



DIG1CAB

**Comisión de
Transformación Digital**

**Ilustre Colegio de la
Abogacía de Barcelona**





DIGICAB

**INICIACIÓN EN LA
CIBERSEGURIDAD PARA
PROFESIONALES DE LA
ABOGACÍA**

**18, 20, 25 y 27 de febrero
de 2020**





DIGICAB



Iniciación en la Ciberseguridad para Profesionales de la Abogacía

Objetivo de la formación:

Dar una primera visión sobre el mundo de la ciberseguridad, proporcionando nociones básicas en este tema, y aspectos tales como gobernanza de la ciberseguridad, como protegernos ante amenazas, cultura de la seguridad de la información, y normas y buenas prácticas internacionales de la gestión de la seguridad informática.

Dirigido a:

Abogados y Abogadas que, por diferentes motivos profesionales, tengan interés en iniciarse en el campo de la ciberseguridad

PONENTE

- Ramiro Cid (IT security officer a Linde Group)



DIGICAB



PROGRAMA

18 de febrero de 2020

Conceptos básicos en materia de ciberseguridad. Ciber-resiliencia.

- Definición de la Ciberseguridad, de que estamos hablando, contexto histórico. Evolución...
- Privacidad, Disponibilidad, Integridad, Autenticación y Trazabilidad
- Los elementos del riesgo: Activos, Amenazas, Vulnerabilidades, Impacto, Controles y riesgo . Introducción a las metodologías de análisis de riesgo.
- DRP o BCP, Tiempo hasta la recuperación, punto en que vuelves después de la recuperación.
- Introducción a la Segregación de funciones en la seguridad.

Cultura de la seguridad de la información (*security awareness*, privacidad y uso de los datos)

- El profesional de la abogacía como usuario de sistemas de información y la obligación de secreto profesional.
- Plan de concienciación en ciberseguridad - Security awareness
- Buenas prácticas en el uso del mail, ordenador, dispositivos móviles y otras herramientas electrónicas.
- Antimalware, copias de seguridad, password, cifrado disco y usb, borrado seguro, actualización de las aplicaciones, uso email, uso wifi, navegación segura, formación continuada en seguridad.



DIGICAB



PROGRAMA

20 de febrero de 2020

Gobernanza de la seguridad informática

- Política de seguridad y compromiso de la dirección
- Segregación de responsabilidades y funciones
- Gestión de riesgos. ISO 31000. Herramientas para realizar un análisis de riesgos, Etapas posteriores.
- Formación y concienciación
- Mejora continua. Ciclo de Deming – PDCA. El círculo virtuoso de cualquier Sistema de gestión desde el enfoque ISO)

25 de febrero de 2020

Ciber amenazas: como detectarlas y medidas de protección

- Clasificación de las amenazas y de las vulnerabilidades
- Ataques comunes que se dan en la actualidad (Phishing, ransomware, Zero-Day,)
- Arquitectura de los sistemas de protección
- Sistemas de detección
- Mecanismos de defensa
- Ingeniería social, suplantación de identidad y otros delitos informáticos



DIGICAB



PROGRAMA

27 de febrero de 2020

Gestión de proveedores encargados de los SGSI y normas

- Normas internacionales y nacionales de seguridad de la información (ISO/IEC 27001:2013, COBIT 2019, Esquema Nacional de Seguridad-ENS)
- Estándares y certificaciones de privacidad (ISO/IEC 27018:2019, ISO/IEC 27701:2019, ISO/IEC 29100:2011, SOC 2 y 3)
- Como evaluar un proveedor de seguridad (ISOs relacionadas, RFP, Modelo Carter 10 C's, ISO 9001:2015) -> Incluir proveedores Cloud (y breve mención a ISOs y otras relacionadas con la seguridad de los proveedores cloud como la certificación STAR de la CSA o ISO/IEC 27036, ISO 28000:2007)
- Puntos claves a tener en cuenta a la hora de negociar un contrato con un proveedor de seguridad de la información. Recomendaciones a incluir en el clausulado



DIGICAB



FECHAS: Martes y Jueves 18, 20, 25 i 27 de febrero

HORARIO: De 18 h a 20 h. 30'

SALA 62

Número máximo de alumnos recomendado: 30