UBT | L&C

Compliance • Privacidad • Asesoría legal • PBCFT

Fenin Tecnología Sanitaria

Protección Jurídica frente a un Ciberataque

Garantizar la seguridad y prevenir el negocio con la gestión de las pruebas digitales

UBT | Legal
Derecho Digital · Asesoría de Negocio · Derecho Procesal

UBT | Compliance
Privacidad · Cumplimiento Normativo · Ciberseguridad · PBCFT

laworatory

UBTLAB Formación

KEY auditors

Ponente: Oscar López

✓ Abogado especializado en Corporate, Derecho Digital y Compliance.

✓ CEO del despacho de abogados **UBT Legal & Compliance**

✓ CEO de la compañía **Laworatory** (soluciones tecnológicas para el mundo legal)

✓ Presidente del Grupo de Regulación y del Observatorio de Privacidad de **Autelsi**

✓ **UNE** - Asociación Española de Normalización:

- Vocal CTN 71, CTN 320

- Presidente SC 5 - Ciberseguridad, protección de datos e identidad digital.

✓ **Aenor** - Auditor jefe de las normas **UNE-ISO 27701** y **UNE 71505**.

Contexto

En un mundo de Hiperconexión y Globalización, la gestión preventiva de la **seguridad** de la información y la gestión de la prueba electrónica se ha convertido en una prioridad estratégica para todas las empresas.

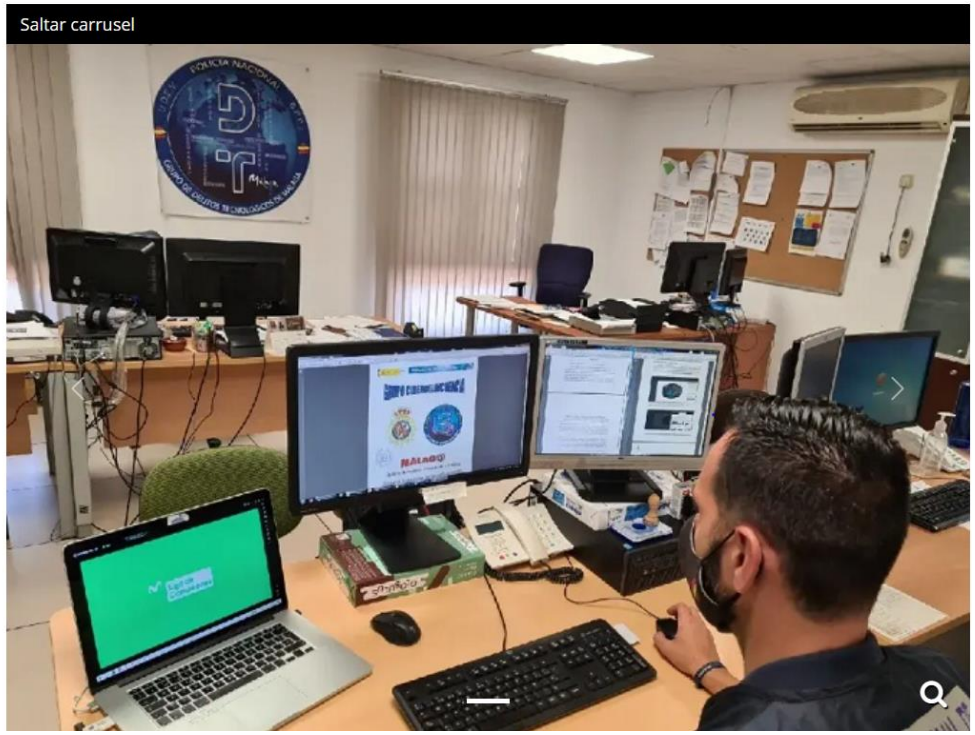
En esta sesión informativa e interactiva, examinaremos de cerca los desafíos legales de la seguridad que enfrentan las empresas en la era digital y cómo puedes proteger tu negocio de las crecientes **amenazas cibernéticas**.

- **Situación actual de la seguridad de la información y los sistemas**
- **La responsabilidad y la regulación**
- **Las buenas prácticas en la protección frente a Ciberataques**
- **Las acciones jurídicas de defensa preventiva, reactiva y correctiva**

Situación actual de la seguridad de la información y los sistemas

España registró 374.737 ciberdelitos en 2022

España 20/10/23



Informe sobre la Cibercriminalidad 2022

AUGE DEL CIBERDELITO

INCIBE gestionó más de 118.000 incidentes de ciberseguridad durante 2022, un 9% más que en 2021

05/04/2023

110.000 corresponden a ciudadanos y a empresas, 546 a operadores estratégicos y 7.980 a la Red Académica.

Situación actual de la seguridad de la información y los sistemas

- **Ransomware** (54% de los incidentes) y Ataque DDOS.

  Delito de extorsión y/o daños informáticos tipificado en el artículo 264 del Código penal.

  La entidad tiene consideración de víctima al igual que una persona física.
- **Violaciones y robos de datos** (46%).

  Delito de descubrimiento y revelación de secretos tipificado en el artículo 197.2 del Código Penal

Las fuerzas y cuerpos de seguridad (Policía Nacional, Guardia Civil, Policía Foral de Navarra, Ertzaintza, Mossos d' Esquadra y los distintos cuerpos de policía local)

***La Unidad de Investigación Tecnológica (UIT)**
*** El Grupo de Delitos Telemáticos (GDT)**

+Delitos informáticos:

- Estafas y fraudes
- Contra la propiedad intelectual o industrial

* (¡suplantación de identidad!)

Situación actual de la seguridad de la información y los sistemas

"La información, y las tecnologías que la soportan, son activos críticos"

- **¿Inventario y responsables internos?**
- **¿Conocemos los riesgos?**
- *Dimensiones a proteger: Confidencialidad, Integridad, Disponibilidad, Trazabilidad, Autenticación

****España ocupa el 2ª puesto en #incidentes de ciberseguridad en el sector salud en la Unión Europea (fuente: Informe Health Threat Landscape ENISA, jul 2023)**

La responsabilidad y la regulación

- ✓ Reglamento EU sobre la ciberseguridad (Reglamento 2019/881 de 7 de junio)
- ✓ Directiva **NIS 2 -UE 2022/2555** (transposición antes del 17 de octubre de 2024) "Network and Information Security"

- Aplica a entidades esenciales e importantes de un total de 18 sectores y a sus proveedores

- Medidas para la gestión de **riesgos de ciberseguridad** y obligaciones de notificación con sanciones deberán ser efectivas, proporcionales y disuasorias (>10 M- 2%)

1 - Responsable de Seguridad (CISO) vs Compliance Officer vs asesor legal vs DPO

2 - La responsabilidad de la alta dirección

***la responsabilidad penal de persona jurídica**

Las buenas prácticas en la protección frente a Ciberataques

¡Los ciberdelincuentes son buenos!

- Ingeniería social (manipulación):
  - Identificación de la persona relevante
  - fishing (Vishing)
  - Robo de credenciales
  - Inclusión del malware
  - Ejecución y ocultación

RANSOMHOUSE Y EL HOSPITAL CLINIC

LA PRIMERA FILTRACIÓN FUE EN MARZO

Los hackers que piratearon al Hospital Clínic de Barcelona vuelven a publicar datos

El Hospital Clínic y la Agencia de Ciberseguridad continúan trabajando coordinados desde el primer ciberataque

Las buenas prácticas en la protección frente a Ciberataques

ACCIONES PREVENTIVAS de seguridad (directiva NIS2)

- **Desarrollar una cultura de ciberseguridad basada en el riesgo:**
  - Educación: Planes de formación orientados al riesgo
  - Buenas prácticas: Políticas y Protocolos de actuación
  - Contar con un SGSI (metodología de mejora continua PDCA) (ENS)
  - Responsabilidad proactiva: Contar con una Infraestructura de la información (1) robusta y (2) resiliente (RECORDAD Covid-19)

- Auditorias (Pen Test)
- Protección de equipos (bastionado) ¡OJO a los dispositivos móviles!
- Formación, mucha sensibilización
- Antivirus, antimalware
- Cifrado, enmascaramiento
- Redes seguras
- Requisitos de seguridad proveedores

Las acciones jurídicas de defensa preventiva, reactiva y correctiva

¿Y quién es el autor?

La evidencia (prueba) electrónica: (1) Generación, (2) custodia y (3) obtención

***LIMITES AL USO DE LA PRUEBA**
Ley 3/2018 Artículo 87. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.

(2) ASEGURAMIENTO DE LA PRUEBA
Tecnología Blockchain, certificados electrónicos, registros, fechados de tiempo, …

(3) Investigación privada y presentación (clonado y presencia Notarial, técnicas de análisis forense)
FASES DEL ANALISIS FORENSE (policial o pericial):

- Identificación
- Adquisición
- Análisis
- Presentación informe pericial

Proceso documentado: imparcialidad e independencia

Las acciones jurídicas …. Buenas prácticas

1.- ¿Cuál es la primera actuación ante un ciberataque? Llamar al CISO, aislar y DENUNCIAR

Art 201 del CP "será necesaria la denuncia de la persona agraviada o de su representante legal". No será precisa la denuncia para perseguir estos ataques cuando la comisión del delito afecte a los intereses generales, o a una pluralidad de personas.

2.- ¿Qué actuaciones policiales se llevan a cabo tras la denuncia de un ciberataque?. incoa diligencias de investigación. Análisis forense, clonado de discos, y evaluación de daños.

*Problema de la cadena de custodia (STS de 10 de marzo de 2014)

**Se necesita auto judicial para el clonado del disco duro y su posterior análisis pericial: la actuación del secretario judicial

3.- Es conveniente dar parte a la compañía del seguro

4.- La importancia del informe pericial.

¿se debió a un mal funcionamiento de los sistemas de seguridad? OJO! ..hacer frente a los daños y perjuicios provocados por el ciberataque, independientemente de las responsabilidades penales de los autores.

Próximo webinar:

GESTION DEL CUMPLIMENTO Y DEL RIESGO LEGAL CORPORATIVO

UBT Legal & Compliance

¡ Nos especializamos!

UBT | Compliance

UBT Legal & Compliance pretende ser el partner de confianza en la implementación y seguimiento de modelos de prevención y sistemas de gestión de riesgos legales.

- Privacidad
- Compliance
- PBCFT
- IT & Seguridad

UBT | Legal

Soluciones jurídicas vanguardistas

- Derecho Digital
- Asesoría de Negocio
- Derecho Procesal

Auditores independientes expertos en verificación del cumplimiento legal y estándares internacionales (UNE-ISO)

- PBCFT
- Due Diligence Compliance
- Auditores Privacidad
- Auditores Sistemas de Gestión de Cumplimiento Legal

KEY auditors

laworatory

Laboratorio LegalTech de ideas que cohesiona el mundo legal y la tecnología

- CompaaS Privacidad y Seguridad
- CompaaS Compliance
- CompaaS PBCFT
- CompaaS Multicanal
- CompaaS Next Generation

Formación legal

- Formación Jurídica
- Presencial
- Híbrida
- e-Learning

UBTLAB Formación

Garantía profesional

AENOR

Nuestros profesionales auditores colaboran con AENOR, líder en certificación de sistemas de gestión, productos y servicios, y responsable del desarrollo y difusión de las normas UNE

UNE
NormalizaciónEspañola

Vocal y secretario del comité de normalización UNE de ciberseguridad y protección de datos (CTN320-SC5)

WORLD COMPLIANCE ASSOCIATION

Presidente de la comisión de ciber seguridad de la WCA. Miembro del Comité de certificación de Compliance

autelsi | OPDD
OBSERVATORIO DE PRIVACIDAD Y DERECHOS DIGITALES

Presidimos del Grupo de Regulación de AUTELSI desarrollando trabajos relacionados con Cumplimiento Normativo.

ENAC
Entidad Nacional de Acreditación

Una de las tres únicas empresas españolas acreditadas para ser auditores en PBCFT

INBLAC

Miembros del Instituto de Expertos Externos en PBCFT (INBLAC).
Expertos Externos certificados por INBLAC.

Entre nuestros clientes…

21 de nov. de 2023

Muchas gracias

Nuestro compromiso: desde el inicio, siempre contigo

WWW.UBT-LC.COM

info@ubtcompliance.com

+34 915 63 36 12

Calle Lagasca 105 1°Dcha,
28006 Madrid, Spain