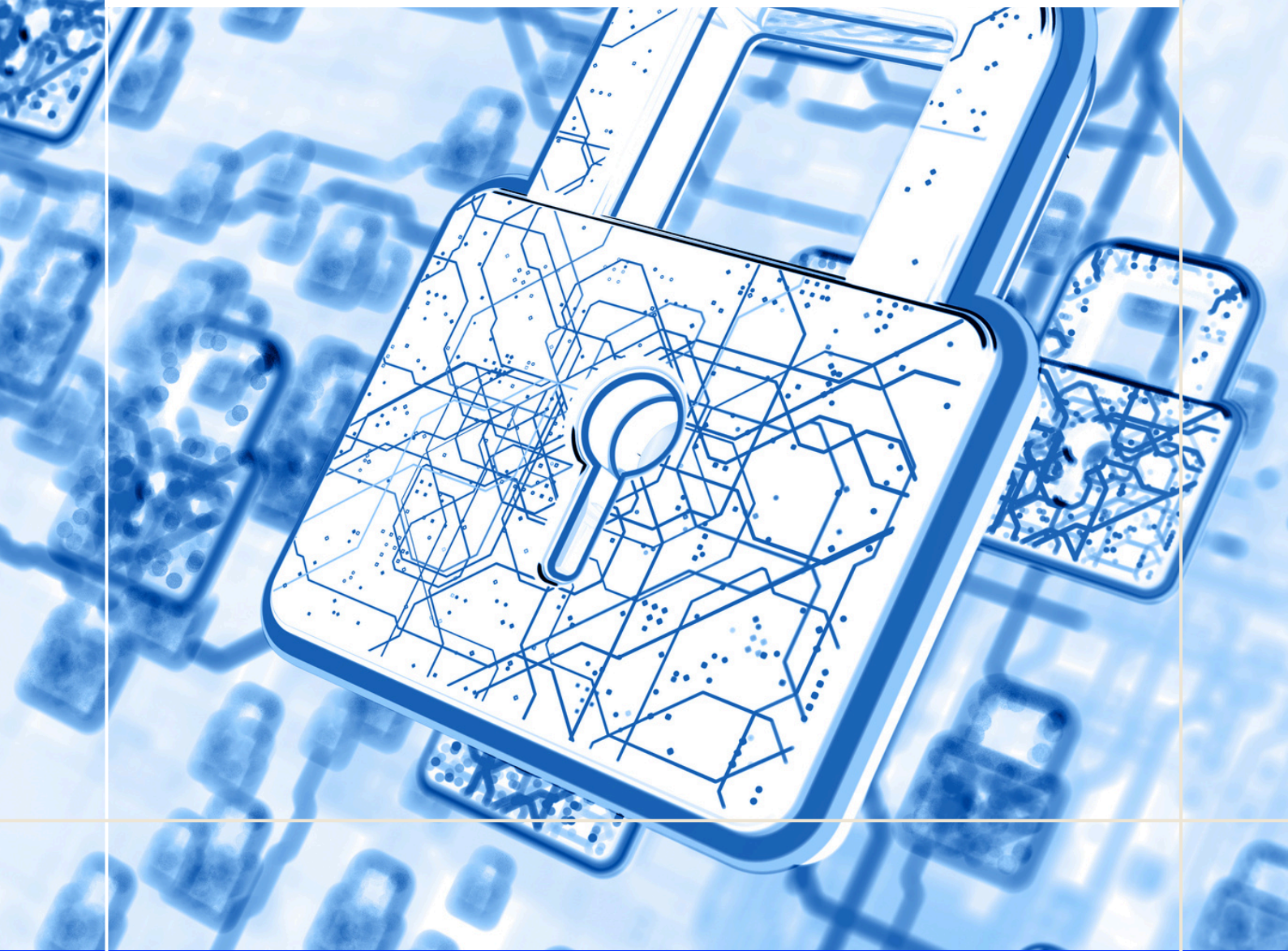
GUÍA GRATUITA PARA EMPRESAS DIGITALES

CIBERRESILIENCIA

ISO 27001 & SGSI

Cómo mantener la operatividad de la empresa, y la seguridad de la información, ante posibles ataques de carácter cibernético.



HOLA, SOMOS LARA Y LEYRE, CO-FUNDADORAS DE EDJ XTECH LAW SCHOOL.

Leyre, CEO y experta en transformación digital con más de 15 años de experiencia. Desde 2008 a 2017 trabajé en marketing digital en agencias como Havas, Ogilvy UK o Mediacom UK para marcas como IBM o Procter & Gamble. Desde el 2017, me he dedicado a la disrupción tecnológica de industrias como la banca y los seguros. Fui la Responsable de Originación Digital en EVO Banco durante la transición de la entidad hacia un banco digital y participando en el diseño del onboarding digital de la Cuenta Inteligente y el lanzamiento de la primera hipoteca 100% digital en España.

Posteriormente, asumí el rol de responsable de adquisición digital y web en Liberty Mutual en Europa.

Más recientemente, ocupé el cargo de Chief Growth Officer en Asistensi, la primera insurtech especializada en capitalizar el mercado de las remesas, ofreciendo seguros de salud adaptados a migrantes.

A nivel académico, tengo dos títulos universitarios: uno en Publicidad y Relaciones Públicas y otro en Derecho, y varios masters, postgrados y cursos de especialización en e-commerce, analítica web, growth hacking, big data & data science, ciberinteligencia, ciberseguridad y protección de datos.

"Autoras libro abogados innovadores: el manual definitivo para sobrevivir a la era digital."

Lara, COO y abogada con una sólida experiencia de 15 años en el asesoramiento integral en asuntos de tecnologías exponenciales y protección de datos. He ejercido como abogada en un despacho de primer nivel de 2008-2014 llevando asuntos a nivel nacional e internacional y, posteriormente, he desempeñando puestos en la función pública, como Capitán Auditor Asesora jurídica en la Armada Española y en la Jurisdicción militar hasta 2023.

Además, he sido profesora de opositores al Cuerpo Jurídico Militar desde 2016, profesora de Derecho en la Escuela de Intendencia de la Armada entre 2018-2021 y tutora de una tesina sobre ciberseguridad en el Master de Derecho Militar de la EMEJ-Universidad de Alcalá en 2022.

Siempre he estado en constante formación, contando con varios Master, cursos y especializaciones, destacando entre mis estudios el Máster de Derecho y Negocio Marítimo en ICADE (2008), el Máster oficial de Derecho Militar de la UCAM (2017) y el Diploma jurídico de especialización del Ministerio de Defensa (2021), habiendo realizado la tesina sobre "Las implicaciones para la seguridad de los buques autónomos".

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.

¿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.

LA NORMA ISO 27001

La norma ISO/IEC 27001 es actualmente la norma internacional más reconocida para los sistemas de gestión de la seguridad de la información.

Ayuda a las organizaciones a establecer la **política y los objetivos de gestión de la seguridad de la información** y a comprender cómo se pueden gestionar los aspectos importantes, aplicar los controles necesarios y establecer objetivos claros para mejorar la seguridad de la información.

Permite a una organización gestionar su obligación de **cumplir con los requisitos legales aplicables, como el GDPR (junto con la norma ISO 27701) y comprobar periódicamente el estado de cumplimiento**. Esto permite una mejora continua del sistema para garantizar la protección y abordar las vulnerabilidades.

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

Puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande.

Adopta un **enfoque integral de la seguridad de la información**. Los activos que necesitan protección van desde la información digital, los documentos en papel y los activos físicos (ordenadores y redes) hasta los conocimientos de los empleados individuales. Las cuestiones que hay que abordar van desde el desarrollo de la competencia del personal a la protección técnica contra el fraude informático.

La norma ISO 27001 está diseñada para ser **compatible y armonizada con otras normas reconocidas de sistemas de gestión**. Por lo tanto, es ideal para su integración en los sistemas y procesos de gestión existentes.

¿PARA QUÉ SIRVE UN SGSI?

El sistema de seguridad de la información o SGSI (Information Security Management System) tiene como objetivo evaluar todos los riesgos asociados con los datos e información que se manejan en una empresa.

El SGSI es un elemento fundamental de la norma internacional **ISO 27001** (Sistemas de Gestión de la Seguridad de la Información), que persigue asegurar la integridad y confidencialidad de los datos y los sistemas encargados de procesarlos.

Los principales **beneficios** que obtiene una empresa al implantar un sistema SGSI para la seguridad de sus datos son:

- **Reducción de riesgos.** Se identificarán los riesgos y amenazas gracias a controles, protocolos, políticas y monitorización de procesos logrando reducir el número de amenazas de forma notable. En caso de que se produzca un incidente relacionado con los datos, el negocio estará preparado para actuar de forma inmediata minimizando su impacto.
- **Reducción de costes.** Se optimizará todo el proceso para evaluar y detectar amenazas descartando aquellos poco eficaces. Con un uso racional de los recursos se conseguirá un ahorro de costes en seguridad.
- **Integración de la seguridad en el negocio.** Este sistema requiere de la implicación de todos los miembros de la empresa y del cambio de mentalidad, pasando a ser la seguridad uno de los componentes más importantes en cualquier proceso o actividad del negocio.
- **Cumplimiento de la normativa vigente en seguridad.** Las leyes nacionales e internacionales para el tratamiento y protección de datos estarán cubiertas garantizando que se cumplen en todos los niveles o áreas de la empresa.
- **Incremento de la competitividad.** Con este sistema se dispondrá de una prestigiosa certificación ISO de seguridad que será un elemento diferenciador con la competencia. Los clientes se sentirán más confiados y seguros de compartir sus datos personales, bancarios, gustos, y similares al saber que la empresa utiliza las mejores prácticas para garantizar que estén seguros.

CARACTERÍSTICAS DE SGSI

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

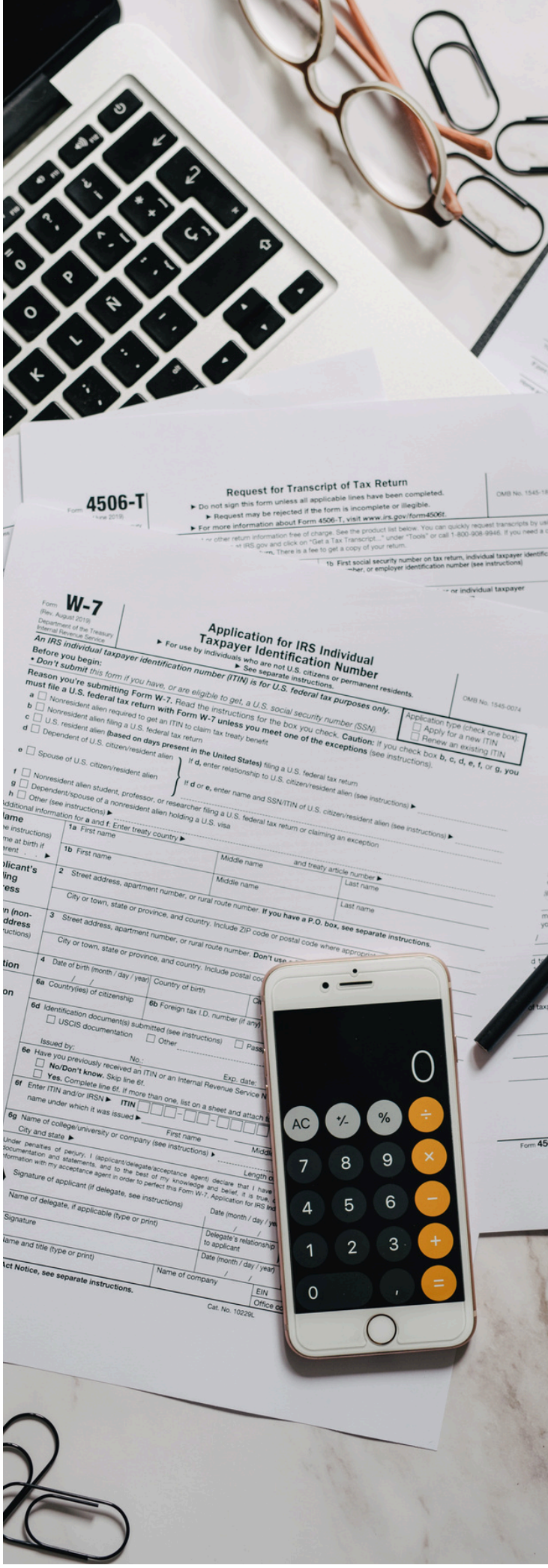
Asegurar la **integridad de los datos** es esencial para la toma de decisiones. Para garantizar que los datos se mantienen intactos y libres de modificaciones o alteraciones por terceros se debe cifrar la información mediante un método de autenticidad como una contraseña o mediante huella digital con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



CONTROLES Y FASES SGSI

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/

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

GRACIAS

Gracias por haber tomado el tiempo de leer esta guía sobre ciberresiliencia para empresas. Esperamos que esta guía te haya proporcionado una visión sólida de las claves básicas a tener en consideración para la adaptación al AI Act, así como de su trascendencia jurídica en tu empresa.

Te animamos a continuar explorando y profundizando en este tema, ya que las las sanciones que podrían llegar a imponerse en esta materia son importantes y es fundamental estar preparados para enfrentar los desafíos que surgen en el mundo digital.

¡Únete a nuestro grupo de Telegram CONSULTAS JURÍDICAS TECH!

SCAN ME

1ª CONSULTA JURÍDICA TECNOLÓGICA GRATIS


Emprendeo

LEYRE PÉREZ, CEO DE EDJ XTECH LAW SCHOOL

"QUEREMOS CERRAR LA BRECH EL DERECHO Y LA TECNOLOGÍA"

EDJ XTech Law School cubre la necesidad de for especializados en los retos de las startups y mejo de supervivencia de estas con formación tecnoju

En este contexto nace EDJ XTech Law School. ¿Con qué objetivos?
Nacemos para dar respuesta a las necesidades tecnojurídicas propias de un ecosistema que mueve más de 3.000 millones de euros anuales. Queremos cerrar la brecha entre el derecho y la tecnología, con un doble objetivo. Por un lado, velar por una innovación ética. Por otro, mejorar la supervivencia de las startups, bien con formación de aspectos legales, bien aportándoles profesionales del derecho

EDJ XTech Law Sc tecnojurídica robótica, blockc protección

Novis y Leyre Pérez, COO y CEO, ctivamente, de EDJ XTech Law School.

ecosistema español de startups cnológicas vive un momento auge, lo que supone todo un io para los profesionales y pero también

y su convergen través de la pr protección de de derechos h

¿Cómo es

En

En **EDJ** entendemos la convergencia entre la tecnología y el derecho, y los 15 años de experiencia de nuestras CEO y COO en el asesoramiento en transformación digital y en el asesoramiento integral en proyectos de índole tecnológica, nos avalan para ofrecer la mejor consultoría.

Nuestra oferta de consultoría y plataforma educativa nos permite abarcar las necesidades legales completas de las empresas en su crecimiento tecnológico, asesorando y formando cuando es necesario a su personal.

Además, formar parte del ecosistema emprendedor de innovación de Madrid nos permite estar en contacto con las necesidades legales reales de los proyectos tecnológicos.

Entra en nuestra web y reserva tu cita GRATIS

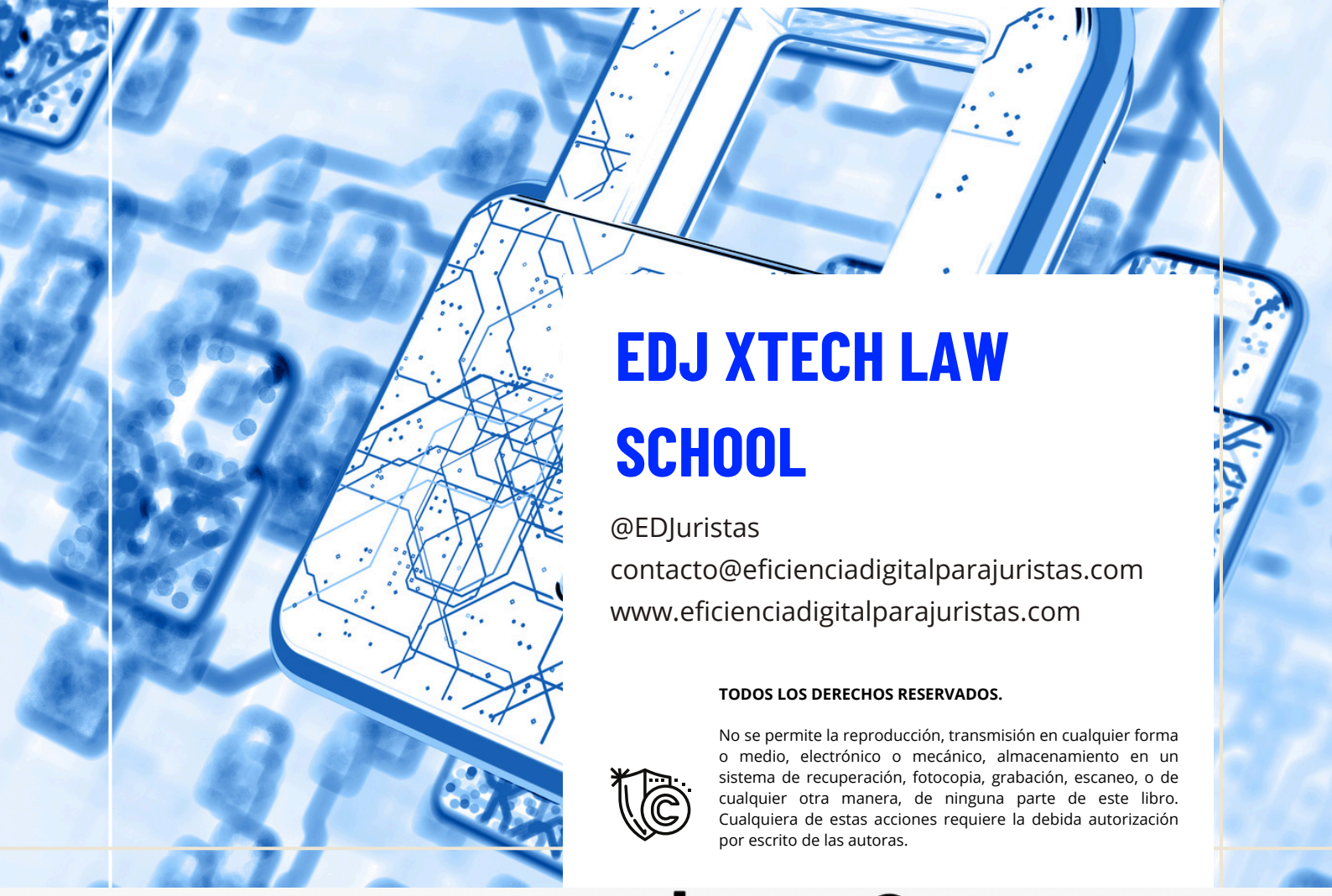
www.edjxtechlawschool.com

GUÍA GRATUITA PARA EMPRESAS DIGITALES

CIBERRESILIENCIA

ISO 27001 & SGSI

Cómo mantener la operatividad de la empresa, y la seguridad de la información, ante posibles ataques de carácter cibernético.



EDJ XTECH LAW SCHOOL

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

MadridEmprende | LA NAVE CENTRO DE INNOVACIÓN | Madrid innovation | European Institute of Innovation & Technology | Funded by the European Union