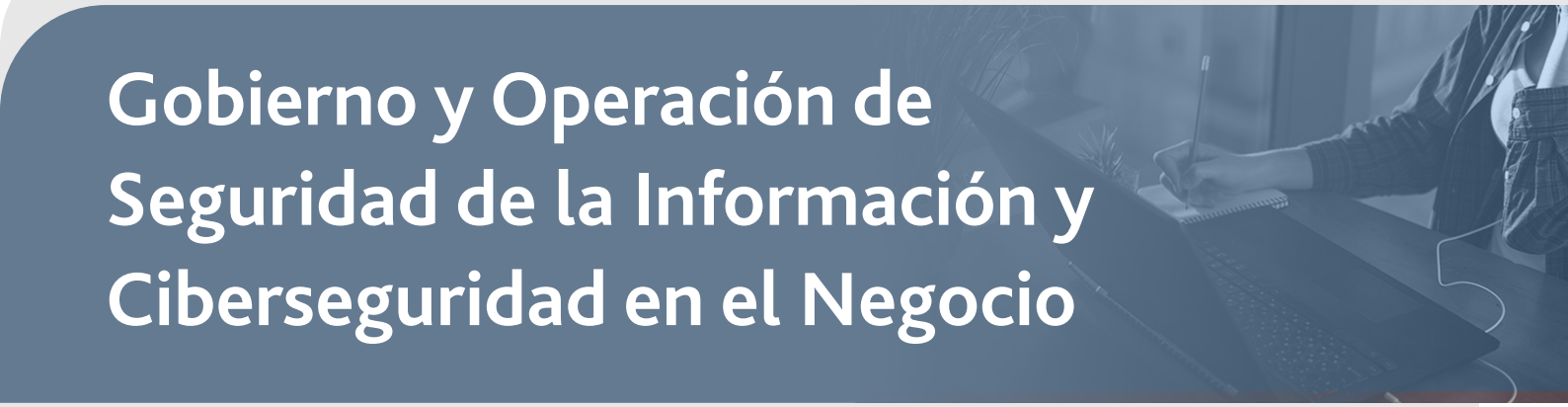
◦ Curso de especialización

Gobierno y Operación de Seguridad de la Información y Ciberseguridad en el Negocio



Duración
5 encuentros de 2 horas c/u (total 10hs)

Plataforma:
Microsoft Teams

Objetivo

Brindar a los participantes los principales conceptos y orientación sobre la relación entre la seguridad de la información y la ciberseguridad, y su importancia para un gobierno estratégico de su negocio.

POWERED BY BDO Academy

Módulos

Módulo de aseguramiento de objetivos del plan de negocio

- Relación de la seguridad de la información con el negocio
- Definiciones y alcances de la seguridad de la información y ciberseguridad
- Relación en el framework normativo ISO/IEC 27001, ISO/IEC 27701 e ISO/IEC 27032
- Análisis de contexto organizacional para la seguridad de la información y ciberseguridad
- Enfoque de negocio para la innovación y transformación digital segura (confianza digital)
- Aspectos de estrategia corporativa (negocio y mercado)
- Aspectos de estrategia de cumplimiento
- Aspectos de estrategia tecnológica
- Planificación estratégica para el gobierno tecnológico
- Plan de negocios / Plan de IT / Plan de seguridad de la información y ciberseguridad
- Ciberseguridad en la gestión de riesgos corporativos y tecnológicos
- Ciberseguridad en la gestión de incidentes corporativos
- Control del gobierno corporativo en seguridad de la información y ciberseguridad
- Seguridad de la Información/Ciberseguridad y la 2da línea de defensa
- Auditoría y controles de seguridad de la información y ciberseguridad
- Continuidad del negocio y su relación con la seguridad de la información y ciberseguridad
- Economía de la seguridad de la información
- ROSI – Modelo económico de la seguridad de la información
- Definición estratégica del área de seguridad de la información y ciberseguridad
- Indicadores de gestión y métricas en procesos de servicios de seguridad de la información y ciberseguridad

Dirigido a:

A los CEOs, CIOs, CISOs, CFOs, Directores, Gerentes y Jefes de áreas de negocio, Gerentes y Jefes de áreas tecnológicas, Técnicos administradores de servicios tecnológicos y de ciberseguridad

Módulo Técnico/Práctico

I.CIBERSEGURIDAD
- Presentación de las principales prácticas de ataques de hackers y las consecuencias sociales de dichos ataques.
- Introducción al Ethical Hacking.
- Ciberseguridad: tendencias actuales

II. CONCEPTOS GENERALES
- Estructuras y elementos de redes y comunicaciones
- Zonas seguras / DMZs
- Firewalls, routers, switches
- Concepto de pentest: interno, externo, de aplicaciones. Black, grey y White box

III. CIBERATAQUES
- Estrategias y consideraciones generales de los Cyber ataques
- Motivos
- Organizaciones
- Tipos de ataques; robo de información, DDOS, phishing, hacktivismo

IV. SEGURIDAD EN REDES SOCIALES
- Redes sociales
- Confidencialidad y cuidados. (Información corporativa personal expuesta)
- Grooming
- Ingeniería social

Equipo docente

Fabián Descalzo
BDO en Argentina | Socio

Fabián posee 30 años de experiencia en el área de gestión e implementación de Gobierno de Seguridad de la Información, Gobierno de TI, Compliance y Auditoría de TI en Argentina y Latinoamérica, y asesoramiento para el cumplimiento de Leyes y Normativas Nacionales e Internacionales en compañías de primer nivel de diferentes áreas de negocio. Es docente universitario de gobierno tecnológico, seguridad de la información y ciberseguridad en el Instituto Tecnológico Buenos Aires (ITBA), la Universidad Nacional de Río Negro y la Universidad Argentina de la Empresa (UADE). Es docente para la auditoría e implementación de normas de certificación ISO para TÜV Rheinland Argentina, y Miembro del Comité Directivo de ISACA Buenos Aires Chapter, Miembro del Comité Directivo del "Cyber Security for Critical Assets LATAM" para Qatalys Global y Miembro del Comité Científico del IEEE (Institute of Electrical and Electronics Engineers) y poseedor de múltiples certificaciones en la temática.

Matías Srur
Ethical Hacker, Consultor en Ciberseguridad y Forensia

PERFIL & ESPECIALIZACIÓN
- Gestión de seguridad de la información
- Hacking ético
- Ciberseguridad
- Forense Digital
- Red Team
- Blue Team

OTROS ANTECEDENTES
- Funciones desempeñadas en el área de Ciberseguridad:
- Análisis técnico de plataformas
- Ethical Hacker y Forense Digital
- Implementador y administrador de soluciones de software para servicios gestionados
- Diseñador de bootcamp para la práctica y análisis de ataques de ciberseguridad
- Investigador y analista de ciberseguridad
- Instructor técnico de ciberseguridad

EDUCACION
- Diplomatura en Seguridad de la información en la Universidad Tecnológica Nacional (2020)
- Programador Web Avanzado Fullstack certificado en la Universidad Tecnológica Nacional (2019)

CERTIFICACIONES
- Certificado internacional en "Cyber Security Foundation Professional Certificate (CSFPC)"
- Ciberseguridad en el desarrollo seguro de proyectos tecnológicos (BDO ACADEMY)

Material de apoyo:

Los participantes recibirán individualmente acceso a nuestro campus virtual para acceder al contenido del curso.

Examen:

El último día se tomará un examen online de 1 hora de duración, que será elaborado y corregido por el docente. La modalidad del examen es online y mediante 20 preguntas con selección de respuesta (multiple-choice)

Certificado:

Aquellos participantes que superen con éxito el examen (75% de preguntas con respuestas correctas) recibirán certificado de aprobación. Caso contrario recibirán certificado de asistencia.

Modalidad Aula virtual:

Las capacitaciones en aula virtual se llevan a cabo como un curso normal en un aula y a una hora fija programada. Sin embargo, es flexible en cuanto a la ubicación y puede participar en línea desde cualquier lugar. Con la ayuda de una herramienta (Pc, Notebook, Tablet), los participantes y docente están conectados en un aula virtual. La ventaja del aula virtual es que puede hacerle preguntas al docente o debatir con los demás participantes, de forma similar a una formación clásica en el aula.

Hemos resumido todos nuestros cursos de formación en digital para usted, consulte por cursos In Company con esta modalidad.

Infraestructura:

Pc, Notebook o Tablet con una conexión a Internet estable y auriculares.