CIBERRESILIENCIA

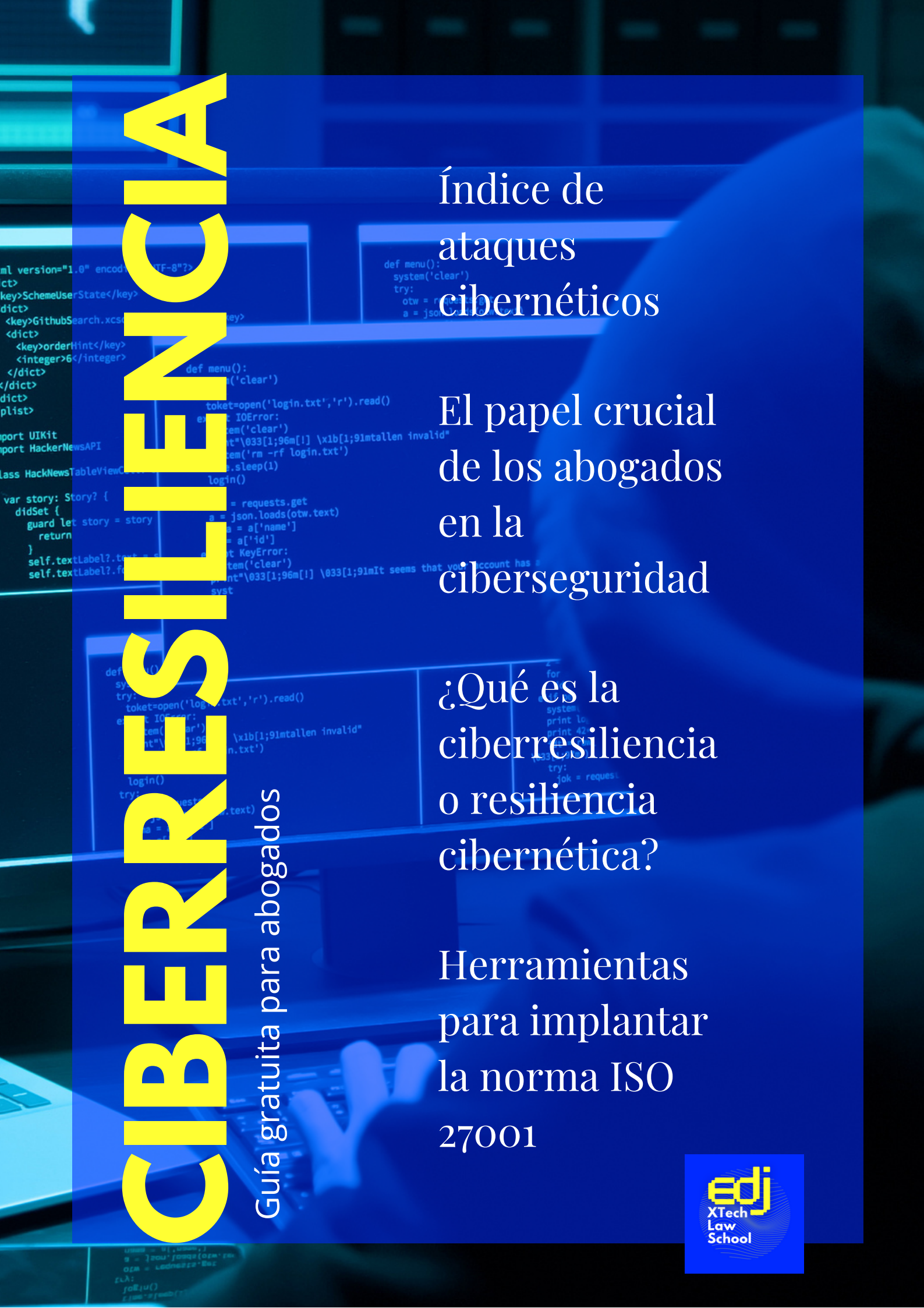
Guía gratuita para abogados

Índice de ataques cibernéticos

El papel crucial de los abogados en la ciberseguridad

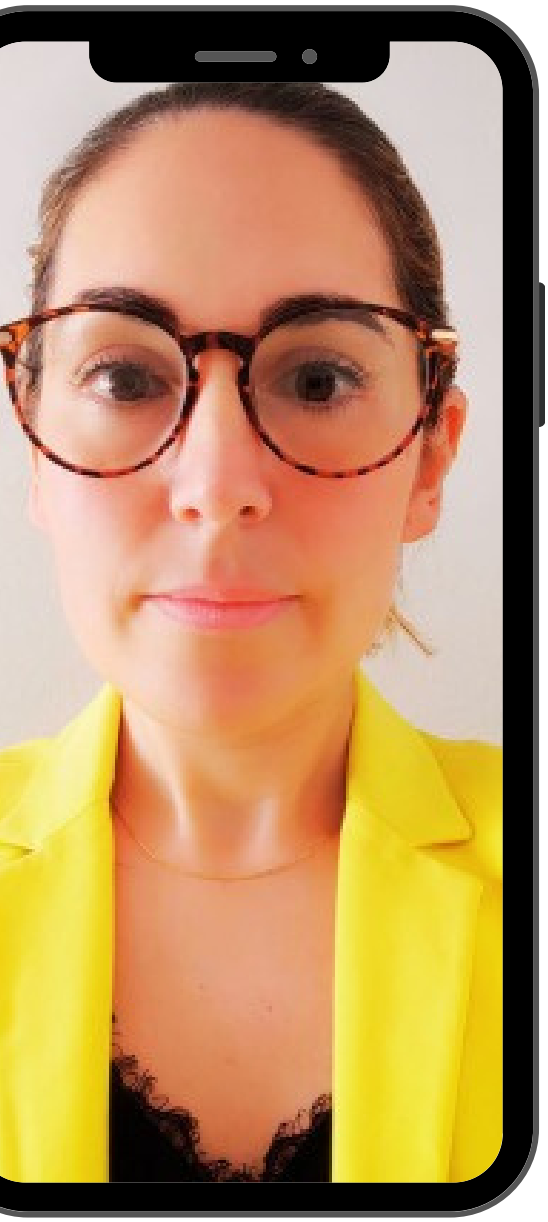
¿Qué es la ciberresiliencia o resiliencia cibernética?

Herramientas para implantar la norma ISO 27001



edj XTech Law School

¡Hola!



¡Bienvenidos a la guía de ciberresiliencia para despachos de abogados!

Soy Leyre Pérez, CEO y Co-Fundadora de EDJ XTECH LAW SCHOOL, la primera escuela de negocios online para abogados especializada en tecnología.

En un mundo cada vez más conectado, la ciberseguridad se ha convertido en un aspecto fundamental en nuestras vidas. Hoy en día, tanto individuos como organizaciones están expuestos a diversas amenazas cibernéticas que pueden comprometer la confidencialidad, integridad y disponibilidad de la información. Por ello, nos complace presentarles esta guía gratuita de ciberresiliencia, la cual tiene como objetivo principal fortalecer nuestra capacidad para enfrentar y recuperarnos de posibles incidentes de seguridad en el entorno digital.

Al ofrecer esta guía de ciberresiliencia de manera gratuita, buscamos proporcionar herramientas y conocimientos que permitan a las personas adquirir habilidades y capacidades para protegerse en línea. Creemos firmemente en el acceso equitativo a la información y en brindar recursos que ayuden a contrarrestar los riesgos asociados con las amenazas cibernéticas.

Índice

Como institución educativa, tenemos la responsabilidad de fomentar una cultura de seguridad cibernética y promover buenas prácticas en el uso de la tecnología.

El 43% de ciberataques van dirigidos a las pequeñas empresas

El 43% de los ciberataques van dirigidos a las pequeñas empresas. Esas son las conclusiones del Estudio de Accenture sobre el coste de la ciberdelincuencia.

También, el estudio de Check Point Research sobre los ataques cibernéticos ocasionados en el primer trimestre del año, informa de un incremento del 7% en los ataques semanales con respecto al mismo periodo del 2022, es decir, se produjeron hasta los 1.248 ciberataques por semana de media.

El Informe global de la Semana de la ciberprotección de Acronis de 2023 recoge que un 36% de las interrupciones de actividad en las empresas a lo largo de 2021 se debió a ataques cibernéticos.

Por su parte, Antonio Pastor - abogado y socio de Círculo Legal - refiere que, como consecuencia de ciberataques, en 2022 más del 43 % de las empresas españolas dejaron de estar operativas.

Ante esta situación, las empresas deben desarrollar una adecuada resiliencia cibernética.

El papel crucial de los abogados en la ciberseguridad

En la era digital en la que vivimos, la ciberseguridad se ha convertido en un tema de vital importancia tanto para empresas como para individuos. Los avances tecnológicos han abierto nuevas puertas y oportunidades, pero también han dado paso a una serie de amenazas y desafíos que requieren una atención especializada.

En este contexto, los abogados desempeñan un papel crucial en la protección de los derechos y la seguridad de sus clientes en el ámbito de la ciberseguridad.

El Consejo General de la Abogacía resalta que es importante que el abogado pierda el temor a asumir un papel protagonista en la gestión de incidentes de seguridad informática para asumir el liderazgo en necesidades internas de la empresa o despacho, y externas con clientes y proveedores:

Al hablar de necesidades internas nos referimos a las iniciativas de prevención (redacción de políticas internas, cláusulas contractuales y otra documentación, formación, etc.) y de gestión frente a posibles daños que puedan haberse producido en la empresa como resultado de un ciberataque.

Por ejemplo: coordinar una investigación interna, preparar y presentar una denuncia, asesorar en la recopilación de pruebas, prepararse para un posible proceso judicial futuro, interactuar con las fuerzas y cuerpos de seguridad del Estado y, en su caso, con la Fiscalía, así como trabajar con la compañía de seguros y el departamento de comunicación de la organización para revisar los mensajes relacionados con el incidente que se emiten hacia el exterior.

Y las necesidades externas abarcan las reclamaciones de clientes o proveedores, las acciones del regulador, la protección de la responsabilidad de los administradores y directivos, las crisis de reputación, etc.

"Los abogados desempeñan un papel crucial en la protección de los derechos y la seguridad de las personas y las empresas."

¿Qué es la ciberresiliencia o resiliencia cibernética?

La resiliencia es la capacidad de hacer frente a las adversidades de la vida y salir más fuertes de estas experiencias; lo que trasladado al sector de la seguridad de la información es conocido coloquialmente como ciberresiliencia.

Así, la resiliencia cibernética se puede definir como la capacidad de una empresa de resistir a los ataques cibernéticos y de recuperarse de forma efectiva en el menor tiempo posible.

El propósito principal es mantener la operatividad de la empresa, y la seguridad de la información, ante posibles ataques de carácter cibernético a los que pueda estar expuesta la empresa, tales como, filtraciones de información, secuestro de datos o robos de identidad.

Pero, ¿cuáles son las ventajas?

Ventaja 01

1. Mejora de la gestión de riesgos.

Ventaja 02

2. Minimiza las pérdidas económicas.

Ventaja 03

3. Logra la confianza del cliente mejorando la reputación del negocio.

Ventaja 04

4. Aumenta la ventaja competitiva.

Consejos paso a paso

¿Cómo lograr ser ciberresiliente?

Uno de los elementos básicos para lograr una empresa ciberresiliente es cumplir con los requisitos previstos en la Norma ISO 27001. Aunque las ISO no tienen el valor de norma jurídica, y por tanto, son voluntarias, su seguimiento aporta garantías sobre el cumplimiento por tu empresa de los estándares destinados a ordenar y mejorar su gestión. De hecho, en algunos ámbitos el sector asegurador puede exigir el cumplimiento de estas normas técnicas, pues son una garantía del cumplimiento.

La Norma ISO 27001 recoge los 3 pilares necesarios para establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información (SGSI). Si falla uno de los componentes nos encontramos ante un peligro para nuestra seguridad de la información.

1. Confidencialidad de la información

Establecer los **objetivos** de confidencialidad de la información permite prevenir el acceso a la información, evita la divulgación de la información a personas o sistemas que no se encuentran autorizados y protege del uso indebido de la información.

Recuerda que la confidencialidad es especialmente importante para la protección de los datos personales y financieros.

Diseña las **medidas** para garantizar la confidencialidad como el control de acceso, cifrado, implementación de políticas de seguridad de datos y la verificación periódica de los sistemas de seguridad.

Es importante tener un plan de contingencia para enfrentar incidentes de seguridad, así como concienciar a los usuarios sobre la importancia de esta con políticas claras para el uso y acceso a la información.

2. Integridad de los datos

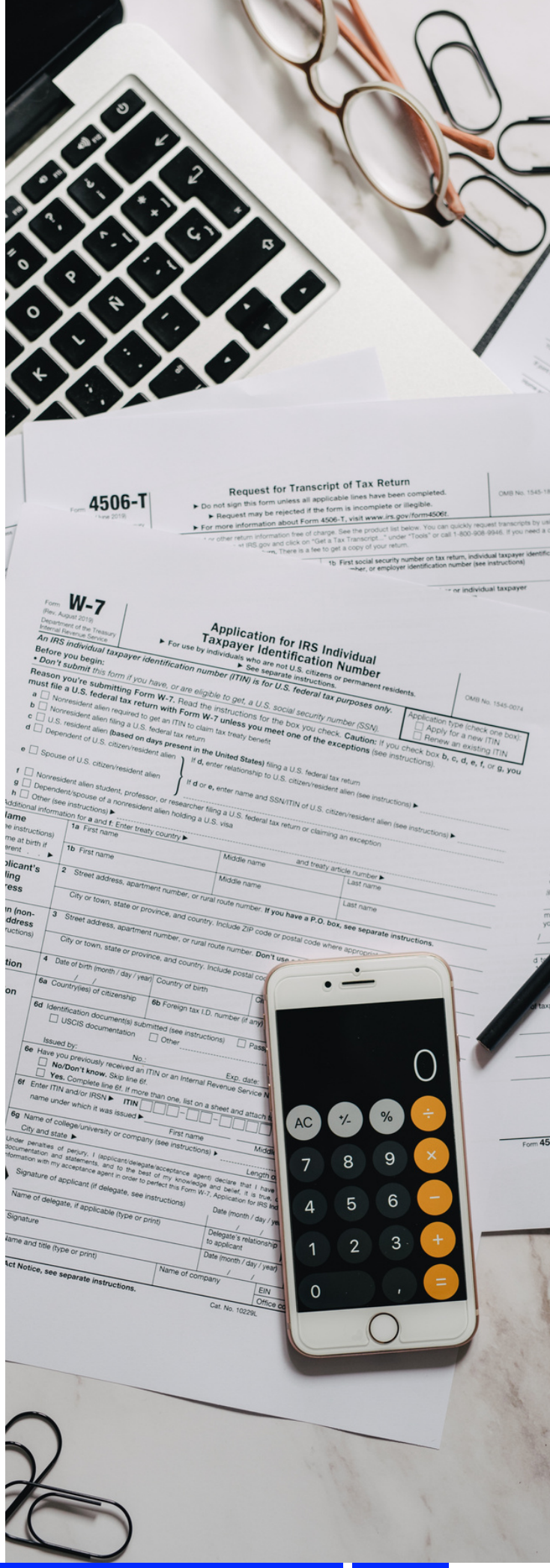
Asegurar la **integridad de los datos** es esencial para la toma de decisiones. Para garantizar que los datos se mantienen intactos y libres de modificaciones o alteraciones por terceros se debe cifrar la información mediante un método de autenticidad como una contraseña o mediante huella digital con control de acceso.

También implementar un plan de contingencia para enfrentar incidentes de seguridad que puedan afectar la integridad de la información.

3. Disponibilidad de la información:

Tener disponible la información cuando el usuario necesite realizar una consulta exige implementar medidas de seguridad para evitar interrupciones o indisponibilidades, como circuitos de internet, dispositivos de red, estructuras de respaldo y recuperación de datos.

> Desarrolla políticas que puedan activarse en caso de fallas o incidentes de seguridad.



Fases de detección de riesgos

1	Fase 1. Definir el alcance El primer paso a la hora de llevar a cabo el análisis de riesgos, es establecer el alcance del estudio. Recomendamos que el análisis de riesgos cubra la totalidad del alcance del Plan Director de Seguridad, dónde se han seleccionado las áreas estratégicas sobre las que mejorar la seguridad.
2	Fase 2. Identificar los activos Una vez definido el alcance, debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio. Para mantener un inventario de activos sencillo puede ser suficiente con hacer uso de una hoja de cálculo o tabla.
3	Fase 3. Identificar / seleccionar las amenazas Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado.
4	Fase 4. Identificar vulnerabilidades y salvaguardas Estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades. Por ejemplo, una posible vulnerabilidad puede ser identificar un conjunto de ordenadores o servidores cuyo sistemas antivirus no están actualizados.
5	Fase 5. Evaluar el riesgo Llegado a este punto disponemos de los siguientes elementos: Inventario de activos; conjunto de amenazas de cada activo; conjunto de vulnerabilidades de cada activo; medidas de seguridad implantadas. Con esta información, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría.
6	Fase 6. Tratar el riesgo Una vez calculado el riesgo, debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido. A la hora de tratar el riesgo, existen cuatro estrategias principales: Transferir el riesgo a un tercero. Eliminar el riesgo. Asumir el riesgo, siempre justificadamente. Implantar medidas para mitigarlo.

Fuente información: Instituto Nacional de Ciberseguridad: INCIBE.

NETWIX

Se anuncia como una plataforma para el análisis del comportamiento del usuario y la mitigación de riesgos que le permite controlar los cambios, el acceso y la configuración en los sistemas e instalaciones.

https://www.netwrix.es/ISO_IEC_Compliance.html

Herramientas para implantar la norma ISO 27001

ISOWIN

Es una aplicación web para la implantación, administración y certificación de Sistemas de Gestión de la Seguridad de la Información según la norma ISO 27001.

https://isowin.es/software-ISO-27001/

QMKEY QUALITY

Es un programa para el cumplimiento de la norma Iso 27001, a partir del software para ISO 9001, y que incluye la evaluación de riesgos, la implementación de controles y la gestión de la documentación.

https://www.kmkey.com/software-para-iso-27001/

GRACIAS

Gracias por haber tomado el tiempo de leer esta guía sobre ciberresiliencia para abogados. Esperamos que esta guía les haya proporcionado una visión sólida del papel de los profesionales del derecho en la ciberseguridad, así como su aplicación en la gestión del riesgo empresarial.

Te animamos a continuar explorando y profundizando en este tema, ya que las brechas de seguridad son cada vez más frecuentes y es fundamental estar preparados para enfrentar los desafíos que surgen en el mundo digital..

¿NECESITAS AYUDA PARA ENTENDER TODOS ESTOS AVANCES?

Infórmate sobre nuestros cursos de formación continua

ADQUIERE EL MANUAL DEFINITIVO PARA SOBREVIVIR A LA ERA DIGITAL

Si has estado leyendo las noticias, seguramente te hayas dado cuenta de que la tecnología está cambiando la forma en que se llevan a cabo los negocios, las interacciones entre las personas, la adquisición de bienes, la firma de contratos e incluso la contratación de abogados.

Este libro es una guía completa que te ayudará a sumergirte en la ola de la tecnología, automatizar tu despacho, atraer nuevos clientes y evitar ser reemplazado por un abogado innovador (o un robot).

FUENTES DE INFORMACIÓN

[1] Internxt. (2023, Enero 19). Cómo crear una cultura basada en ciberseguridad en tu pequeña empresa. Recuperado de https://blog.internxt.com/es/cultura-de-ciberseguridad-para-pequenas-empresas/

[2] Channel Partner (2023, Mayo 2). Aumentan los ciberataques en el mundo aunque bajan en españa. Recuperado de https://www.channelpartner.es/seguridad/aumentan-los-ciberataques-en-el-mundo-aunque-bajan-en-espana/

[3] Ciberseguridad Latam. (2023, Abril 30). Los ciberataques mundiales aumentaron un 7% en el primer trimestre de 2023. Recuperado de: https://www.ciberseguridadlatam.com/2023/04/30/los-ciberataques-mundiales-aumentaron-un-7-en-el-primer-trimestre-de-2023/

[4] Acronis. (2022, Agosto 25). Acronis presenta la próxima generación de Acronis Cyber Protect Cloud. Recuperado de https://www.acronis.com/es-es/pr/2022/08/25-09-53.html

[5] Antonio Pastor: Higuera, A. (2021, Julio 1). El coste medio de los ciberataques a las empresas españolas supera los 100.000 euros. 20 minutos. https://www.20minutos.es/tecnologia/ciberseguridad/el-coste-medio-de-los-ciberataques-a-las-empresas-espanolas-supera-los-100-000-euros-5017284/

[6] Ostec. (2023, Abril 28) Los pilares de la Seguridad de la Información, según la norma ISO 27001 - OSTEC | Segurança digital de resultados. Recuperado de https://ostec.blog/es/aprendizaje-descubrimiento/los-pilares-de-la-seguridad-de-la-informacion-segun-la-norma-iso-27001/

[7] Incibe. (2027, Enero 17). ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. Recuperado de ://www.incibe.es/empresas/blog/analisis-riesgos-pasos-sencillo

CIBERRESILIENCIA

Guía gratuita para abogados

EDJ EXTECH LAW SCHOOL

@EDJuristas
contacto@eficienciadigitalparajuristas.com
www.eficienciadigitalparajuristas.com