Jornada de Ciberseguridad en la era digital. Protegiendo lo inevaluable. 28 noviembre 2023.

FREMM

Notas prácticas para los asistentes

Ponente: Laura Giménez de Béjar

BLOQUE 1: ¿A qué riesgos se enfrentan las PyMES? Compliance con normas de Europa y España.

La problemática de la identidad digital de la empresa y su reputación online:

¿Qué es la reputación on line?

Conjunto de información sobre una empresa expuesta en Internet (imágenes, datos, registros, noticias, comentarios…) que conforma una descripción de dicha organización en el plano digital.

Indudablemente la identidad digital empresarial o corporativa tiene múltiples beneficios como puede ser la promoción de productos, la captación de clientes a través de sus canales de comunicación, el sondeo de mercado…

PERO vivimos en la ECONOMÍA DIGITAL; el dato es la base de la economía (el petróleo del S. XXI) y cualquier empresa maneja datos:

-bases de datos de clientes,

-de proveedores,

-datos bancarios y financieros

-información referida a secretos industriales

-propiedad intelectual e industrial, etc

Ejemplos de riesgos a los que se puede ver expuesta la empresa

-Fugas de información,

-phishing,

-publicaciones negativas de terceros,

-utilización no consentida de derechos de propiedad intelectual, marca…

¿Qué es más importante, la competitividad de una empresa o su ciberseguridad?

En el panorama legal actual nos encontramos en un momento en que se está poniendo en contraposición la competitividad de las empresas, del

mercado frente a la seguridad, ganando en este caso la seguridad/ ciberseguridad.

Pensemos en el RGPD y la normativa nacional (Ley 3/2018 de protección de datos personales y garantía de derechos digitales), normativa sobre el canal de denuncias, Ley de servicios de seguridad de la información, Esquema Nacional de Seguridad, y otras normativas específicas según el sector empresarial.

Pensemos que el legislador europeo con su normativa nos viene a decir que el tema de la ciberseguridad es un tema de responsabilidad de las empresas: si éstas no cumplen con el suficiente grado de diligencia se le exigen responsabilidades:

responsabilidad por ciberataques a nuestra organización de la que derivan denuncias de los afectados, acciones por responsabilidad contractual, sanciones por incumplimiento de normativa…

de todo ello deriva el impacto que puede tener en la empresa además del daño económico el daño reputacional.

¿Cómo se protegen las empresas ante esto? La armadura del Compliance Digital

Con la armadura del **Compliance digital** se presenta como método de protección para la empresa: la empresa que invierte en compliance en seguridad de la información y en cumplimiento normativo, evita pérdidas económicas y reputacionales, y sanciones, gana en competitividad, gana en confianza de los clientes y potencia su marca.

BLOQUE 2: ¿Cómo actuar durante un incidente? Gestión reputacional y comunicación a afectados.

Tendremos que tener en cuenta el incidente de que se trate pero a grandes rasgos diremos que por un lado es importante reforzar la seguridad de la empresa y consolidar la imagen de la empresa, a través de redes sociales, newsletter o la propia web para transmitir seguridad a los clientes.

Preservar pruebas favorables a la empresa (necesario asesoramiento técnico + legal)

En líneas generales, dado que la mayor parte de las medidas son de tipo técnico y en ese campo entra en juego el asesoramiento de empresas de ciberseguridad, desde la parte legal nos dedicamos de forma conjunta con especialistas técnicos en la materia a gestionar que se preserven las pruebas digitales, utilizando testigos online y el asesoramiento sobre la denuncia ante las fuerzas y cuerpos de seguridad del estado para obtener pruebas a favor de la empresa que ayuden a su defensa y reducir su responsabilidad justificando su diligencia y buen hacer respecto a las medidas preventivas.

Comunicación de la brecha de seguridad

En lo que se refiere a la protección de datos de carácter personal, tenemos que tener en cuenta la obligación de comunicar las brechas de seguridad a la AEPD antes de 72 horas desde que se produjo el incidente y también a los interesados en aquellos casos en los que el incidente pueda suponer un riesgo para sus derechos y libertades.

BLOQUE 3: ¿Cómo aprender de los errores? Consecuencias legales y defensa legal durante la misma.

Dentro de la defensa legal hablamos de la interposición de acciones judiciales en función del incidente, la obtención y conservación de las pruebas digitales y la responsabilidad de la empresa.

Interposición de acciones judiciales

Habrá que estudiar el caso concreto, a grandes rasgos podemos citar:

- Denuncia ante las FFCCSSEE o juzgado de guardia por la comisión del delito que se trate (estafas, suplantación de identidad, calumnias/injurias…)
- Demanda por intromisión en el derecho al honor de la empresa
- Demanda por el uso de la marca o el logo por terceros in consentimiento, etc.
- Medidas extrajudiciales de solución de conflictos derivados del uso fraudulento de nombres de dominio, a través de la entidad Red.es

Obtención y preservación de la prueba digital

Dado que nos movemos en el ámbito digital la obtención de las pruebas y su conservación es fundamental para poder acreditar los hechos en sede judicial. Tendremos que tener en cuenta:

- La obtención de las pruebas y el acceso a las mismas no puede vulnerar derechos fundamentales. Pensemos por ejemplo en el acceso a correo electrónico del trabajador por la dirección de la empresa.
- La prueba digital en sí misma presenta unas características que hacen que sea una prueba más difícil de obtener o de conservar: puede ser alterada, destruida o copiada con mayor facilidad que

otro tipo de prueba. Por ello es fundamental la determinación de su huella digital para llegado el momento acreditar que no ha sido manipulada.

Responsabilidad de la empresa

Artículo 31 bis del CP establece que las empresas son responsables penalmente por:

- Los delitos que sus representantes legales y administradores, de hecho o de derecho, cometan en su nombre o por su cuenta, que resulten en beneficio directo o indirecto para la entidad.
- Los delitos cometidos por los trabajadores, en el desempeño de sus actividades para la entidad y por cuenta y en beneficio directo o indirecto de la empresa, sin que se hayan establecido por parte de la entidad los medios de control debidos sobre ellos.

Conclusiones

-La seguridad digital de tu empresa importa

-La seguridad digital de tu empresa tiene dos patas:

-Técnica: experto en ciberseguridad

-Legal: abogado especializado en derecho digital

-Los riesgos existen:

-Reputación

-Económicos

-Penal

-Necesitas una armadura para tu empresa:

-Medidas técnicas de ciberseguridad

-Medidas legales: compliance digital + asesoramiento especializado

-Seguro

-Ante un incidente/ciberataque/fuga de datos:

-Si tienes armadura:

-Freno, mayor control del impacto y previsión de futuros ataques

-Gestión correcta de la crisis reputacional

-Obtención y conservación de pruebas favorables

-Seguimiento de protocolos legales

-Limitación de responsabilidad:

-Daños a terceros que piden indemnizaciones a la empresa

-Sanciones o multas

-Responsabilidad penal

-Limitación de la carga económica: el seguro responde

-Si NO tienes armadura:

-Descontrol del impacto

-Gestión de la crisis reputacional sin estrategia

-Posible pérdida de pruebas favorables

-Posible falta de seguimiento de protocolos legales

-Posiblemente asunción de responsabilidad completa:

-Asunción de la carga económica completa

Cualquier duda o pregunta, quedamos a vuestra disposición