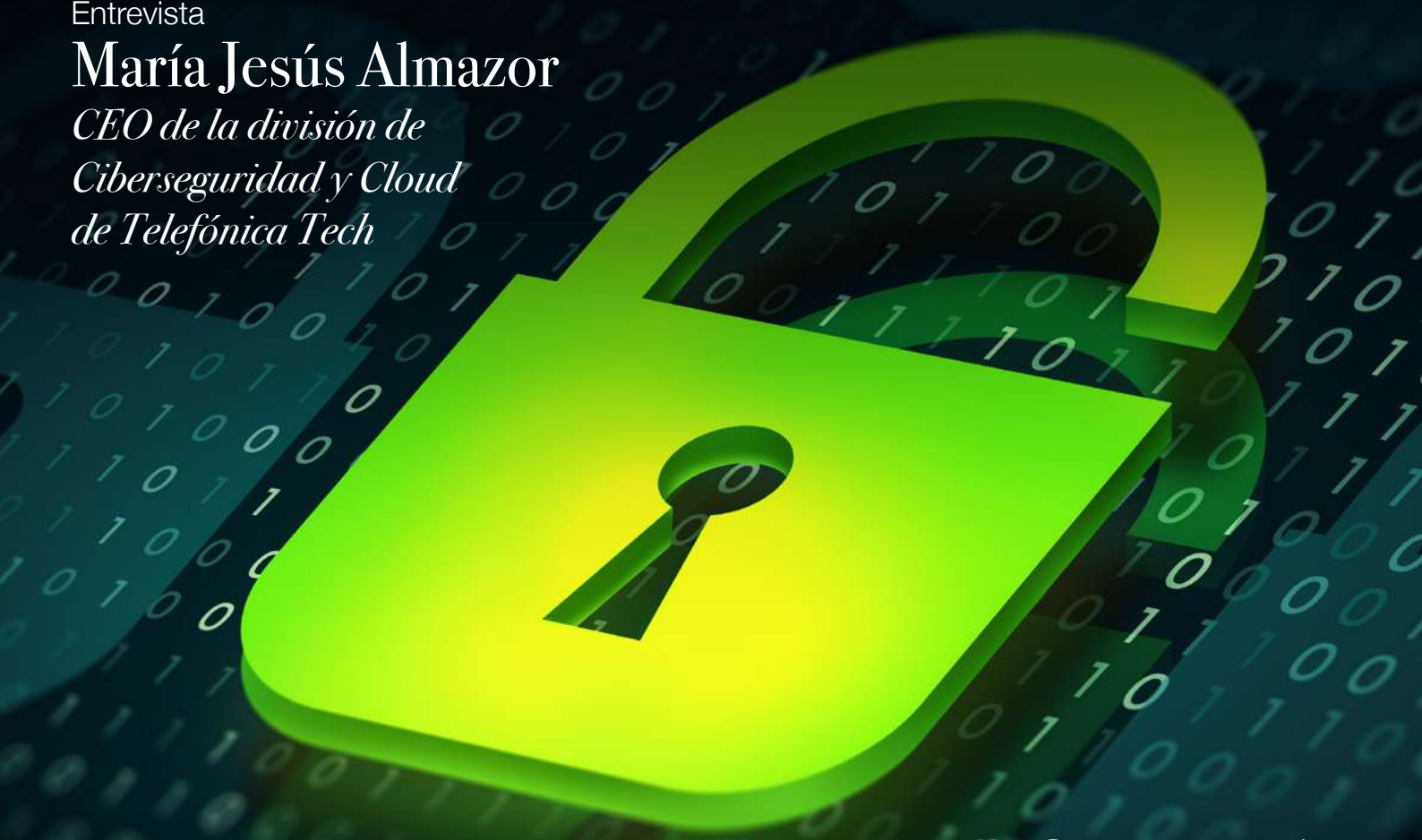
Revista de la ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
www.aec.es | N° III 2022

ISSN: 1576-4915 • 10€

# Revista Calidad

# Ciberseguridad

Entrevista
## María Jesús Almazor
*CEO de la división de Ciberseguridad y Cloud de Telefónica Tech*



*La AEC celebra el*
## Día Mundial de la Calidad

## V Congreso de Industria Conectada
*del Ministerio de Industria, Comercio y Turismo*

**ENS e ISO 27001 para cumplir con el RGPD**

**Taller de Implantación de ISO 27001**


**Requisitos y Controles para Implantar ISO/IEC 27701:2019**

**Taller de Implantación del Esquema Nacional de Seguridad (ENS)**

## Formación en Sistemas de Gestión

La Asociación Española para la Calidad junto con Govertis Advisory Services te ayudan a proteger tu organización mediante **Sistemas de Gestión de la Seguridad de la Información**. Una formación dirigida a profesionales que quieren conocer las claves de las nuevas normativas recientemente publicadas: **ISO 27002 y ENS**.

Una experiencia innovadora, práctica e impartida por los **más destacados profesionales** de la materia.

### ¡Contacta con nosotros y reserva ya tu plaza!

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

© Asociación Española para la Calidad (AEC) | www.aec.es | for@aec.es | 912 108 120

Sigue a la AEC en @aec_es https://www.facebook.com/aecalidad asociacion-espanola-para-la-calidad

Revista Calidad


**ISSN:** 1576-4915.
**Depósito legal:** M-3470-1990

**Edita:** Asociación Española para la Calidad. Claudio Coello, 92. 28006 Madrid

Tfno.: 915 752 750. Fax: 915 765 258. aec@aec.es • www.aec.es

**Presidenta:** Beatriz López Gil

**Comisión Ejecutiva:** Beatriz López Gil, Juan José Caballero García, Mayda López Belmonte, Óscar Gil del Barco, Ana Roldán Lázaro, Isaac Navarro Cabeza, Miguel Udaondo Durán

**Director General y Secretario de la Comisión Ejecutiva:** Avelino Brito

**Colaboración Técnica:** Comisión Técnica de la AEC

**Redacción:** Karen Von Burucker [kvonburucker@aec.es]

Impreso en España • Printed in Spain.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Certificada según las normas UNE_EN ISO 9001:2015 y UNE-EN ISO 14001:2015

MIEMBRO DE EUROPEAN ORGANIZATION FOR QUALITY

AEC WORLD PARTNER DE ASQ

APOYAMOS EL PACTO MUNDIAL

ONA DE FUNDIBEQ

PATROCINADORES AEC

AENOR Confía · brains · Johnson & Johnson · Medallia · NIPPON GASES The Gas Professionals · Telefónica Tech · THALES · TRIGO Global Quality Solutions

La AEC está compuesta por 385 socios individuales y 781 socios colectivos, 8 Comunidades y 6 Comités y todos representados en la Junta Directiva formada por 32 vocales. "Revista Calidad" es una publicación de la Asociación Española para la Calidad, entidad sin ánimo de lucro, que promueve el debate responsable de todas las ideas para la mejora de la calidad, el medio ambiente y la responsabilidad social e informa de las actividades de la AEC, sin que las opiniones de los autores sean necesariamente las de la propia Asociación.

## INSTITUCIONAL



## ARTÍCULOS


**Recuerda que la Revista Calidad está disponible en formato digital**

Telefónica Tech

# The Next Generation *Technology* Integrator

Big Data

Cloud

IoT

Connectivity

Cyber Security

telefonicatech.com

FOLLOW US!

# Estimado socio de la Asociación Española para la Calidad:


En un encuentro reciente, de los muchos que celebramos en nuestra Asociación, escuché a uno de nuestros socios, directivo de una empresa líder en servicios tecnológicos, decir que atendían una media de 5 incidentes graves al mes por robo de datos y posterior chantaje; chantaje para poder recuperar los datos y para evitar males aún mayores como consecuencia de su venta en uno de esos Internets de siniestro nombre, no recuerdo si era el deep o el dark. Incidentes graves de verdad, de los que ponen caras de terror y hasta alguna lágrima en curtidos ejecutivos de reputadas organizaciones.

Le escuché hablar de las cifras de negocio de los que llamaba "los malos", los delincuentes de la información; creo recordar que esa cifra rondaba los 1000 millones al año en alguna de sus estrellas. Eso es aproximadamente 8 veces lo que gana el mejor jugador de fútbol del mundo. Libres de impuestos, desde una mesa con un ordenador, sin lesiones, sin cansarse.

Pero, al fin y al cabo, el dinero no es más que dinero, por eso ésta no es la peor de las nuevas amenazas que vienen con las tecnologías. Peores son las que afectan a los derechos fundamentales de las personas, incluido el de la vida.

Por ejemplo el derecho al olvido, eso que tan poco le gusta a Internet. Alguien mencionó que Blockchain es aún más rencoroso, porque Blockchain nunca olvida, por definición.

Aprendí algo sobre neurociencia, sobre la necesidad de preservar la privacidad de la huella cerebral, y las posibilidades, parece ser que ya reales, de condicionar a las personas a partir de esa información.

Tuve ocasión de asustarme con los riesgos de la inteligencia artificial. Ahora que los programas informáticos, en base al tratamiento de enormes volúmenes de datos, lo mismo deciden la calidad de un aguacate, que las rutas de las patrullas de la policía, seleccionan los candidatos a un puesto de trabajo, o actúan sobre la apertura de un semáforo para dar pista libre a una ambulancia. ¿Quién y cómo controlará la ética de los algoritmos y la seguridad de sus decisiones?, si es que eso puede controlarse.

Las personas de mi generación hemos visto desarrollarse las tecnologías de la información y las comunicaciones. Conocimos el pueblo, con una centralita en donde se encargaban conferencias para el día siguiente. Conocimos el primer ordenador personal, el primer fax, el primer teléfono móvil, pusimos el primer correo electrónico, hicimos clic por primera vez en Internet. Hemos visto el cambio radical en la actividad económica y en el entorno en el que vivimos las personas. Hemos visto a las organizaciones crecer en sus capacidades y a las personas adquirir súper poderes, gracias a un pequeño aparato que cabe en el bolsillo.

Pero también hemos visto convertirse en una realidad creíble el imposible aquel del Gran Hermano, el Gran Hermano de 1984 que yo conocí en mi adolescencia, que vigilaba a todos los ciudadanos a través de una pantalla en el salón. Aquello que entonces parecía tan distópico como irreal, ¿lo llevamos ahora en el bolsillo?

Es el momento de la ciberseguridad. Este nuevo mundo digital, del que estoy convencido que sólo hemos visto una patita asomando por la puerta, plantea nuevos riesgos y desafíos. Y muy gordos.

Las organizaciones tendrán que dedicar mucho dinero a la seguridad de la información. Hará falta mucho esfuerzo para implantar medidas de seguridad adecuadas. Se desarrollarán marcos legislativos que plantearán muchas dificultades a los profesionales. Y todo esto no lo hará la inteligencia artificial, lo tendrá que hacer la de toda la vida, la de las personas. ¿Quién dijo que la digitalización significaba menos trabajo para las personas?

Como siempre, nuestra revista es una ventana abierta a lo que hacen nuestros socios, en esta edición, en seguridad de la información, o, como se dice ahora, en ciberseguridad.

Entrevista

# María Jesús Almazor

*CEO de la división de Ciberseguridad y Cloud de Telefónica Tech*

**Karen Von Burucker**

Directora de Comunicación y RRII. **Asociación Española para la Calidad, AEC**

kvonburucker@aec.es

www.linkedin.com/in/karenvonburucker

**María Jesús Almazor comenzó su carrera profesional en Telefónica en 1994. Dirigió las operaciones de la compañía en la zona norte y luego en el sur para posteriormente ejercer de Directora del Territorio Sur hasta 2018, cuando pasó a ser Consejera Delegada para España. En 2021 María Jesús Almazor se sumó al proyecto de Telefónica Tech, línea estratégica de Grupo Telefónica, como Consejera Delegada de la división que engloba los negocios de Ciberseguridad y Cloud.**

**¿Por qué la Ciberseguridad es clave para asegurar la calidad de negocios y empresas?**

Estamos inmersos en la transformación digital de la sociedad, porque sectores vitales para la población como el transporte, la energía o la sanidad presentan ahora una mayor dependencia de las tecnologías.

La irrupción de la tecnología en nuestras actividades cotidianas ha generado también una toma de conciencia del impacto que puede tener en aspectos tan relevantes como la privacidad. Existe una mayor

conciencia por parte del ciudadano respecto a los derechos que les amparan en materia de protección de datos. Por tanto, existe una conciencia de clientes o potenciales clientes de una organización.

Y esta conciencia lleva a que, en la percepción de la calidad de los servicios, cada vez más influyan cuestiones como la gestión que hacen las empresas de los datos personales. Por ejemplo, un cliente asume que una gestión diligente de los datos forma parte de la calidad de los servicios; como también una recogida responsable e informada atendiendo los requisitos de la regulación; una correcta atención en los ejercicios de derechos que le amparan en protección de datos; una comunicación responsable cuando se producen brechas de seguridad, etc.

Además de la gestión de los datos personales, recalcar la importancia de la ciberseguridad para garantizar la continuidad del negocio es fundamental: hay ataques que buscan quebrar las operaciones habituales de las empresas.

Por eso la ciberseguridad, de la mano con la protección de datos, son armas clave para garantizar la calidad de los negocios y la confianza de los clientes.

**¿Están las PYMES expuestas a los mismos ataques y amenazas que las grandes empresas?, ¿cuáles son las principales amenazas y retos a los que se enfrentan?**

Las PYMES también están expuestas a riesgos similares a los de las grandes empresas. Por ejemplo, el 40,5% de los ataques de ransomware recibidos en el mundo lo reciben empresas de menos de 100 empleados.

En España, en concreto, algunos estudios indican que el 70% de todos los incidentes en seguridad se producen en empresas con menos de 100 empleados. La PYME es uno de los eslabones más vulnerables en esta cadena por falta de medios, tiempo y concienciación. Es habitual que una PYME no tenga personal dedicado. Los cibercriminales advierten que requiere menos esfuerzo y es más rentable hacer muchos pequeños ataques que un gran ataque, por lo que les es más interesante atacar a este segmento.

> La irrupción de la tecnología en nuestras actividades cotidianas ha generado también una toma de conciencia del impacto que puede tener en aspectos tan relevantes como la privacidad

Nosotros sacamos un estudio desde el Grupo Telefónica que analizaba los ataques a autónomos y pequeñas empresas y vimos que alrededor del 20% de las pequeñas y medianas empresas habían sufrido algún ataque, especialmente de ransomware o phishing, ataques que habían supuesto pérdida de información importante o perjuicios económicos de relieve en un alto porcentaje de estas empresas.

Las principales amenazas serían esa menor concienciación y los ataques tanto de ransomware como los intentos de intrusión o robo de datos mediante técnicas de phishing.

En Telefónica Tech contamos con soluciones específicas para PYMES, como por ejemplo 'Tu Empresa Segura', que tiene ya más de 5.500 clientes en España y que ofrece un paquete de servicios de seguridad con soporte personalizado para proteger la actividad digital de las pequeñas y medianas empresas, que por tamaño no pueden realizar grandes inversiones ni cuentan con personal especializado para gestionarlo.

**¿Cuál es el error, o los errores, que más habitualmente cometen las empresas en relación con la Ciberseguridad?**

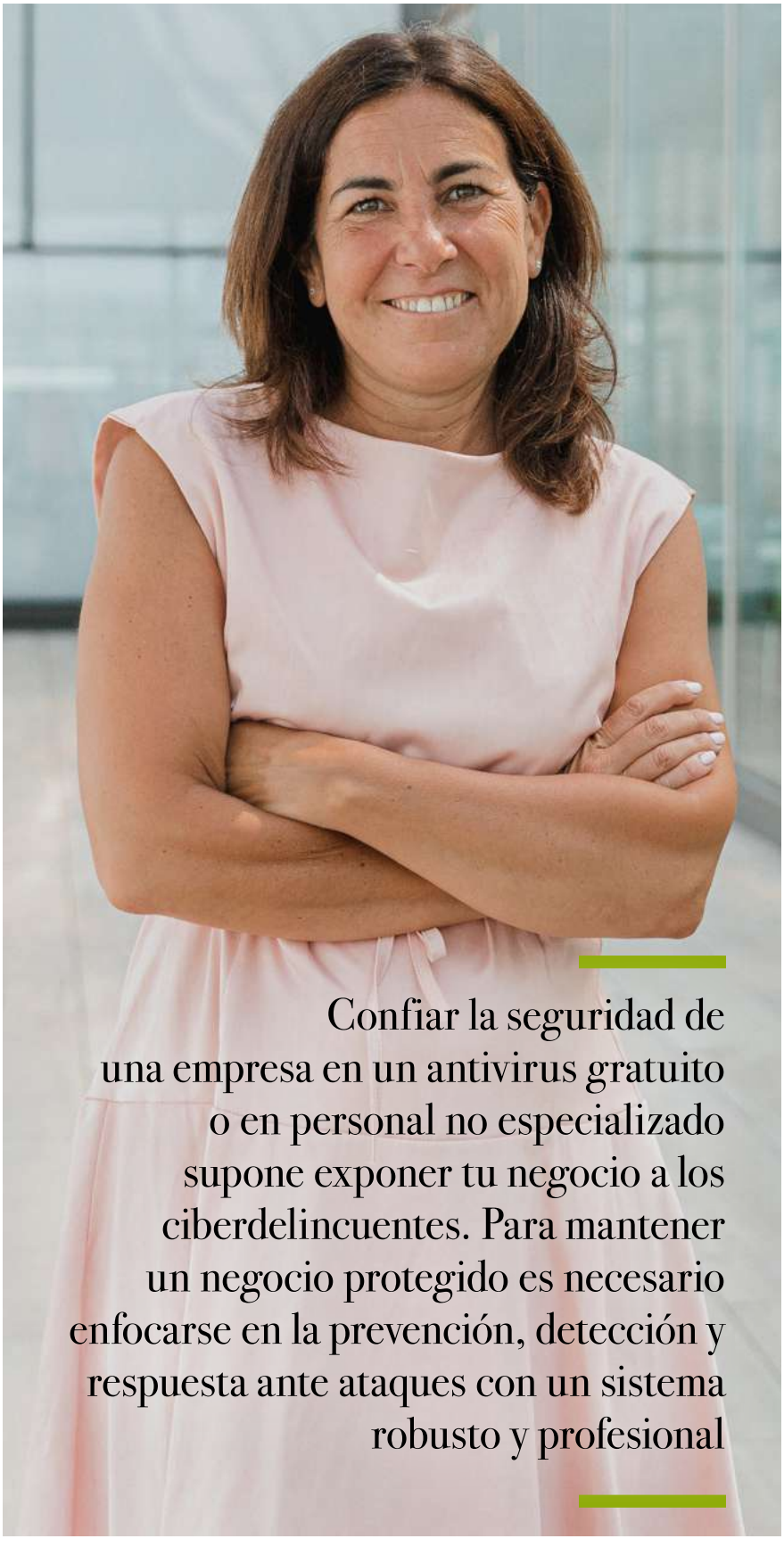
Hay que distinguir entre grandes y pequeñas empresas.

Uno de los principales errores que se cometen es no tener un área de seguridad, lo que supone una falta de procedimiento general en materia de ciberseguridad que deriva en errores que se repiten y que ponen en riesgo a las PYMES: no contar con contraseñas robustas, la navegación desde wifis abiertas, no usar VPNs, no usar verificación en dos pasos, la instalación de aplicaciones de fuentes no fiables, no tener un plan de back up de información, etc.

Por el lado de las grandes empresas, cualquier empleado que no siga la política de seguridad supone una brecha de seguridad muy importante. Aparte de los errores citados en las PYMES, que también les afectan, hay otro tipo de errores que se derivan de la explosión de datos y la complejidad derivada de la interdependencia de tecnologías on y off premise, propias y de terceros, el número de dispositivos interconectados y la digitalización de los sistemas industriales. Este despliegue de software industrial y de la infraestructura de comunicaciones asociada evidencia un terreno menos protegido de cara a ataques cibernéticos. Es imprescindible que el mundo de la ciberseguridad IT converja con la seguridad OT porque suponen un tipo de amenazas cuyo impacto en el caso de producirse traspasa a lo físico, en infraestructuras clave de comunicación, transporte y logística, energéticas, sanitarias, etc.

**¿Qué medidas deben priorizar los CISO para implementar estrategias de prevención y de resiliencia?**

El CISO debe convertirse en agente de cambio en el diseño de procesos de



> Confiar la seguridad de una empresa en un antivirus gratuito o en personal no especializado supone exponer tu negocio a los ciberdelincuentes. Para mantener un negocio protegido es necesario enfocarse en la prevención, detección y respuesta ante ataques con un sistema robusto y profesional

negocio seguros desde el origen, porque el cambio de paradigma también cambia su rol: ya no se trata de proteger servidores, sino de proteger el negocio. Se encarga de supervisar, controlar y apoyar la definición de los sistemas de gestión, además de velar por el cumplimiento normativo. Tiene que realizar una gestión de la seguridad en distintos niveles, con autonomía y capacidades de prevención, detección y respuesta en cada uno. La ciberseguridad se transforma en un recurso necesario para los diferentes negocios, para conseguir sus objetivos de fiabilidad de cara a los clientes.

**¿Cómo ayuda Telefónica Tech a las empresas a protegerse y a ser más resilientes, sobre todo en el caso de PYMES que generalmente tienen menos recursos y personal cualificado?**

Confiar la seguridad de una empresa en un antivirus gratuito o en personal no especializado supone exponer tu negocio a los ciberdelincuentes. Para mantener un negocio protegido es necesario enfocarse en la prevención, detección y respuesta ante ataques con un sistema robusto y profesional.

El 66% de las PYMES han sufrido un ciberataque en los últimos 12 meses y el promedio de las pérdidas económicas que ocasionan oscilan entre 20.000 y los 50.000 euros. Además, el 60% de las empresas atacadas cierran en menos de 6 meses.

La seguridad es un proceso de mejora continua. Un bajo nivel de seguridad se traduce en un alto riesgo. La amenaza de sufrir un ataque o incidente que tenga consecuencias adversas para las organizaciones es elevado. Es importante conocer el nivel de seguridad de un negocio para hacer una planificación de las mejoras necesarias y de este modo aumentar el nivel y estar cada vez más y mejor protegidos. Es muy importante identificar los procesos de negocio y los puntos críticos para empezar este proceso de mejora. La protección de datos, medidas de seguridad básica como antivirus y firewalls, cifrado de datos, concienciación y formación de los empleados o revisar y asegurar la web empresarial son tan solo algunos de los puntos prioritarios por los que comenzar a afianzar y mejorar el nivel de seguridad de una empresa para minimizar los riesgos a los que se enfrenta día a día.

Para combatir todo esto, en Telefónica Tech, a través de 'Tu Empresa Segura', ponemos a disposición de las empresas un asesor que realiza una evaluación de seguridad de manera totalmente gratuita, y que obtiene su nivel de seguridad junto con un informe completo para ayudar a la empresa a decidir qué paquete de "Tu Empresa Segura" se ajusta más a sus necesidades.

**Y en caso de sufrir un ciberataque, ¿qué puede hacer una empresa para recuperarse?**

Todas las compañías son susceptibles de sufrir un ataque. Se dice que hay dos tipos de empresas: las que han sufrido un ciberataque y las que no saben que lo han sufrido. Hay barreras tanto económicas como técnicas que hacen muy difícil la protección al 100%. Por eso lo más importante es contar con un plan de contingencias y aplicarlo cuando sepamos que estamos siendo atacados. Es decir, aumentar la resiliencia.

La planificación de la resiliencia cibernética o ciberresiliencia implica crear una estrategia para recuperarse de un ciberataque y proteger a la organización de futuros ataques. Para crear un plan, primero la empresa ha de identificar sus funciones críticas que se basan en tecnologías, evaluar el riesgo y vulnerabilidad de estos frente a ciberataques y desarrollar un proceso para restaurar esas funciones en caso de ciberataque.

Para mantener un negocio protegido es necesario enfocarse en la prevención, detección y respuesta ante ataques con un sistema robusto y profesional.

En el caso de que la prevención no haya funcionado y una empresa sea víctima de un ciberataque, la detección y respuesta deberá ser rápida y eficaz, especialmente en sus funciones críticas.

**En Telefónica Tech habéis fusionado bajo una misma dirección Cloud y Ciberseguridad. ¿Cuáles son los beneficios de esta unión?**

No hay digitalización sin seguridad y por eso en Telefónica Tech contamos con una única propuesta de valor de ciberseguridad y cloud, para acompañar a nuestros clientes en un entorno multi-cloud con la seguridad como atributo indispensable. Nuestros expertos identifican la tecnología que necesita el cliente y le acompañan en su implementación.

Es por eso que, con esta fusión, vamos un paso por delante en la unión de cloud y ciberseguridad, ya que estamos presentes en toda la cadena de valor y contamos con un portfolio integral de soluciones de cloud y seguridad.

Para ello, contamos con recursos especializados, pero también con la mejor tecnología y plataformas, con un ecosistema de partners dinámico y con acuerdos estratégicos con todos los líderes del mercado.

**¿Qué servicios ofrece Telefónica Tech en el ámbito de la Ciberseguridad?**

En Telefónica Tech nos enfocamos en la prevención, detección y respuesta apropiada ante las posibles amenazas con el fin de disminuir los ataques, proteger los servicios digitales de nuestros clientes y así garantizar la ciberresiliencia de sus negocios. Nos adelantamos a los ataques más sofisticados y frecuentes. Contamos con un porfolio completo de servicios de seguridad gestionada inteligente, desde iMSS y Detección y Respuesta Gestionada (MDR) hasta la consultoría, pasando por la reventa de hardware y software. Operamos la seguridad a través de nuestro DOC (Centro de Operaciones Digitales de Cloud y Ciberseguridad) global, situado en nuestra sede de Madrid, y de nuestros 11 SOC (Centros de Operaciones de Seguridad) repartidos por el mundo.


*El DOC de Telefónica Tech es un centro de Ciberseguridad de referencia a nivel global* »

Otra tendencia detectada son los ataques ciberfísicos, es decir, ataques en la industria 4.0. Lo físico y lo digital se unen: lo que ocurre en el ámbito digital tendrá un impacto en lo físico. Por esto es relevante para aquellas empresas de este sector avanzar en seguridad IT, pero también en seguridad OT

Además, trabajamos con nuestros partners para conseguir los mayores niveles de certificación, tanto a nivel de compañía como de los profesionales que formamos Telefónica Tech.

**¿Qué evolución vamos a ver en los próximos años en el mercado de la Ciberseguridad?**

La ciberseguridad ha dejado de ser un asunto aislado del área de TI. Este cambio de postura respecto a la gestión de la ciberseguridad también se refleja en las tendencias que van a seguir las empresas en este campo.

Se incrementará la necesidad de ofrecer una mejor experiencia al cliente: tanto al cliente final con, por ejemplo, mayor regulación de privacidad de datos personales, como al propio cliente de servicios de ciberseguridad, puesto que se observa una estrategia de acceder a una plataforma SSE (Secure Service Edge), que aúne la web, servicios de cloud y acceso privado de aplicaciones, que también tiene que ver con un pensamiento de integrar capacidades de seguridad o de combinación de soluciones.

Seguiremos basándonos en el paradigma Zero-trust o entornos de confianza cero a la hora de desarrollar o adoptar soluciones de ciberseguridad, y esto se alineará a nivel de stakeholders, es decir, que tiene que estar ligado a los objetivos de negocio. Este alineamiento de negocio también afectará a la relación con empresas terceras: a la hora de firmar acuerdos con proveedores, cómo este tercero gestiona la ciberseguridad será importante a la hora de tomar decisiones de contratación.

Otra tendencia detectada son los ataques ciberfísicos, es decir, ataques en la industria 4.0. Lo físico y lo digital se unen: lo que ocurre en el ámbito digital tendrá un impacto en lo físico. Por esto es relevante para aquellas empresas de este sector avanzar en seguridad IT, pero también en seguridad OT.

Y, finalmente, mayor avance en este cambio de paradigma: se intentará avanzar en desarrollar una cultura más resiliente en relación con los riesgos de seguridad, y esto se verá a todos los niveles, incluido los comités de dirección de las empresas.

El ritmo de evolución tecnológica en ciberseguridad nunca ha sido tan rápido. Esto nos obliga a ser muy flexibles y a pensar la seguridad desde el negocio.

CIBERSEGURIDAD

# En AENOR, sabemos que cuando un empleado hace clic, una empresa puede hacer crack

Cada día, millones de empleados y usuarios navegan por internet o descargan información sin pensar en lo que eso supone para la seguridad de su empresa. En AENOR, hemos trabajado en un **nuevo ecosistema digital** donde respondemos a las nuevas **necesidades de ciberseguridad y privacidad,** reduciendo el riesgo de que el clic de un trabajador provoque el crack de la compañía.

**Todas las respuestas que buscas están en** aenorciberseguridad.com

AENOR

Confía

# La AEC celebra el Día Mundial de la Calidad y otorga el "Premio al Liderazgo Directivo" y el "Premio Líder en Calidad" 2022


**La Asociación Española para la Calidad (AEC) celebró el Día Mundial de la Calidad en el Auditorio de la Fábrica Nacional de Moneda y Timbre (FNMT) de Madrid el pasado 17 de noviembre bajo el lema *"DigiCalidad".***




Con Sus Majestades los Reyes como presidentes de honor, la bienvenida institucional estuvo a cargo de la presidenta de la AEC, Beatriz López Gil; el secretario general de Industria y de la PYME del Ministerio de Industria, Comercio y Turismo (MINCOTUR), Raül Blanco; y la presidenta del Consejo de Administración y directora general de la FNMT, María Isabel Valldecabres.

El encuentro, que se desarrolló bajo el lema "DigiCalidad", estuvo presentado por la periodista y comunicadora, Teresa Viejo, y arrancó con la conferencia inspiradora de Genís Roca, presidente de la Fundació PuntCat, especialista en desarrollo de negocio y cultura digital. A continuación, Avelino Brito, director general de la AEC, fue el encargado de la ponencia magistral "Hablando de Calidad" en la que abordó los nuevos desafíos, cambios e incertidumbre en el contexto global actual, y su evolución hacia un modelo de Calidad 4.0.

Enrique Fernández, director de Digitalización y Arquitectura de REPSOL; Roberto Megías, vicepresidente & country manager para España y Portugal de Medallia; y Gabriela Chang, CSO y Cofundadora de ETHICHUB, fueron los responsables de abordar la "Economía digital" en una mesa que más tarde dio paso a la entrevista de Alberto González, Director de Operaciones y TI de la AEC, para hablar de "Seguridad digital" que contó con la participación de Rosalía Simón, Cyber and Cloud Global Consulting Director de Telefónica Tech.

Por último, la Dra. Paloma Fuentes, responsable de Transformación de Personas y Organizaciones desde la Felicidad, exgerente de Felicidad de MAHOU, abordó el impacto de la tecnología en la salud de los usuarios.


# Galar-dona-dos

## Galardonados

Un año más la celebración del Día Mundial de la Calidad fue el escenario perfecto para la entrega de los galardones y reconocimientos que entrega anualmente la Asociación Española para la Calidad. En esta ocasión, el Premio AEC al Liderazgo Directivo recayó en la figura de Jesús Sánchez Bargos, Presidente & CEO en Thales España, en reconocimiento a su compromiso personal y profesional con la excelencia en la gestión y a una trayectoria que sirve de inspiración a nuevas generaciones y posiciona a España como referente de excelencia y calidad.

Durante su intervención, Jesús Sánchez Bargos señaló que “es fundamental concienciar a las organizaciones de la necesidad de implantar una cultura de mejora continua y de innovación como elemento clave para alcanzar la excelencia empresarial”. Y a continuación se refirió a una línea de actuación con importante desarrollo en el seno de las actividades de la AEC, la Experiencia de Cliente, destacando que “en Thales España la orientación al cliente es parte del modelo empresarial, ya que entender las necesidades de los clientes y el mercado han sido factores de éxito”.

Por su parte, el Premio AEC Líder en Calidad 2022, que recayó en la figura de Mariluz Villamor, Directora de Calidad de Proveedores en Mercedes Benz España. Este galardón tiene como objetivo premiar la labor de aquellos responsables de organizaciones que han situado a la Calidad en el centro de sus organizaciones, tengan la capacidad de gestionar equipos y estén habituados al uso de herramientas para adaptarse a los cambios. Además, el ganador será el representante español para el “European Quality Leader of the Year” que otorga la European Organization for Quality (EOQ).


A continuación, se hizo entrega de los nombramientos de Socio Distinguido a Félix Torres Garrido, Presidente del Comité AEC Industrias y Servicios para la Defensa, y Director de Mercados de Defensa y Seguridad de Indra Sistemas; y José Miguel Tudela Olivares, Presidente de la Comunidad AEC Responsabilidad Social Empresarial, y Director de Sostenibilidad y Acción Climática de Enagás.

Por último, la AEC reconoció la labor de Miguel Udaondo por su contribución de forma notable al desarrollo de la Asociación como Socio de Honor. Presidente de la AEC entre los años 2014 y 2022, Miguel Udaondo se dio de alta como socio en 1980, y a lo largo de estos 42 años de trayectoria asociativa ha ostentado diversos cargos de responsabilidad. Fue Vicepresidente Primero durante el mandato de Armando Veganzones; Presidente de la Sección de Entidades Financieras entre 1993 y 1995; y de la Sección de Industrias Energéticas en 1989. Además, ha participado de forma activa en diferentes Comunidades y Comités desde su incorporación.


El encuentro celebrado en el Auditorio de La Fábrica Nacional de Moneda y Timbre contó con aforo completo y fue seguido por streaming por más de 300 personas

# El "V Congreso de Industria Conectada" se consolida como espacio de referencia de la Industria y de las pymes


El congreso se ha convertido en un espacio referente de divulgación, sensibilización e intercambio de experiencias y retos a los que se enfrenta el tejido industrial español y, en especial, las pymes.

El Ministerio de Industria, Comercio y Turismo (MINCOTUR) celebró el pasado 7 y 8 de noviembre en el Palacio de Congresos de Valencia el "V Congreso de Industria Conectada" bajo el título "El momento de la Industria". El encuentro, que contó con Argentina como país invitado, ha sido el de mayor dimensión desde su creación hasta ahora con más de 1500 inscritos, 855 asistentes, y más de 4000 visualizaciones en streaming.

La apertura institucional estuvo a cargo de la vicepresenta de la Asociación Española para la Calidad (AEC), Mayda López Belmonte, que durante su discurso destacó la importancia de la Industria en la creación de la AEC, que desde hace 61 años impulsa los valores de la Calidad gracias al apoyo de sus más de 1200 socios, y agradeció al Ministerio de Industria Comercio y Turismo (MINCOTUR) la confianza depositada un año más en nuestra Asociación como partner estratégico del V Congreso de Industria Conectada.

A continuación, fue el turno de intervención de las diversas autoridades de la Comunitat Valenciana y el Ayuntamiento de la ciudad. El primero, Borja Sanjuán Roca, concejal de Hacienda y Desarrollo Innovador de Sectores Económicos y Emprendimiento del Ayuntamiento de Valencia, que agradeció la celebración del encuentro en la ciudad de Valencia como una oportunidad para poner en valor el papel de las ciudades en la construcción de las industrias y viceversa; así como el impacto que ello provoca en la retención del talento local. Un argumento que reforzó el presidente de la Confederación Empresarial de la Comunitat Valenciana (CEV) y vicepresidente de la Confederación Española de Organizaciones Empresariales (CEOE), Salvador Navarro, que subrayó la importancia de contar con una industria competitiva, diversificada y de alto valor añadido, destacando que la Comunitat Valenciana cuenta con una industria sólida que representa el 10% del PIB de la industria española. Por último, y en esta misma línea, Rafael Climent, Conseller de Economía, Sectores Productivos, Comercio y Trabajo de la Generalitat Valenciana, destacó la importancia de la digitalización en la Industria en el nuevo escenario mundial.


En representación de Argentina, país invitado del encuentro, estuvo el secretario general de Industria y Desarrollo Productivo, José Ignacio de Mendiguren, que durante su intervención abordó la situación actual del país sudamericano que se encuentra en un proceso de cambio del modelo productivo, "apostando por el desarrollo de la industria 4.0".

Por último, y en representación del Ministerio de Defensa, el Jefe del Mando de Apoyo Logístico del Ejército de Tierra, Teniente General, García de las Hijas, agradeció a la ministra de Industria, Comercio y Turismo, Reyes Maroto, y al Secretario General de Industria y de la PYME, Raül Blanco, su apoyo durante la pandemia del Covid-19, y destacó la importancia del encuentro en un momento en el que las Fuerzas Armadas están en un proceso de transformación y modernización en el umbral 20 / 35.

El cierre de la bienvenida institucional estuvo a cargo de la Ministra de Industria, Comercio y Turismo del Gobierno de España, Reyes Maroto, que anunció la puesta en marcha de un Programa de Apoyo a los Digital Innovation Hubs (PADIH) dotado con 37,59 millones de euros. Según explicó el objetivo del programa es la creación en España de una red de centros europeos de innovación digital y aprovechar la capacidad que tienen estos centros para dotar a las pymes de las herramientas de digitalización avanzadas necesarias para hacer frente a los retos que se derivan de la transición digital. Con ello se »


» pretende crear 25 Digital Innovation Hubs en España y contribuir a la digitalización de 1.253 pymes. También destacó el redimensionamiento del evento queriendo ser un espacio que aúne a toda la industria y las pymes y en el que no solo se hable de Industria 4.0, sino de todos los retos a abordar para la transformación verde y digital de la industria y pymes nacionales.

## Un Congreso de referencia para la Industria y las PYMES

El "V Congreso de Industria Conectada" impulsado por el Ministerio de Industria, Comercio y Turismo se ha convertido en un espacio referente de divulgación, sensibilización e intercambio de experiencias y retos para la industria nacional con una clara vocación e influencia internacional.

En concreto, este año ha tenido una duración de dos jornadas, ha contado con 190 ponentes, 7 salas y 50 mesas de trabajo. Además, ha contado con el apoyo de marcas impulsoras como Accenture, AENOR, Nippon, Siemens y Telefónica. Además del apoyo institucional de la Empresa Nacional de Innovación (ENISA), la Escuela de Organización Industrial (EOI), la Oficina Española de Patentes y Marcas, el Ayuntamiento de Valencia y la Generalitat Valenciana.

Durante las dos jornadas se ha hablado de emprendimiento, innovación, digitalización y habilitadores, formación, entornos colaborativos, ayudas públicas en el marco de los Fondos de Recuperación o soberanía industrial, abordando todos estos temas desde el punto de vista sectorial y de la administración, enriqueciendo de esta manera el debate y acercando al tejido industrial las acciones puestas en marcha para la mejora de su competitividad, trasformación y resiliencia.

# *Premios Nacionales Industria Conectada 4.0*

Durante el Congreso se ha hecho entrega de los “IV Premios Nacionales Industria Conectada 4.0” que tras la deliberación del jurado han recaído en BIOLAN MICROBIOSENSORES en la categoría de Pyme, y REPSOL en la categoría de gran empresa. Han quedado finalistas: Bodega Matarromera y Michelin.



Los Premios Nacionales de Industria Conectada 4.0 nacen con el objetivo de reconocer a aquellas organizaciones, empresas e industrias que hayan realizado un esfuerzo destacado en su transformación digital, logrando la excelencia empresarial en actividades encuadradas en la Sección C, Divisiones 10 a 32, de la Clasificación Nacional de Actividades Económicas 2009 (CNAE 2009). Asimismo, buscan otorgar un mayor prestigio social al sector industrial, presentándolo en un entorno de calidad y de excelencia, reconociendo los méritos de las empresas industriales que destaquen por sus proyectos y acciones de digitalización y por sus planes de innovación en materia de organización y procesos bajo las principales dimensiones que definen el paradigma de la Industria Conectada 4.0: Estrategia de Negocio y Mercado, Procesos, Organización y Personas, Infraestructuras, y Productos y Servicios.

Pueden acceder a más contenido del CIC40 a través de este QR

# Actividades de nuestros espacios de relación

*Diciembre*

14 Dic
**V Congreso de Privacidad Club DPD**
*"Diálogos de DPDs"*

*Noviembre*

17 Nov
**Día Mundial de la Calidad 2022**
*"Digicalidad"*

7 y 8 Nov
**V Congreso de Industria Conectada**
*"El momento de la industria"*

*Octubre*

27 Oct
**V Congreso AEC Open Experience**
*"Organizaciones CX 5.0. Preferidas de empleados. Favoritas de clientes"*

25 Oct
**Canal AEC**
*II Insight Club DPD 2022*

19 y 20 Oct
**I Congreso de la Industria de Canarias**
*"Estrategia de Desarrollo Industrial de Canarias 2022-2027 (EDIC)"*

6 Oct
**Canal AEC**
*"Nueva Directiva de Debida Diligencia de la UE: impacto en Sostenibilidad"*

*Septiembre*

CLUBAECDPD

# El Club del DPD de la Asociación Española para la Calidad celebra el **"V CONGRESO PRIVACIDAD DIÁLOGOS DE DPDs"**

**El Club del DPD de la Asociación Española para la Calidad (AEC) celebró el pasado 14 de diciembre el "V Congreso Privacidad "Diálogos DPDs" en el Espacio Fundación Telefónica, Madrid. La cita, que contó con más de 100 asistentes presenciales y más de 500 visualizaciones online, estuvo a cargo de Alberto González, director de Operaciones, TI y Gestor del Club DPD de la AEC, que ejerció como conductor del encuentro que se ha convertido en un espacio de referencia para el sector.**


Con la colaboración de Telefónica Tech y Govertis como Partners Estratégicos, la cita arrancó con la bienvenida institucional de María Jesús Almazor, CEO de Cyber&Cloud de Telefónica Tech, y Avelino Brito, director general de la Asociación Española para la Calidad.

Ambos representantes institucionales coincidieron en la importancia de la ciberseguridad y el tratamiento de los datos de una forma responsable en estos momentos de transformación digital. Y Avelino Brito puso también el foco en el "factor humano" poniendo de relieve la importancia que tiene su figura, y la excelente labor de la Agencia Española de Protección de Datos.

Adrián Palma, Profesor de Derecho Administrativo de la Universidad de Valencia y miembro del área de privacidad de OdiseIA, fue el encargado de abrir la jornada con la ponencia "El cumplimiento de la protección de datos de carácter personal en el ciclo de vida de los sistemas de IA: Una aproximación práctica para los DPDs que habló sobre las implicaciones legales presentes durante el ciclo de vida de los sistemas de inteligencia artificial tomando como referencia la normativa de protección de datos personales. Poniendo especial énfasis en la importancia del principio de privacidad desde el diseño en las fases iniciales del desarrollo de los sistemas de IA. Y, por último, destacó los retos que supondrá para los DPDs la integración y superposición del futuro reglamento de inteligencia artificial y el Reglamento General de Protección de Datos. »

CLUBAECDPD



» A continuación, Boris Delgado, director de Soluciones de Digitalización y Tecnología, de AENOR, trató "La nueva ISO 27001: 2022 integrando ciberseguridad y privacidad" en la que expuso "el Ecosistema Digital para responder a las distintas necesidades de las organizaciones en ciberseguridad. Se enfocó en la experiencia sobre la certificación ISO/IEC 27001-Sistema de Gestión de Seguridad de la Información y los aspectos clave de la nueva versión del estándar, la cual se adapta a los nuevos riesgos que amenazan a las organizaciones, aportando una solución a la organización a través del análisis de riesgos y mejora continua de sus procesos de negocio y servicios de TIC.

La primera mesa de debate estuvo a cargo de Eduard Chaveli, Head of Consulting Strategy en Govertis, que moderó un encuentro dedicado a abordar protección de datos, compliance y canal de denuncias. Analizando los antecedentes e implicaciones de la directiva europea en un encuentro titulado "Canales de denuncias y privacidad ante la inminente transposición Directiva Whistleblowing" que contó con la partipación de Jordi Morera, Lead Advisor Compliance, Govertis; Mayra Conesa, Manager de Compliance y Buen Gobierno, AENOR; y Sandra Garcinuño, Senior Manager Compliance, Telefónica.

A mediodía, y tras un espacio para el networking, Óscar Bou, Head of Consulting Business en Govertis, moderó la mesa "Protección de datos en el sector público" que abordó, entre otros asuntos, el Esquema Nacional de Seguridad de la mano de Fernando Suárez, Director del Área de Transparencia y Gobierno Abierto de la Diputación de Ourense; Juan Enrique Vión, Delegado de Protección de Datos y Jefe de Servicio de Transparencia, Participación ciudadana, Calidad y Atención al ciudadano de la Diputación de Badajoz; Francisco López, Jefe del Servicio de Prevención Sanidad y Consumo del Ayuntamiento de Xirivella; y Marcos Almeida, DPD de la Universidad de Santiago de Compostela.




A continuación, fue el turno de participación de los dos ganadores del concurso de ponencias para el "V Congreso Privacidad "Diálogos DPDs", Carlos Fernández, DPD de la Secretaría de Estado de Seguridad (Ministerio del Interior), que abordó "La relación entre de los DPDs de las organizaciones y los de las autoridades competentes ante la aplicación de la normativa especial de tratamiento de datos personales con finalidad de prevención, detección e investigación de delitos"; y José Ignacio Atance, CEO de Acudata, que expuso su ponencia "Neurodatos: privacidad y riesgos del cerebro conectado".

Por último, los asistentes pudieron escuchar la ponencia conjunta de Javier Cao, Cybersecurity, Privacy and IT Risk Leader en Govertis; y Martiniano Mallavibarrena, Global Head of DFIR & Threat Hunting de Telefónica Tech que analizaron la "Gestión práctica de Incidentes desde una perspectiva tanto operativa como normativa". Dando paso a María Rosario Heras, responsable de la Secretaría Permanente de la Red Iberoamericana de Protección de Datos, y jefe de la división de Relaciones Internacionales de la Agencia Española de Protección de Datos, que cerró la jornada aportando una visión internacional con su ponencia "La certificación de DPD: Una visión Iberoamericana".

La clausura del "V Congreso Privacidad "Diálogos DPDs" estuvo a cargo de Julián Prieto, subdirector de Promoción y Autorizaciones de la Agencia Española de Protección de Datos (AEPD) que en su intervención abordó la función del DPD como elemento clave para el cumplimiento de la normativa, y como garantía del derecho fundamental de la protección de datos.

# *El Club DPD de la AEC celebra el II Insight del 2022 bajo la temática del "Metaverso: implicaciones jurídicas prácticas, con especial referencia a privacidad"*

**La Asociación Española para la Calidad, AEC, celebró el pasado 25 de octubre el segundo Insight del año. El Club DPD de la AEC, con más de 275 profesionales, es el primer Club en España dirigido a la Comunidad de Delegados de Protección de Datos, un espacio referente en conocimiento, intercambio de experiencias y buenas prácticas para la profesión.**

El encuentro, bajo el título "Metaverso: implicaciones jurídicas prácticas y con especial referencia a privacidad", estuvo a cargo de Alberto González, director de Operaciones y TI, Gestor del Club DPD de la AEC; y la conducción de Eduard Chaveli, Head of Consulting Strategy de Govertis, una compañía de Telefónica Tech.

Óscar Casado Oliva, Legal Director Privacy, IP & Digital Business de Telefónica, fue el encargado de abrir la jornada con su ponencia "Metaverso: implicaciones jurídicas prácticas, con especial referencia a privacidad". A continuación, Lorenzo Cotino Hueso, Catedrático de Derecho Constitucional de la Universidad de Valencia, profundizó en la temática a través de su charla "Hay privacidad más allá de la Privacidad: intersecciones con otros marcos normativos", dando paso al taller exclusivo para miembros del Club DPD a cargo de Lucía Arías, Responsable del Centro de Excelencia en GOVERTIS, que abordó "El nuevo Esquema Nacional de Seguridad (RD 311/2022)".

COMUNIDADAECEXPERIENCIADECLIENTE

# *V Edición del Congreso AEC Open Experience "Organizaciones CX 5.0: Preferidas de empleados. Favoritas de clientes"*



**La Asociación Española para la Calidad, AEC, celebró el "V Congreso AEC Open Experience" organizado por la Comunidad AEC Experiencia de Cliente, bajo el lema "Organizaciones CX 5.0: Preferidas de empleados. Favoritas de clientes". La cita contó con aforo completo y se desarrolló de forma presencial en el Auditorio BNP Paribas, Madrid, con la conducción de la periodista Teresa Viejo.**

La bienvenida institucional estuvo a cargo del director general de la AEC, Avelino Brito, y Alicia García, presidenta de la Comunidad AEC Experiencia de Cliente. Ambos coincidieron en destacar la importancia de Comunidad "como un punto de encuentro para compartir, conocer e impulsar la cultura de la experiencia de cliente". Así mismo, Alicia García profundizó "en el valor que aporta la Experiencia de Cliente, su impacto en el negocio y su capacidad de transformación cultural de las empresas", señalando las herramientas disponibles a través de la comunidad para alcanzar ese objetivo, tales como el site de la comunidad, el blog y el grupo de LinkedIn, a través de los que se busca perdurabilidad e influencia del grupo y de la disciplina en los canales online, así sí como la apuesta por eventos "experienciales, relacionales y emocionales" entre los canales off line.

La programación arrancó con la intervención de Igor Romero, EMEA Solutions Principal, de Medallia, partner impulsor de la Comunidad AEC de Experiencia de Cliente; y Guillermo Calderón, director de Experiencia de Cliente de Generali, que abordaron:"¿Cómo hacer que tu organización respire Cliente?". Un diálogo en primera persona que relató la experiencia de Generali que, con la ayuda de Medallia, consiguió alcanzar el objetivo de integrar la experiencia de cliente como disciplina en todos los puntos de contacto, adoptando un enfoque multifuncional, en el que todos los departamentos están involucrados.

A continuación, Alberto López, director Comercial de Porsche, estuvo a cargo de la conferencia “Experiencia de marca para toda la vida” en la que explicó la importancia de llevar la cultura de “experiencia y promesa de marca a toda la red”, trasladando la experiencia de cliente en todos los puntos de contacto, y convirtiéndola en una experiencia para toda la vida. Así, y tras un breve descanso para el café y networking en el que se realizó una encuesta entre los vocales para saber cuáles son los temas de interés, el congreso dio paso a la conferencia “Impacto económico de la experiencia de cliente” a cargo de Antonio Monje, Customer Experience & Innovation Lead, de ING, que abordó la fórmula para convertir la experiencia de cliente en un asunto tangible que permita su rentabilidad.

Por último, la gran cita del anual de la Comunidad AEC Experiencia de Cliente dio paso a la mesa “Experiencia de empleado y RRHH: retos y oportunidades en el nuevo entorno”. Un encuentro que contó con la participación de Fernanda Armada, director of Employee Experience, de Willis Tower Watson; Cristina Magdalena, Executive Partner, Gartner; Elena Franchi, Head of Business Development, de Château Forum España; y Massimo Begelle, Regional Manager, de Top Employers Institute.

La clausura del congreso estuvo a cargo de la presidenta de la Comunidad AEC Experiencia de Cliente, Alicia García, que agradeció a los asistentes.



COMITÉ**AEC**INDUSTRIAS Y SERVICIOS PARA LA DEFENSA

# *Se celebró la 129ª Reunión Plenaria del Comité AEC de Industrias y Servicios para la Defensa*

**El Comité AEC de Industrias y Servicios para la Defensa celebró su 129ª Reunión Plenaria el pasado 29 de noviembre, de manera presencial, en las instalaciones del INTA.** En el encuentro se presentó la propuesta de Planificación de Actividades del Comité para el 2023, y se revisó el seguimiento de las actividades del Grupo de Trabajo sobre “Calidad software”. Además, se comunicó a los asistentes que se daba comienzo al proceso de recepción de candidaturas para la presidencia del Comité; ya que la legislatura de 4 años del presidente Felix Torres de INDRA ha concluido.


Entre los temas de interés para el próximo año destacan: calidad del software, la nueva edición de la norma PECAL 2210, normas PECON, y Aeronavegabilidad, normas PERAM. La próxima cita del Comité está planificada para el mes de febrero del 2023.

AECCICAN

# *La AEC y la Consejería de Turismo, Industria y Comercio del Gobierno de Canarias celebran el "I Congreso de la Industria de Canarias"*




**La cita tuvo lugar el pasado 19 y 20 de octubre en el Auditorio Adán Martín de Santa Cruz de Tenerife**

El I Congreso de la Industria de Canarias reunió a finales de octubre a una treintena de ponentes de reconocido prestigio, líderes institucionales, empresariales y profesionales, además de la asistencia estimada de más de 250 agentes del ecosistema industrial canario, para poner en común conocimiento y experiencia a lo largo de diversas conferencias, entrevistas, mesas de debate y presentaciones de casos de éxito de crecimiento empresarial en Canarias.

El Congreso se enmarca dentro de la Estrategia de Desarrollo Industrial de Canarias 2022-2027, que recoge objetivos, actuaciones y medidas para generar un cambio positivo y relevante en el papel de la industria para la economía canaria, y que da origen al lema del CICAN 'el impulso de nuestra industria'.

Tras la bienvenida institucional a cargo de Yaiza Castilla, consejera de Turismo, Industria y Comercio, Gobierno de Canarias, el programa arrancó con la presentación de la "Estrategia de Desarrollo Industrial de Canarias 2022-2027 (EDIC)". Un documento que según explicó el viceconsejero de Industria, Comercio y Consumo del Gobierno de Canarias, Justo Artiles, identifica una visión para la industria canaria y unos objetivos orientados específicamente a generar impulso y promover el desarrollo del sector industrial de las Islas.

A continuación, intervino el director general de Industria y de la Pyme del Ministerio de Industria, Comercio y Turismo (MINCOTUR), Galo Gutiérrez, que presentó los programas de ayudas del MINCOTUR en la conferencia **"Apoyo a proyectos para la transición industrial".**

La primera mesa debate **"Manufactura"** estuvo moderada por el viceconsejero de Industria, Comercio y Consumo del Gobierno de Canarias, Justo Artiles, y contó con la participación de Naveen Mehra, consejera delegada de la Compañía Cervecera de Canarias; Raquel Malo, CEO de Protisa; Javier Marrero, CEO de Biomca Química, SL; y José Luis León, director general de Aguas Minerales de Firgas.

La segunda mesa "**Formación y Talento"** estuvo a cargo de Raúl García, presidente de la Asociación Industrial de Canarias (ASINCA), y en ella participaron Rosa María Aguilar, Rectora de la Universidad de La Laguna y miembro de la Conferencia de Rectores de las Universidades Españolas (CRUE); Vicente Marrero, presidente de la Confederación Regional de Empresarios del Metal (CREM); Julen Elgeta, presidente de Hetel y Juan Ángel Gómez, director de Recursos Humanos de Schreiber Foods Canarias.

Por la tarde la cita continúo con la conferencia "**¿Cómo las empresas y los profesionales pueden afrontar los retos y desafíos de la Cuarta Revolución Industrial?"** de Luis Pardo, CEO de focus in growth: Leadership/ Digitalization/ Sustainability, que dio paso a la mesa de debate sobre **"Sostenibilidad"** moderada por David Padrón, director general de Investigación y Coordinación del Desarrollo Sostenible del Gobierno de Canarias, que contó con la participación de Íñigo Núñez, CEO de Ewaste Canarias; Susana García, Segment Marketing Manager para Sur de Europa de Carburos Metálicos; y Federico León, director técnico de ELMASA Tecnología del Agua.

La última actividad del día estuvo a cargo de nuestro director general, Avelino Brito, que hizo las veces de moderador y realizó una **"Entrevista"** a Jorge Barrero, director general de la Fundación COTEC para la Innovación.

## Segunda Jornada.

El segundo día de Congreso comenzó con la mesa debate "**Digitalización: ¿Retos en la digitalización de la industria?"** moderada por la directora general de Industria del Gobierno de Canarias, Yolanda Luaces, y la participación de Jordi Llinares, subdirector general de Digitalización de la Industria y Entornos Colaborativos del Ministerio de Industria, Comercio y Turismo; Jorge Sánchez, director general de Aperitivos Snack; y Oswaldo Brito, presidente del clúster Canarias Excelencia Tecnológica.

A continuación, Gabriel Megías, gerente del Instituto Tecnológico de Canaria, presentó la conferencia "**Impulso del Instituto Tecnológico de Canarias a la industria canaria"**, dando paso a continuación a la presentación de tres casos de éxito de crecimiento empresarial, de Esteban Alberto Pérez, director general del Grupo Ganaderos de Fuerteventura (Maxorata); José Luis Fernández, director de Desarrollo de Negocio de Industrial Recense; y Martín Tabares, CEO de Klingele Embalajes Canarias.

Por último, se procedió a celebrar la **"Conferencia Inspiradora"** de Enrique Dans, conferenciante inspirador & Senior Advisor for Innovation and Digital Transformation, IE Business School.

## Premio Excelencia Empresarial

Al cierre de la jornada se procedió a la entrega de la "**XI Edición del Premio Canario a la Excelencia Empresarial",** en la que resultaron ganadoras las empresas **Subsea Mechatronics,** en la modalidad de Pequeña Empresa no Industrial; **Ascanio Química,** en la categoría de Pequeña Empresa Industrial; y **Brok Air Aviation Group** en la modalidad de Mediana-Gran Empresa.

Asimismo, resultaron distinguidas en el marco de este premio con menciones especiales la firma Asesoramientos Agronómicos Canarios en la modalidad de pequeña empresa no industrial; Lavatur Canarias y Publiservic Canarias, en la modalidad pequeña empresa industrial; y Bioksan Naturalmente Juntos, y Explotaciones y Apartamentos Balcón del Mar en la modalidad de mediana-gran empresa.

Creado en 2009 por el Gobierno de Canarias, el Premio Canario a la Excelencia Empresarial es un galardón de referencia para el mundo empresarial y promueve los principios de excelencia, innovación y competitividad en la labor de gestión que desarrollan las compañías del Archipiélago.

El CICAN 2022 se organizó con la colaboración de la Asociación Española de Calidad, el Instituto Tecnológico de Canarias (ITC) y la Asociación Industrial de Canarias (ASINCA).

COMUNIDADAECCALIDAD

# *La Comunidad AEC Calidad presenta una herramienta de autodiagnóstico de excelencia operacional*

**La Comisión de Excelencia Operacional de la Comunidad AEC Calidad ha lanzado un método de autodiagnóstico que ayuda a identificar las herramientas de excelencia operacional y buenas prácticas que dan respuesta a muchos de los problemas que sufren las empresas.**

El objetivo de ésta es proporcionar una recomendación genérica de herramientas a los problemas que las organizaciones han identificado previamente. De esta manera, con la herramienta se puede buscar y seleccionar un problema y, una vez seleccionado, se obtiene información priorizada de las herramientas más adecuadas para superarlo y, además, se hace una autoevaluación con respecto a las buenas prácticas de cada una.

Una vez realizado el proceso, que consta de 3 sencillos pasos, se obtiene un informe para cada problema con las herramientas que le pueden ayudar, su priorización y los resultados de la evaluación frente a cada una de ellas.


**Accede ahora al autodiagnóstico, se trata de una herramienta de acceso libre para cualquier socio de la AEC.**

# *La Comunidad de Calidad elabora un documento que relaciona los requisitos de la especificación UNE 0060:2018 "Sistema de gestión para la digitalización. Requisitos" con las herramientas y técnicas propias de la ingeniería de la calidad*

**La Comisión de Ingeniería de la Calidad de la Comunidad AEC Calidad, consciente de la importancia que el cambio a la digitalización tiene para las empresas en el suministro de sus productos y servicios, ha elaborado un documento en el que ha relacionado los requisitos de la especificación UNE 0060:2018 "Sistema de gestión para la digitalización. Requisitos" con las herramientas y técnicas propias de la ingeniería de la calidad.**

Los puntos incluidos en el documento se han extraído de los capítulos siete, Operación, y del ocho, Innovación, de la especificación. La Comisión ha considerado que la aportación sobre estos dos apartados de la UNE 0060 de la ingeniería de la calidad puede ser significativa, por lo que contribuirá, en consecuencia, a la mejora de la eficacia y eficiencia en la gestión de la Norma.

Para cada capítulo de la especificación se describen los requisitos del sistema de gestión de acuerdo a la UNE 0060:2018 y, a continuación, se desarrolla la referencia a las distintas herramientas y metodologías de la ingeniería que son aplicables para el cumplimiento de estos requisitos.

**DESCARGA**

COMUNIDAD**AEC**INNOVACIÓN

# *Arranca este el ciclo "Viernes de Innovación"*

**La Comunidad AEC de Innovación arrancó el pasado viernes 16 de diciembre el ciclo "Viernes de Innovación". Un formato dinámico de encuentro pensado en movilizar y centralizar la actividad de las más de 250 personas y 150 empresas que conforman la Comunidad.**

Bajo la premisa de reconectar y dar a conocer la actividad en torno a la innovación que realiza cada una de las empresas y profesionales participantes, se reunirán un viernes al mes en un encuentro que tendrá 45 minutos de duración, divididos en una charla tipo TED, un espacio para las preguntas, y un momento para el networking.

En este primer encuentro, los asistentes pudieron conocer de primera mano la estrategia de innovación en digitalización de AIRBUS. El próximo contará con la participación de la entidad financiera CAJAMAR.


ACUERDOS**AEC**

# *Nippon Gases firma un acuerdo de patrocinio con la AEC*

**La colaboración entre la AEC y Nippon Gases permitirá impulsar la calidad a través de objetivos comunes.**

Nippon Gases, una de las principales empresas mundiales de gases industriales y la Asociación Española para la Calidad – AEC han firmado un acuerdo de colaboración el pasado 15 de diciembre.

La Asociación Española para la Calidad es una organización sin ánimo de lucro, fundada en 1961 y cuyo propósito es el de impulsar la calidad como motor de la competitividad y la sostenibilidad de los profesionales y las empresas del país. En la actualidad son más de 1.000 empresas y de 3.500 profesionales comprometidos con la misión de la AEC, quienes hacen de la Asociación Española para la Calidad una de las comunidades empresariales de referencia para el impulso transformador de nuestra economía.

De esta manera, Nippon Gases se une a Thales, Aenor, Medallia, Johnson&Johnson, Trigo y Brains International School como patrocinadores de la AEC en su objetivo por promover un entorno empresarial de calidad mediante la difusión de conocimiento, contenidos y realización de sinergias conjuntas encaminadas a lograr una industria de calidad compartiendo *know-how.*


AECINSTITUCIONAL

# *Beatriz López Gil participa en el «I Foro Español Mujer y Sociedad Civil» organizado por la Cámara de Comercio de Madrid*

**La presidenta de la AEC, Beatriz López Gil, participó el pasado 26 de octubre en el I Foro Español Mujer y Sociedad Civil organizado por la Escuela de Negocios de la Cámara de Comercio de Madrid que abordó el papel de la mujer en diversos aspectos empresariales, con el objetivo de potenciar la igualdad de género dentro del tejido empresarial madrileño e impulsar el liderazgo femenino.**

La cita tuvo lugar los días 26 y 27 de octubre en el Aula Magna de la Escuela de Negocios de la Cámara de Madrid, fue inaugurado por la directora general de Igualdad de la Comunidad de Madrid, Patricia Reyes Rivera, y la vicepresidenta primera de la Cámara de Comercio e Industria y Servicios de Madrid y presidenta de la Asociación Española de Mujeres Empresarias ASEME, Eva Serrano.

La primera jornada del I Foro Español de Mujer y Sociedad Civil contó con varias mesas redondas sobre 'Mujeres Liderando la Educación'; 'Mujeres y Responsabilidad Social'; 'Mujeres en la gestión y desarrollo de personas' y 'Sostenibilidad y la aportación de la mujer', moderada por Rut Ballesteros Gil, miembro de la Junta Directiva de la AEC. A continuación, dió paso a un debate sobre 'Mujeres liderando la Sociedad Civil / Asociaciones', que contó con la participación entre otras figuras de la presidenta de la AEC, Beatriz López Gil; la presidenta de EJECON, Asociación Española de Ejecutivos y Consejeros y presidenta de la Fundación Wolters Kluwer; Carmen Panadero, presidenta de WIRES; o María Rosa Rotondo, presidenta de la Asociación de Profesionales de las Relaciones Institucionales y de la Plataforma Europea de Asuntos Públicos. La segunda jornada comenzó con una mesa redonda en torno a la figura de la 'Mujer y Abogacía' en la que participaron cinco mujeres referentes dentro del sector jurídico. Continuó con un encuentro sobre 'Mujeres Liderando la empresa' y otra mesa redonda sobre 'El futuro de la Sociedad Civil en España'.

El encuentro concluyó con la intervención de la periodista Marta Pastor, directora de programas que fomentan el empoderamiento de la mujer como "Ellas Pueden" y "Sin Género de Duda".

AECFORMACIÓN

# *La Asociación Española para la Calidad lanza su Catálogo de Formación 2023*


**Como actividad fundamental la AEC acompaña a sus socios, empresas y profesionales en sus necesidades formativas como un aliado estratégico de confianza. La AEC nace en 1961, momento de extraordinarios cambios, desde el compromiso de profesionales que creen en la Calidad como una disciplina capaz de impulsar a sus empresas y a su país.**

A lo largo de nuestra trayectoria son más de 65.000 los profesionales y empresas que han confiado en nuestra formación para impulsar sus carreras. Y hoy, más que nunca, seguimos en esta senda, mejorando y haciendo crecer nuestra formación ONLINE, ampliando nuestra metodología formativa EN DIRECTO para hacerla llegar a todos, sea cual sea la ubicación en la que se encuentren; y recuperando la formación PRESENCIAL para todos aquellos que prefieran participar desde nuestras aulas físicas.

En un entorno nunca visto en generaciones, en estado de transformación permanente, volvemos a ser protagonistas del cambio. En estos años tan retadores, inspirada en su misma misión fundacional, la AEC se reinventa y se potencia con la transformación digital en todos sus servicios.

Como grandes proyectos para este año, seguimos ampliando nuestra fortaleza formativa en los Sistemas de Gestión y potenciando las materias más actuales y clave para la competitividad de las organizaciones: Sostenibilidad y Gestión de la Energía, Excelencia Operacional e Innovación, Protección de Datos, Ciberseguridad y Seguridad de la Información. Nuestra formación, espacios de relación, comunidades, comités, y eventos se pueden vivir de forma presencial y virtual, sin limitaciones, multiplicando las posibilidades de elección. Y hemos creado y consolidado nuevos servicios como el Canal AEC, para difundir la actualidad más relevante en Calidad y Gestión.

En la actualidad más de 800 empresas y de 3.500 profesionales comprometidos con la misión de la AEC, hacen de la Asociación Española para la Calidad una de las comunidades empresariales de referencia en el impulso transformador de nuestra economía.

## Entidades colaboradoras

buljan& partners · GOVERTIS Part of Telefónica Tech · TRIGO Global Quality Solutions · ControlSolutions International · creara · milagros moreno · ECOCUADRADO · ACE-IGS · ARN Consulting · AyC · cavala · Quid Qualitas · SinCeO2 · Sisteplant · Smart&City · EQA · Futura Soluciones · grupoInnova · Kamaleon · strategos inowa · SYGS · ThinkersC · WORLD LEX

## Profesionales

- Alfredo Rozalén Tato
- Ana Mª Corbalán
- Andrés Redchuck
- Antonio José Fernández
- Carlos Capacés
- Emilio López
- Félix Gómez
- Fredy Alarcón Duque
- Francisco Aguilera
- Gisela Villasevil Pau
- Iván Ludeña
- Jenny Lorena Victoria
- Jesús Atienza
- José Ruiz-Canela
- José Vilar
- Juan Torrubiano
- Julián Román
- Luis F. Rubio
- María Jesús Ruiz
- Mariano Prieto
- Miguel Ángel Escalona
- Miguel Ángel Fernández
- Paco Corma
- Paloma Fuentes
- Patricia Acosta
- Pelayo Benito
- Rafael Lucero
- Raquel San Antonio
- Susana Jiménez
- Tomasz Smardzewski
- Vicente Córdoba
- Virginia Martín

NOMBRAMIENTOS**AEC**

# Victoria Muriel, *nueva presidenta del Comité AEC Industrias de la Moda*

**La Manager de Sostenibilidad de Loewe (LVMH) sustituye en el cargo a José Luis Velasco, que ha liderado este espacio desde el año 2016.**

Victoria Muriel Miguel, manager de Sostenibilidad en Loewe (LVMH), ha asumido la presidencia del Comité AEC Industrias de la Moda, cargo que hasta la fecha ostentaba José Luis Velasco Escudero, EMA Regional Quality Manager, Flow Control Division (FCD) de Flowserve.

En su plan de actuación, la nueva presidenta ha anunciado que quiere continuar con los objetivos marcados por su predecesor. Asimismo, se ha propuesto fomentar la participación de las empresas miembros para conocer sus expectativas, fortalezas y temas de interés. Además de impulsar la participación de empresas externas como consultoras de sostenibilidad, empresas de innovación y escuelas de moda y universidades. El objetivo de estas propuestas es promover las colaboraciones beneficiosas para todas las partes.

El cambio de presidencia se ha hecho público durante la celebración de la 46ª reunión plenaria del Comité AEC, celebrada el 11 de octubre en las instalaciones de la Asociación. En el marco de este encuentro, la AEC ha querido reconocer la labor de José Luis Velasco, y el director general de la AEC, Avelino Brito, le ha hecho entrega de un diploma en reconocimiento y agradecimiento por su compromiso personal, entrega y su valiosa contribución como presidente del Comité.

## Sobre Victoria Muriel

*La nueva presidenta es licenciada en Biología por la Universidad Complutense de Madrid y cuenta con un Máster en Gestión Integrada en CFE y Programa de Dirección de Proyectos de la EOI. Inició su carrera profesional en diferentes sectores, pero su pasión por la moda le llevó hace seis años a formar parte de LOEWE, donde lidera los proyectos de Sostenibilidad de la marca.*

# David Verano, *nuevo presidente del Comité AEC Agroalimentario*

**El Comité AEC Agroalimentario ha designado a David Verano, director de Certificación de Kiwa España, como nuevo presidente de este foro de referencia, debate e información para toda la cadena de valor del sector agroalimentario.**

Con más de 20 años de experiencia en el sector agroalimentario, David Verano se ha propuesto liderar este Comité con el objetivo de ampliar el número de miembros y dotarlo de una mayor visibilidad través de webinars o jornadas donde se promuevan temáticas de interés para el sector y los miembros del Comité.

En su programa de actuación también se ha propuesto convertir al Comité en un foro de discusión sobre las nuevas tendencias, que afectan a los profesionales que trabajan en el ámbito de la calidad en este sector.

La presentación del nuevo presidente se realizará en la próxima reunión plenaria del Comité AEC, cita en la que David Verano elegirá a su equipo de gobierno y propondrá las nuevas actividades para el plan operativo del Comité.

## Sobre David Verano

*El nuevo presidente es licenciado en Ciencias Químicas, especialidad Química Analítica, por la UCM. Además, cuenta con un máster en Calidad y Medio Ambiente por IDE CESEM. Ha trabajado en el ámbito de la calidad y la seguridad alimentaria desde el año 1998, tanto en laboratorios (públicos y privados), Industria agroalimentaria (Jefe de calidad y Medio ambiente de Pedro Domecq del año 1999 al 2001) y en entidades de certificación como AENOR (primer auditor IFS en España y como Director del área agroalimentaria), hasta su cargo actual en Kiwa España, multinacional neerlandesa especializada en certificación agroalimentaria en España.*

»

# Ramón Mayor Gambín, *nuevo presidente del Comité AEC Aeroespacial*

**Con esa designación, Ramón Mayor, responsable de Calidad de los Programas de Aviación Militar en Airbus Defence & Space, sustituye en el cargo a Segundo Sánchez, Head of Operations A350 & Composites Manufacturing en Airbus.**

Ramón Mayor, responsable de Calidad de los Programas de Aviación Militar de Airbus Defence & Space, ha sido designado como presidente del Comité AEC Aeroespacial para los próximos cuatro años.

El nuevo presidente ha señalado en su candidatura que quiere mantener el legado del trabajo realizado por su predecesor, Segundo Sánchez, Head of Operations A350 & Composites Manufacturing en Airbus; y se ha propuesto, además, trabajar para que este sector sea un referente de calidad a nivel mundial. Entre sus objetivos planteados, Ramón Mayor quiere que los vocales de este foro de relación estén al día en cuanto a las últimas tendencias en herramientas de gestión de calidad y excelencia operacional, organizando sesiones con expertos del sector y con visitas a empresas para conocer in situ las tecnologías y procesos, que han sido clave para su éxito. Además, seguirá fomentando las relaciones con la Administración, autoridades, TEDAE, otros proveedores de la cadena de suministro y clústers del sector.

La presentación del nuevo presidente se ha producido durante la celebración de la 31ª reunión plenaria del Comité en las instalaciones de Aciturri en Miranda de Ebro. En el marco de ésta, Ramón Mayor se ha dirigido a los vocales y ha presentado a su órgano de gobierno.

## Sobre Ramón Mayor

*El nuevo presidente es Ingeniero Técnico Superior Aeronáutico, Master APQP, Black Belt (Arizona State University), PMP certified y Auditor interno del Sistema de Calidad. A lo largo de su carrera profesional ha trabajado en distintos puestos y programas del sector aeroespacial: cualificación de proveedores en Airbus, aseguramiento de la calidad de los Servicios prestados flota española del programa Eurofighter, ha sido el responsable de Calidad de Eurofighter GmbH (en Munich) y ha desplegado las herramientas de mejora como el APQP en Airbus DS.*

Nombramientos

# Adrián Palma Ortigosa

## Profesor de Derecho Administrativo de la Universidad de Valencia y miembro del área de privacidad de OdiseIA

**Karen Von Burucker**

Directora de Comunicación y RRII. **Asociación Española para la Calidad, AEC**

kvonburucker@aec.es

www.linkedin.com/in/karenvonburucker

Artículo publicado en el portal elderecho.com

**Entrevistamos a Adrián Palma Ortigosa, Profesor de Derecho Administrativo de la Universidad de Valencia y miembro del área de privacidad de OdiseIA, con motivo de la reciente celebración del Congreso del DPD, organizado por la AEC, y su ponencia: *"El cumplimiento de la protección de datos de carácter personal en el ciclo de vida de los sistemas de IA: Una aproximación práctica para los DPD"*.**

**Hola Adrián, para empezar y pensando en aquellos lectores que no conozcan el área de privacidad de OdiseIA ¿podrías presentárnosla e indicar quiénes forman parte de ella?**

Antes de nada me gustaría comenzar mencionando el papel de OdiseIA, se trata de uno de los observatorios sobre inteligencia artificial más importantes a nivel nacional formado por expertos de diferentes ramas del conocimiento y sectores productivos que tiene como objetivo velar por el buen uso de la inteligencia artificial. Dentro de esta organización, el área de privacidad, de la cual es director Lorenzo Cotino Hueso y de la que formo parte, analiza las implicaciones legales que tiene el uso de sistemas de inteligencia artificial sobre la normativa de protección de datos. Esta área está integrada por una serie de expertos y expertas sobre privacidad procedentes tanto del ámbito privado como público. Entre los trabajaos que hemos realizado se encuentra la "GuIA de buenas prácticas en el uso de la inteligencia artificial ética".

**Tu ponencia versa sobre el cumplimiento de la normativa de Protección de DDPP en el ciclo de vida de los sistemas de IA. ¿Qué hemos de entender por ciclo de vida de los sistemas de IA? ¿Cuándo empieza y cuando termina?**

El ciclo de vida de los sistemas de IA está integrado por todas aquellas etapas que van desde que se plantea la idea de desarrollar el sistema y comienza su diseño, hasta que éste se retira del mercado. Las dos grandes fases que integran este ciclo de vida son: la fase de desarrollo, cuyo objetivo principal es diseñar y elaborar el sistema de IA y, la fase de despliegue, la cual tiene como finalidad la puesta en marcha del sistema en el entorno donde éste desplegará sus efectos.

**¿Cuáles son los principios que han de orientar el ordenamiento jurídico de Protección de DDPP conforme a la reciente recomendación de la Unesco sobre la Ética de la IA, los DDHH y los ODS?**

La recomendación de la Unesco sobre Ética de la IA supone un paso muy importante en la apuesta por el desarrollo ético de sistemas de IA, no sólo porque es el primer texto –no vinculante- que establece una serie de principios éticos aplicables a la IA a nivel internacional sino también por su contenido, el cual marca unas pautas adecuadas para el desarrollo y uso de los sistemas de IA. Por lo que se refiere al principio de privacidad, podemos destacar algunas de las propuestas específicas que desarrollan este principio. Así, es de alabar el apartado 34 de la recomendación que expresamente establece la necesidad de que se incorpore desde la fase de concepción de los sistemas de IA el elemento de privacidad, es decir, un reflejo del principio de privacidad desde el diseño reconocido en el artículo 25 del RGPD. Se destaca también la necesidad de implementar evaluaciones de impacto ético en las que se tenga en cuenta específicamente la privacidad y las consecuencias socioeconómicas derivadas de los tratamientos de datos presentes durante el ciclo de vida de los sistemas de IA. En la Universidad de Valencia hemos hecho toda una serie de videos y píldoras educativas sobre cada uno de los principios éticos que se reconocen en esta norma, entre los cuales se encuentra el de privacidad.

*El ciclo de vida de los sistemas de IA está integrado por todas aquellas etapas que van desde que se plantea la idea de desarrollar el sistema y comienza su diseño, hasta que éste se retira del mercado*

**Has considerado como "normativa neutral" la actual regulación de Protección de Datos en materia de IA. ¿Qué se entiende como normativa neutral?**

El RGPD adopta un enfoque neutral a la hora de regular las tecnologías que tratan datos personales. Esto es lógico. Me explico, el RGPD tiene como objetivo establecer un marco adecuado de protección del tratamiento de los datos personales. Es decir, esta norma no está diseñada para regular un ámbito específico de una determinada tecnología que pueda tratar datos personales sino que, cuando esa determinada tecnología lleve a cabo tratamientos de datos personales, esta norma resultará plenamente aplicable. Esa misma idea tenemos que trasladarla al ciclo de vida de los sistemas de IA cuando traten datos personales. El derecho a la protección de datos irremediablemente quedará afectado por el desarrollo de los avances tecnológicos, sin embargo, el hecho de que se utilice una tecnología u otra no puede ser el elemento esencial para establecer por ejemplo la aplicación o no de la normativa. Dicho lo anterior, es cierto que el RGPD hace mención a varios tratamientos de datos que están estrechamente relacionados con algunas de las fases presentes durante el ciclo de vida de los sistemas de IA, me estoy refiriendo a las decisiones plenamente automatizadas que generan efectos relevantes (Artículo 22) y la elaboración de perfiles (Artículo 4.4).

**¿Debería la normativa de Protección de Datos aplicada a los sistemas de IA contar con un enfoque diferencial con respecto al resto de sistemas?**

No, creo que el RGPD apuesta por un enfoque muy interesante para dicho trato diferencial. Me estoy refiriendo al enfoque del riesgo, »

*La automatización de los procesos decisorios en las organizaciones es un fenómeno que está eclosionando en los últimos años. Tanto el sector público como el privado son conscientes de las ventajas que implica e implicará el uso de la IA para estos*

» este enfoque obliga a las organizaciones a valorar el riesgo presente en los tratamientos de datos que llevan a cabo y, en función del ese riesgo, prever unas u otras medidas y garantías para mitigarlo. Es cierto que en muchos casos, el uso de un sistema de IA presentará un riesgo mayor que otro sistema algorítmico que no sea de IA, sin embargo, en otros supuestos puede ser diferente. Piénsese por ejemplo en el uso de un sistema algorítmico relativamente sencillo y no basado en técnicas de inteligencia artificial que se utiliza para denegar una subvención y un sistema de IA que tiene como objetivo recomendar una película. Los riesgos potenciales que se pueden derivar del tratamiento de datos del primer sistema pueden ser en muchos casos mayores que los del segundo, a pesar de que la IA no esté presente en el primero. Lo que quiero decir, y ya de camino vuelvo a hilar con la pregunta anterior, es que la tecnología que se utilice no siempre será el elemento esencial diferenciador sobre el cual pivote el establecimiento de más o menos exigencias, las organizaciones deben valorar si ese concreto algoritmo, sea o no de inteligencia artificial, puede generar más o menos riesgos para los particulares afectados por esos sistemas.

**¿Hasta qué punto es importante poner especial atención en la fase de diseño de los sistemas de IA para garantizar la privacidad, teniendo en cuenta que la aplicación de la tecnología Machine Learning hace evolucionar a la propia IA?**

El principio de privacidad desde el diseño resulta esencial en este contexto (Artículo 25). Tenemos que tener en cuenta que durante la fase de despliegue la normativa de protección de datos entrará en juego en la mayoría de las ocasiones donde las decisiones adoptadas por un sistema de IA afecten a particulares. Si esas exigencias normativas no se han previsto o programado durante la fase de desarrollo de los sistemas algorítmicos, posiblemente estos sistemas presentarán defectos de cumplimiento normativo en materia de protección de datos cuando se incorporen al entorno donde éste irradiará sus efectos. Y ello, independientemente de si en la fase de diseño se trataron o no datos personales. Por ejemplo, los sistemas de IA se deben desarrollar teniendo en cuenta que los titulares de los datos personales sobre los que se adoptarán decisiones podrán en su caso ejercer los derechos que la normativa de protección de datos reconoce en su favor. Entre otros, derecho de acceso, rectificación, supresión, supervisión humana, impugnación de la decisión, etc. Esta misma idea es trasladable a los sistemas evolutivos de machine learning, es decir, corresponde a los desarrolladores implementar herramientas que aseguren que, a pesar de que el sistema pueda evolucionar, la normativa de protección de datos se siga cumpliendo, por ejemplo demostrando que el sistema mantiene los niveles de precisión adecuados cuando se ingresan datos similares a los que se utilizaron para la construcción del sistema.

**¿Sería necesario desarrollar una ISO específica en Protección de Datos aplicada a los sistemas de IA? ¿Por qué?**

Algunas características presentes durante el ciclo de vida de los sistemas de IA aportan un factor de complejidad relevante a los tratamientos de datos personales. Las normas ISO pueden ser una buena herramienta para estandarizar y mitigar en parte algunos de los riesgos presentes en este ecosistema tal y como ocurre por ejemplo con la norma ISO de seguridad de la información. En este sentido, la propuesta de Reglamento de Inteligencia artificial contempla la necesidad de que los desarrolladores de sistemas de IA deban pasar un proceso de evaluación de conformidad de sus productos de IA, entre las opciones para pasar dicha conformidad destaca el uso de normas armonizadas elaboradas por organismos de normalización o certificación. Muy posiblemente, estas normas podrán ser utilizadas en parte por las organizaciones para demostrar el cumplimiento de la normativa de protección de datos. Por ejemplo, la propuesta de Reglamento de IA establece que los desarrolladores han de

diseñar sistemas de IA lo suficiente transparente para que las organizaciones que posteriormente los utilicen puedan comprender su funcionamiento. Esta información que se les facilitará a las organizaciones usuarias de los sistemas de IA será útil para cumplir con algunas de las obligaciones de transparencia que se derivan de la normativa de protección de datos personales.

**Has señalado que lo datos inferidos o inferencias generadas por los sistemas de IA son datos personales. ¿Qué consecuencias jurídicas se derivan de esta afirmación desde el punto de vista de la normativa de protección de datos?**

Los datos inferidos o inferencias son aquella información que infiere un algoritmo una vez que ha procesado los datos de una persona física. Esta información puede o no ser cierta, sin embargo, la organización la utiliza para generar sobre el particular una serie de consecuencias. Por ejemplo, un algoritmo puede inferir que las personas que escuchan un determinado tipo de música a unas determinadas horas del día son personas que están deprimidas y, en función de esa información, la organización envía publicidad de antidepresivos. Es decir, el sistema infiere que la persona está deprimida y una vez inferida esa información, se adopta un proceso que afecta al particular. Por tanto, desde el momento que esa información queda vinculada a esa persona y sobre la cual se generan ciertas consecuencias, el concepto de dato personal entra en juego. Ello supone entre otras cosas que los datos inferidos, al ser considerados datos personales, también les resultará aplicable el conjunto de derechos previsto por esta normativa, entre otros, derechos de acceso, rectificación, etc. Ahora bien, dado que esos datos personales inferidos han sido creados por un algoritmo, es posible que en determinadas ocasiones algunos de estos derechos puedan quedar en parte limitados por otros intereses jurídicos.

**Para terminar y pensando en nuestro público objetivo compuesto principalmente por profesionales jurídicos y DPD. ¿Por qué deberían interesarse por el cumplimiento de la normativa de Protección de Datos en los sistemas y proyectos de IA?**

La automatización de los procesos decisorios en las organizaciones es un fenómeno que está eclosionando en los últimos años. Tanto el sector público como el privado son conscientes de las ventajas que implica e implicará el uso de la IA para estos. Esta automatización no ha sido del todo posible porque hasta ahora no se han dado las condiciones ideales para que este tipo de máquinas puedan incorporarse a dichos procesos decisorios con un nivel de precisión lo suficiente tolerable. Dado que estos sistemas dependen de datos personales durante el ciclo de vida de los sistemas de IA, los profesionales de la privacidad tienen y tendrán un papel sumamente relevante en dichas fases, ya que deberán aportar el factor legal al proceso técnico presente en dicho ciclo de vida.

## Sobre Adrián Palma Ortigosa

Profesor Ayudante Doctor del Departamento de Derecho Administrativo de la Universidad de Valencia y miembro del área de privacidad de OdiseIA. Imparte docencia en el Grado de derecho y Ciencia de datos de la Universidad de Valencia. Recibió el Premio al mejor expediente de su promoción concedido por la Real Academia de Jurisprudencia y Legislación de Granada. Recientemente ha publicado su monografía titulada “Decisiones automatizadas y protección de datos: especial atención a los sistemas de inteligencia artificial”. Actualmente colabora en varios proyectos relacionados con las implicaciones legales del uso de sistemas de inteligencia artificial en diferentes entidades públicas y privadas.

**www.linkedin.com/in/adrián-palma-ortigosa-261136230**

## Telefónica Tech

# Telefónica Tech y Qualys suscriben una alianza para el mercadoibérico

**Telefónica Tech,** y **Qualys, Inc** .(NASDAQ: **QLYS** ), proveedor de soluciones de cumplimiento yseguridad basadas en la nube, han suscrito un acuerdo en el ámbito de la ciberseguridad, en virtuddel cual la plataforma nativa **Qualys Cloud Platform** y sus aplicaciones de nube integradas seincorporan al portfolio de servicios de seguridad gestionada de Telefónica Tech para España yPortugal.

Esta alianza proporciona una tecnología puntera para el equipo de profesionales de seguridad alofrecer visibilidad de 360 grados en instalaciones locales, puestos de trabajo, entornos de nube, contenedores o entornos móviles y permitir, desde una única plataforma cloud, evaluar la inteligenciade seguridad crítica, así como automatizar todo el espectro de auditoría, cumplimiento y protecciónde los sistemas de TI y aplicaciones web.

Alberto Sempere, director de Producto de Ciberseguridad en Telefónica Tech, afirma: “Este acuerdocon Qualys nos permitirá complementar y potenciar nuestro posicionamiento en el ámbito de laciberseguridad de la mano de una tecnología innovadora que permite un enfoque único e integrado,proporcionando un ciclo de protección continuo. De este modo, los centros de operaciones (SOC) deTelefónica Tech podrán hacer frente a la gran complejidad de los entornos híbridos y redes múltiplesde nuestros clientes con una postura de seguridad más ágil, completa y eficaz gracias a la tecnologíade Qualys”.

Por su parte, Sergio Pedroche, country manager de Qualys para España y Portugal, subraya: “Estamosmuy satisfechos de ser un partner de confianza de Telefónica Tech y poder llevar así nuestratecnología a todos sus clientes del mercado ibérico. Esta alianza en España y Portugal es sólo unprimer paso y esperamos poder concretar nuevos acuerdos para que esto sea extensible en lospróximos meses para los cientos de miles de clientes que tienen en Latinoamérica, Estados Unidos yel resto de Europa”. La plataforma de Qualys integra varias soluciones de seguridad críticas en unasola plataforma proporcionando un inventario completo y en tiempo real de todos los activos de TI yofreciendo un ciclo de protección continuo desde un único panel de control. Con flujos de trabajo deorquestación integrados y detección de vulnerabilidades en tiempo real, esta plataforma permitepriorizar, remediar y auditar en entornos de TI cloud y on premise logrando una mayor agilidad y unahorro sustancial de costes.

Aenor

# AENOR, primera entidad acreditada para certificar el nuevo ENS

El Gobierno ha publicado el Real Decreto 311/2022 sobre el Esquema Nacional de Seguridad (ENS), que actualiza la política de seguridad en la utilización de medios electrónicos, y es de obligado cumplimiento para las administraciones públicas y sus proveedores.

AENOR se ha convertido en la primera entidad acreditada por ENAC (Entidad Nacional de Acreditación) para certificar la conformidad con el Real Decreto 311/2022 por el que se regula el ENS. Un reconocimiento avalado por la experiencia de esta entidad de evaluación desde el año 2013 respaldando a las organizaciones que cumplen con este Esquema.

El Esquema Nacional de Seguridad se aplica a todo el sector público y a sus proveedores tecnológicos del sector privado, y establece la obligatoriedad de realizar una auditoría de certificación por una entidad acreditada por ENAC. Este esquema de acreditación ha sido desarrollado por ENAC, en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital y el Centro Criptológico Nacional (CCN).

El ENS se publicó por primera vez en 2010, fue modificado en 2015 y recientemente, en mayo de 2022. Se mantiene actualizado de forma permanente en paralelo al avance de los servicios prestados por las entidades del sector público, la evolución tecnológica, la aparición o consolidación de nuevos estándares internacionales sobre seguridad y auditoría y los riesgos a los que estén expuestos los sistemas de información concernidos. Esta Ley especifica que los sistemas de información de los servicios electrónicos de las Administraciones Públicas deberán estar adecuados al ENS antes de mayo 2024.

La acreditación que acaba de recibir AENOR supone un nuevo respaldo al rigor que viene desarrollando la entidad, que fue en 2017 la primera certificadora en acreditarse para certificar el Esquema Nacional de Seguridad.

La acreditación es el reconocimiento formal de la independencia y capacidad técnica de una entidad de evaluación de la conformidad para desarrollar actividades de certificación. AENOR cuenta con 198 acreditaciones y autorizaciones tanto españolas como de otros países; para ello supera cada año unas 150 jornadas de auditoría realizadas por entidades de acreditación y otros organismos.

**AENOR es la primera entidad acreditada para certificar el nuevo Esquema Nacional de Seguridad el cual se aplica a todo el sector público y a sus proveedores tecnológicos**

## Thales

# La tecnología de Thales se incorporará al nuevo bypass en las líneas de alta velocidad entre Sevilla-Málaga-Granada

Thales ha sido elegida como empresa adjudicataria para llevar a cabo la redacción del proyecto constructivo y ejecución de las obras del enlace que conectará la línea de AV Madrid-Sevilla con Córdoba-Málaga. Se encargará de las instalaciones de control de tráfico, señalización, protección de tren y comunicaciones del ramal, de 1.738 metros de longitud, que discurre entre Almodóvar del Río y La Marota, en la provincia de Córdoba.

Cuando finalicen las obras se podrá operar el nuevo bypass de conexión, lo que supondrá un ahorro de tiempo importante en el viaje de Sevilla a Málaga y Granada. Esta modificación significará una mejora notable en la explotación de la línea.

El proyecto incluye la adecuación de los sistemas control de tráfico o enclavamientos de tecnología Thales, sistemas de detección (circuitos de vía) del tramo; el sistema de protección de tren LZB (que se extenderá a lo largo de la nueva vía del bypass) y sistema ERTMS; así como la adaptación de los sistemas de telecomunicaciones fijas y móviles para adecuarlo a las nuevas condiciones de explotación.

Por otro lado, el contrato también contempla el mantenimiento de las nuevas instalaciones del bypass durante un periodo de seis meses.

**De una longitud aproximada de 1,7 km., este nuevo enlace, todo un hito en transporte ferroviario, conseguirá un ahorro de tiempo en el viaje que una Sevilla con Málaga y Granada, en alta velocidad, a millones de pasajeros al año.**

## Brains

# Cómo reducir un 37% los residuos y fomentar la sostenibilidad en las aulas

Según los últimos datos publicados por Eurostat, en el año 2020 la cantidad de residuos municipales generados en la Unión Europea se elevó a 505 kg, lo que equivaldría a 225,7 millones de toneladas residuales. Pese a que estas cifras son preocupantes, España se situaría entre los siete Estados miembros de la Unión que generarían menos residuos.

Una problemática que ha llevado a las autoridades europeas a proclamar esta penúltima semana de noviembre como la Semana Europea de la Reducción de Residuos, con el objetivo de promulgar acciones de concienciación sobre la gestión sostenible de recursos y residuos. En este sentido, la Unión y sus Estados miembro se han marcado dos metas principales de cara a los próximos años: superar el 55% el reciclaje de residuos domésticos para 2025 y reducir al 10% o menos la disposición de residuos municipales en vertederos para 2035.

## El valor de reducir, reciclar y reutilizar

Una situación que no solo se ha de empezar a regular con políticas de prevención desde las autoridades públicas, sino que se debe cambiar desde la base, comenzando por la educación. Por ello, desde el grupo educativo Brains International Schools, lleva tiempo impulsando su programa "Brains en verde", que busca inculcar valores, hábitos y actitudes ambientales en los alumnos desde edades muy tempranas.

"Brains en verde" también tiene muy presente la "regla de las tres erres" (reducir, reciclar y reutilizar), en beneficio del medioambiente y la preservación para una buena salud pública. Con este concepto quieren reducir la huella medioambiental, sustituyendo materiales como el plástico o el papel por aquellos a los que se puede dar más de un uso.

"Mediante talleres, buscamos enseñar al alumnado a reutilizar los residuos, promover información sobre tasas de reciclaje y que ellos mismos se esfuercen en hacer cada día más visible este problema. Según los últimos datos, hemos conseguido reducir la producción de residuos orgánicos de 35.000 kg a 22.000 kg (un 37% menos) y los residuos orgánicos generados han disminuido en pro a una mejora en la separación del papel y el plástico" señala Cristina Escolar, coordinadora de Brains en Verde.

## Passivhaus Plus y el Proyecto Save The Water, hacia un modelo sostenible en las aulas

Sin embargo, la apuesta de los centros Brains en materia de sostenibilidad no se reduce exclusivamente al reciclaje. El centro María Lombillo cuenta con la certificación de arquitectura e instalaciones Passivhaus Plus, lo que le convierte en el primer colegio de la Comunidad de Madrid con estas características. Se trata de una edificación que permite ayudar a complementar el ahorro energético con energía solar suministrada de forma limpia y renovable.

**El grupo educativo Brains International Schools ha impulsado su programa "Brains en verde", que busca inculcar valores, hábitos y actitudes ambientales en los alumnos desde edades muy tempranas**

Esta modalidad de Passivhaus es referente a una nueva construcción y, entre sus características, destaca la renovación de aire con intercambio de calor y el uso de filtros especiales antibacterianos y antiácaros para crear un ambiente aséptico, que fomente el nivel de atención y rendimiento escolar.

"Este tipo de edificación con certificación Passivhaus, pionera en Europa, va muy acorde con los objetivos del centro, que quiere crear cambios y generar hábitos positivos entre el alumnado en base a un crecimiento y desarrollo sostenible", señala Miguel Ángel Ruiz, Facility Manager de Brains International Schools.

Asimismo, los centros Brains International Schools llevan a cabo proyectos que van más allá de la eficiencia energética. La importancia del agua ha llevado a Brains a implementar en el año 2019 el Proyecto SavetheWater, orientado a gestionar y cuidar el consumo responsable del agua en sus instalaciones. El proyecto, está marcado por una hoja de ruta cuyas acciones principales se basan en la aplicación de ingeniería de los procesos termodinámicos para la recuperación de agua y su posterior utilización en las instalaciones. Gracias al Proyecto SaveTheWater, Brains ha conseguido recuperar la cantidad de 300.000 litros.

"El proyecto SaveTheWater es un proyecto estrella, muy ligado con el cambio climático y al cumplimiento de los objetivos de Desarrollo Sostenible (ODS). La intención no es solo el ahorro del agua, si no inculcar valor cuidando de este recurso entre nuestros alumnos y poder hacer de ella un bien reutilizable para otro tipo de acciones", puntualiza Miguel Ángel Ruiz.

Medallia

# Kantar Insights y Medallia refuerzan su colaboración a nivel europeo

Kantar y Medallia unen sus fuerzas para que las empresas puedan ofrecer las mejores experiencias en tiempo real. Esta alianza ayuda a las organizaciones a aprovechar la voz del cliente en beneficio de la empresa, y a obtener los mejores datos gracias a la tecnología de gestión de la experiencia.

Conjuntamente, Kantar Insights y Medallia ayudan a las empresas a integrar mejor las opiniones de los clientes en los procesos y ofrecer una experiencia única del journey en relación a una determinada marca.

Entre algunos de los datos de esta colaboración, destacan:

- 8 años trabajando juntos
- Más de 40 programas implementados con éxito
- 50.000 horas de experiencia
- 80 personas de Kantar Insights formadas en la tecnología de Medallia
- Presentes en 8 países
- Una única compra con soporte técnico
- Dos socios que confían plenamente el uno en el otro

Ambas empresas han desarrollado un marco de actuación, con el objetivo de construir una cultura del cliente en la organización. Esta colaboración tiene un claro propósito: **ayudar a las empresas a ser admiradas por sus clientes.**

Medallia desarrolla una tecnología que permite a las organizaciones entender y gestionar la experiencia de sus clientes en tiempo real, mientras que Kantar Insights se asegura de que las organizaciones puedan establecer una experiencia que esté en línea con su compromiso de marca.

Cloe Tejtelbaum Tardy, Directora de Satisfacción del Cliente de Renault Trucks, dijo: *"Como usted sabe, las personas, la tecnología (en tiempo real/IA) y el proceso son los mejores ingredientes para una gestión exitosa de la experiencia de cliente. Un equipo para el que la experiencia y la satisfacción del cliente no son algo opcional. Su pasión es la clave. La satisfacción del cliente es nuestra prioridad".*

## Como consecuencia de la unión, cada empresa aporta unos valores únicos:

Kantar Insights asegura que **las marcas son los principales activos de las empresas,** conoce los datos y técnicas para crear una marca fuerte y admirada. Mediante Kantar BrandZ, el estudio de valoración de marcas a nivel mundial, se demuestra que l**a experiencia de cliente** es uno de los cuatro pilares fundamentales y **representa el 70% del valor de la marca**. De hecho, la experiencia directa del producto confirma o desmiente las expectativas que las personas tienen sobre una marca y confirma si es significativa o no. Las marcas tienen que ofrecer una experiencia positiva y significativa, si quieren fidelizar a los compradores para que recomienden su producto. Kantar Insights integra esta filosofía en su encuesta de satisfacción, asegurándose de que lo que dice la marca es experimentado por el cliente.

## Ingeniería: conectar la plataforma Medallia

Los equipos de Kantar Insights están especializados en implementar y conectar estas plataformas al ecosistema de datos de las empresas, aportando aplicaciones relevantes, en el momento adecuado. Además proporcionan un amplio abanico de soluciones que cubren las necesidades de la empresa, para obtener el valor óptimo del programa actual y hacer avanzar la hoja de ruta del cliente hacia adelante.

Las soluciones integrales de transformación de CX de Kantar Insights combinan una sólida especialización en experiencia de cliente y marca, con amplias funciones de consultoría, investigación y análisis avanzado.

Además, la empresa aporta el asesoramiento necesario para la implementación del programa, para el desarrollo del negocio y para la toma de decisiones, así como para el fortalecimiento de la cultura del cliente en la organización.

*"Los asesores de Kantar CX tienen un conocimiento profundo de las expectativas de las marcas y sus limitaciones, para poder ayudarles a diseñar la herramienta adecuada. Cada programa es único",* explica Karen Tartour, Directora de Experiencia del Cliente para Europa Central y del Sur.

Por parte de Medallia, su plataforma líder de gestión de experiencias, Medallia Experience Cloud, utilizada por empresas de todo el mundo, ofrece las mejores experiencias a clientes y empleados en todos los puntos de contacto. Se trata de una plataforma perfecta para la empresa, pues va más allá de las encuestas tradicionales para comprender las necesidades de los clientes y puede descubrir aspectos clave de cada interacción, cerrando el *"close the loop"* con datos en tiempo real.

Con más canales de escucha que el resto, la plataforma de Medallia captura el feedback para conseguir una visión completa de cada cliente y empleado. Analiza las encuestas, las conversaciones, los comportamientos digitales, las redes sociales,… y mucho más, para proporcionar la información necesaria a la hora de realizar cambios. Los empleados pueden ver el resultado completo y actuar en tiempo real, transformando la organización hacia una cultura centrada en el cliente.

La plataforma de Medallia Experience Cloud permite diferenciar las experiencias y mejorar los beneficios. El retorno de la inversión debe comenzar desde el primer día, pues algunas de las soluciones de Medallia, que aprovechan herramientas como la base de datos CRM, están diseñadas a medida tanto para un solo departamento, como para grandes compañías.

## Nippon Gases

# Nippon Gases: "Making life better through gas technology"


Nippon Gases, parte de Nippon Sanso Holdings Corporation, es el socio estratégico en materia de gases industriales y medicinales. Ofrecemos nuestras propias soluciones tecnológicas a una amplia gama de sectores como la acuicultura, la automoción, la industria química, la alimentaria y de bebidas, el vidrio, la industria hospitalaria y la de terapias respiratorias domiciliarias, la producción de metales y la metalurgia, la industria petroquímica, la farmacéutica, el acero, el tratamiento de aguas y aguas residuales, la de soldadura y corte entre otros. Nuestra oferta tecnológica abarca tanto las opciones de suministro más eficientes como aplicaciones a medida para cada cliente o partner. Mejoramos constante y proactivamente la seguridad –la prioridad número uno de nuestra empresa- en nuestras operaciones y en las instalaciones de los clientes, gracias a la búsqueda de factores de riesgo y comportamientos y a la estricta observación de nuestros principios de seguridad por parte de todos nuestros empleados. La excelencia en Compliance se consigue a través de la formación continua y con la aplicación de nuestro Código de Conducta por parte de cada empleado.

Nippon Sanso Holdings Corporation tiene más de 100 años de experiencia y cuenta con una importante presencia en Japón, el sudeste asiático, Australia, Estados Unidos y Canadá, operando en 32 países con más de 19.000 empleados en todo el mundo.

Nuestra presencia en Europa nos posiciona como una empresa líder con más de 3.000 empleados de los cuales el 27% son mujeres, que operan actualmente en 13 países y presta servicio a más de 150.000 clientes. La seguridad, prioridad número uno en nuestra compañía, mejora constantemente gracias a la búsqueda de factores y comportamientos de riesgo y a la observancia de nuestros principios de seguridad por parte de todos nuestros empleados. El compromiso de Nippon Gases con nuestros clientes, empleados y asociados y con las comunidades en las que operamos es un reflejo de nuestra dedicación al medio ambiente y a la sostenibilidad. Juntos, somos "The Gas Professionals" y todos tenemos el mismo objetivo: "Making life better through gas technology"

Trigo

# ¡TRIGO es ahora Proveedor Preferente de Robert BOSCH!

La Alta Dirección de Bosch en el ámbito global del Servicio de Inspección de Calidad ha promovido a TRIGO como “Proveedor Preferido”. Este es el resultado de la asociación a largo plazo a nivel nacional entre BOSCH y las entidades TRIGO, que ahora se va ampliando a un nivel de asociación más estratégico bajo el estatus de “Proveedor Preferido”.

### ¿Qué es el premio BOSCH al proveedor preferente?

El estatus de “Proveedor Preferido” es el premio más honorífico en el área de competencia en Inspecciones de Calidad. TRIGO ha tenido que cumplir con los criterios profesionales y de alta exigencia de los procesos de BOSCH para ser calificado por la Alta Dirección local y mundial para conseguir este premio prestigioso.

Este premio es un gran logro para TRIGO y demuestra el valor de la excelencia operativa en las instalaciones de TRIGO en todo el mundo.

Este reconocimiento permitirá a TRIGO fortalecer y aprovechar aún más la asociación con Bosch hacia servicios avanzados de TRIGO como Ingeniería Residente, Formación, Consultoría y Auditoría.

### ¿Qué criterios han permitido a trigo recibir este premio?

El premio es el resultado de un complejo método de puntuación y evaluación, al que responden los siguientes factores de éxito de TRIGO. La satisfacción del cliente local y global se alcanza gracias a unos empleados motivados y animados, así como a un espíritu de equipo comprometido en la prestación diaria de servicios de TRIGO. La excelencia operativa es el resultado de procesos y métodos bien diseñados.

Según Hans Gerd Düsterwald, Vicepresidente Ejecutivo para Europa Continental, “la estabilidad financiera del GRUPO TRIGO y su huella internacional son también elementos clave para el premio, debido a que TRIGO proporciona una calidad de servicio de forma continua en sus diversas fábricas en el mundo entero y ha sido identificado como un socio estable”.

Además, la capacidad de respuesta de TRIGO, es decir, su capacidad para reaccionar a tiempo ante una solicitud central o local, también fue un factor clave para ganar el premio.

Por último, Hans Gerd se mostró orgulloso: “Nos sentimos honrados por la confianza que BOSCH ha depositado en nuestra empresa, ¡y estamos deseando ver cómo evoluciona nuestra colaboración en los próximos meses y años!”.

**Este reconocimiento permitirá a TRIGO fortalecer y aprovechar aún más la asociación con  hacia servicios avanzados de TRIGO como Ingeniería Residente, Formación, Consultoría y Auditoría.**

Johnson & Johnson

MEDTECH

# Más de 130 años de Innovación en el cuidado de la salud

**Damos vida a ideas, productos y servicios para promover la salud y el bienestar de las personas.**

# Javier García

## Director General de UNE y Vicepresidente de ISO

Javier García, director general de la Asociación Española de Normalización, UNE, se ha convertido en el primer español en ser elegido vicepresidente de la Organización Internacional de Normalización (ISO), posición que ejercerá entre 2023 y 2024. García ha desempeñado numerosas responsabilidades en los organismos internacionales y europeos de normalización, en beneficio de los sectores económicos españoles. Actualmente, es miembro del Consejo de Administración del Comité Europeo de Normalización (CEN). Además, ha sido vicepresidente Técnico del Comité Europeo de Normalización Electrotécnica (CENELEC). También ha formado parte del Consejo de Administración de ISO y del Consejo Técnico de Normalización de la Comisión Electrotécnica Internacional (IEC). García trabaja desde hace 25 años en el organismo de normalización español, en el que ha desempeñado diversos cargos de responsabilidad.

**Karen Von Burucker**

Directora de Comunicación y RRII.
**Asociación Española para la Calidad, AEC**

kvonburucker@aec.es
www.linkedin.com/in/karenvonburucker

**¿Qué supone este nombramiento como vicepresidente de ISO para usted y para los sectores económicos españoles?**

Lo primero que supone es un inmenso honor, además de una gran responsabilidad. Que los miembros de ISO, en el que están presentes 166 países del mundo, me hayan elegido para liderar la vicepresidencia de Gestión Técnica supone una muestra de la reputación y la influencia de la normalización española en el mundo, resultado del gran trabajo que se hace en esta entidad gracias al compromiso y esfuerzo de sus miembros y trabajadores. También quiero agradecer el apoyo del Ministerio de Industria, Comercio y Turismo y del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación.

Este nombramiento representa una gran oportunidad para que nuestro tejido económico y empresarial lidere las normas globales que les ayudarán a superar con éxito sus grandes desafíos. Y los datos nos avalan: el 90% de los comités y subcomités de normalización de ISO cuentan con representación de expertos españoles. Animo a los expertos de organizaciones españolas a participar en los estándares internacionales; estar en ISO supone influir en las decisiones sobre el diseño y prestaciones de futuros productos y servicios, marcar las directrices estratégicas que definen los nuevos mercados internacionales en auge, las mejores prácticas de gestión empresarial, etc.

En esta nueva responsabilidad, tendré el rol de asegurar que las nuevas normas técnicas internacionales se alinean con la Estrategia trazada por ISO para 2030, enfocada a dar respuesta eficaz a los grandes temas que preocupan a la sociedad, como la transición ecológica y energética, la transformación digital o el cumplimiento de los Objetivos de Desarrollo Sostenible (ODS) establecidos por Naciones Unidas para 2030.

**¿Cómo va a influir su incorporación a ISO en el papel de España en el desarrollo de estándares internacionales?**

Mi principal objetivo es concienciar a nivel mundial sobre la importancia de la normalización, cuya misión es contribuir al progreso compartido y a la creación de un mundo más seguro, sostenible y competitivo. Los estándares facilitan el comercio, la competitividad de las empresas y fomentan el desarrollo de buenas prácticas en la gestión empresarial y la seguridad de los productos. Ahora bien, España tiene una gran oportunidad para internacionalizar sus sectores y fortalecer su reputación. Es importante recalcar que las normas aportan aproximadamente el 1% del PIB total español. En el marco de esta responsabilidad, mi intención es incentivar que las organizaciones españolas se involucren aún más activamente en la normalización internacional asumiendo un papel de liderazgo.

*Mi objetivo es concienciar a nivel mundial sobre la importancia de la normalización, cuya misión es contribuir al progreso compartido y a la creación de un mundo más seguro, sostenible y competitivo*

**¿Qué rol juega la normalización española en la esfera internacional en estos momentos?**

Tenemos un papel protagonista y España es un referente internacional en normalización. Cada vez son más las normas UNE que sirven de base para el desarrollo de normas internacionales. En este sentido, me gustaría destacar el activo posicionamiento que tenemos en ámbitos transversales como sostenibilidad, digitalización, ciberseguridad y compliance. Además, lideramos sectores verticales como seguridad industrial, energías renovables y turismo.

Además, los expertos españoles desempeñan cada vez más responsabilidades internacionales y europeas, sumando actualmente 144

Estos hechos y cifras demuestran que la normalización contribuye a la Marca España.

**La reciente COP27 de Egipto ha vuelto a destacar cómo estamos cada vez más cerca del punto de no retorno ante el reto climático. ¿Cómo contribuyen los estándares?**

La reciente Cumbre del Clima (COP27) nos ha vuelto a recordar algo muy importante pero que, por desgracia, olvidamos frecuentemente: sin colaboración ni unión nunca ganaremos la lucha por el cambio climático. Es el momento de pasar a la acción juntos, tendiendo puentes y estableciendo alianzas. En este sentido, los estándares son una clave con la que las organizaciones puedan pasar del compromiso a la acción y lograr no solo sus objetivos medioambientales sino un impacto que sea medible. Las normas recogen el consenso, colaboración y las mejores prácticas para que las organizaciones puedan afrontar este desafío global.

En la COP 27, tanto desde ISO como desde UNE presentamos el nuevo estándar internacional 'Directrices para el cero neto', que nace con la ambición de establecer un marco de entendimiento común que permita alcanzar a las organizaciones el objetivo de cero emisiones. Su presentación en esta Cumbre pone de relevancia la visión de alto impacto con la que se ha desarrollado el documento, así como el firme compromiso de ISO y de sus miembros para elaborar estándares que inspiren acciones eficaces en el reto ambiental. »

*UNE y la AEC son dos importantes actores en el impulso de la calidad en España, con un relevante papel en el salto hacia el progreso que ha experimentado nuestro tejido económico en las últimas décadas*

» Además, ha contado con la coordinación de UNE para su traducción al español, permitiendo así ampliar su difusión e impulsar una aplicación homogénea. Este documento es de libre acceso de forma totalmente excepcional y en el marco de la esponsorización acordada por ISO. Está disponible en la web de UNE.

**En Europa vivimos tiempos de incertidumbre económica, en los que es fundamental fortalecer la recuperación y resiliencia de las organizaciones. ¿Qué papel tiene la nueva Estrategia Europea de Normalización?**
Sin duda, no sólo en Europa, sino también a nivel global. Nos enfrentamos a una compleja situación geopolítica y a una crisis energética que han provocado un contexto de incertidumbre económica.

Superar con éxito los múltiples desafíos a los que se enfrenta Europa en la actualidad dependerá, en gran medida, de su capacidad para reforzar su autonomía estratégica, mejorar su competitividad industrial e impulsar su liderazgo a nivel global.

Precisamente para lograr estos objetivos, la Comisión Europea ha lanzado en 2022 la nueva Estrategia Europea de Normalización, que refuerza el papel clave de las normas técnicas para lograr un mercado único europeo resiliente, ecológico y digital, que permita tanto a las empresas como a la sociedad en su conjunto pisar el acelerador de la recuperación.

En esta senda hacia el crecimiento, la normalización europea debe ser una de las protagonistas, pues contribuye a mejorar, por un lado, la competitividad y autonomía de la industria, brinda también seguridad a los consumidores y al tejido productivo y es la base para consolidar un mercado interior fuerte en la UE; y, por otro, porque permite dinamizarlo para expandir su posición de liderazgo en el mundo.

También importante es la apuesta de la normalización por proporcionar herramientas de gestión y conocimiento a las empresas para fortalecer su actividad, resiliencia y recuperación, así como aportar soluciones para ayudar a la sociedad española a hacer frente a sus retos a través de la normalización. Por ello, hemos impulsado el Comité UNE de gestión de riesgos, seguridad y resiliencia.

**Hablando de Estrategia, UNE ha lanzado la suya con la mirada puesta en el año 2025. ¿Qué objetivos se ha marcado?**
La Estrategia 2025 de UNE nace con el objetivo de ayudar a la sociedad a superar sus grandes desafíos, a través de las actividades de normalización y cooperación internacional.

Esta Estrategia tiene tres grandes objetivos: aportar soluciones a los retos a los que se enfrenta la sociedad, llevar a cabo la transformación digital de la entidad y ser reconocida como una organización ejemplar en la sociedad y el tejido económico español.

Esta Estrategia 2025 es coherente y está alineada con las correspondientes estrategias 2030 de los organismos de normalización europeos (CEN y CENELEC) e internacionales (ISO e IEC). Además, contempla la contribución de UNE y las normas técnicas al cumplimiento de la Agenda 2030 de las Naciones Unidas y de los Objetivos de Desarrollo Sostenible (ODS).

**UNE acaba de presentar su nueva marca y propuesta de valor. ¿Qué pretenden en esta nueva etapa?**
Estamos muy felices de presentar la nueva marca UNE, con la que pretendemos acercarnos a la sociedad y llegar a más públicos, con un lenguaje sencillo y cercano. En esta evolución, la entidad ha definido su propósito, que refleja su esencia, y ha desarrollado una nueva identidad visual más actual, relevante y global.

Con la nueva propuesta de valor “UNE. Progreso Compartido”, buscamos aunar esfuerzos colectivos para ayudar a la sociedad a superar sus grandes retos a través de las normas, ante un entorno en plena transformación económica, social y ambiental. Esta evolución de la marca UNE se ha materializado en una nueva identidad inspirada en el espacio de diálogo y colaboración que facilita la normalización y en su papel global.

El desarrollo de la nueva identidad de UNE se enmarca en su Estrategia 2025, con la que pretendemos ensalzar los valores diferenciales de la normalización, así como la flexibilidad y agilidad de UNE para aportar soluciones a los desafíos a los que se enfrentan las organizaciones y la sociedad españolas. Además, busca descubrir a los sectores empresariales un organismo de normalización evolucionado, que les ayuda a elaborar las normas que necesitan para afrontar la doble transición ecológica y digital.

El cambio de logotipo es un elemento fundamental y en su evolución se ponen en el centro los valores diferenciales de UNE: transparencia, diálogo y consenso, reflejados en el globo que da forma a la letra U.

En este cambio hemos definido nuestro propósito: UNE es una organización global de beneficio para la comunidad cuya misión es crear normas que contribuyen a la construcción de un mundo más seguro, sostenible y competitivo.

Para ello, facilita espacios de colaboración neutrales e inspiradores en los que compartir conocimiento para desarrollar, a través del diálogo y el consenso, normas que sirvan a los intereses de toda la sociedad y que movilicen a los que apuestan decididamente por la excelencia empresarial y la conciencia social.

**UNE y AEC son dos actores relevantes en el ámbito de la calidad en España. ¿En qué se basa esa relación?**

UNE y la AEC son dos importantes actores en el impulso de la calidad en España, con un relevante papel en el salto hacia el progreso que ha experimentado nuestro tejido económico en las últimas décadas.

Ambas entidades vienen colaborando desde hace muchos años. La AEC es miembro corporativo de UNE desde su creación en el año 1986, participa en su Junta Directiva y lidera la elaboración de normas clave para sus asociados. Al mismo tiempo, UNE forma parte de la Junta Directiva de la AEC. Juntos hemos crecido y cambiado y no se entiende la historia de uno sin el otro, como tampoco se puede entender la historia más moderna de este país sin ambas asociaciones.

Me gustaría destacar el compromiso de la AEC con UNE y con la actividad de normalización. A través de su participación en una decena de Comités Técnicos de Normalización, es una voz respetada en los foros de debate y un referente para seguir liderando la normalización y el compromiso con las buenas prácticas.

*Con "UNE. Progreso Compartido", buscamos aunar esfuerzos colectivos para ayudar a la sociedad a superar sus grandes retos a través de las normas, ante un entorno en plena transformación económica, social y ambiental*

# Nueva Directiva Europea NIS; la ciberseguridad en las empresas da un nuevo paso con la NIS2

FRANCISCO LÁZARO ANGUÍS

Gerente de Ciberseguridad y Privacidad (CISO y DPD)

**Renfe**

Contacta:

linkedin.com/in/flazaro

**La nueva Directiva NIS, la NIS2, viene a incrementar la exigencia en la seguridad de las redes y sistemas de información a los estados miembros de la UE y particularmente a sus operadores esenciales e importantes sobre los que descansan los servicios esenciales.**

**Su influencia se espera que sea mucho mayor que la de su predecesora, no tanto por las medidas de seguridad que impone a los operadores, las cuales para una organización con una madurez básica en ciberseguridad no representan una exigencia mayor que la que ya se autoimponen, sino por su mayor alcance y por la responsabilidad directa que los comités de dirección de los operadores tienen sobre la Ciberseguridad y sus resultados.**

**El mayor alcance como veremos viene tanto por la inclusión de nuevos sectores a los esenciales, como por la extensión a un nuevo colectivo de sectores; los sectores importantes, así como por las exigencias que operadores, estados y UE deben ejercer sobre sus cadenas de suministro.**

Según datos del Parlamento Europeo [1], El 28 de noviembre de 2022, el Consejo de la Unión Europea ha aprobado la NIS2, que sustituirá a la actual directiva NIS sobre seguridad y sistemas de información. Esta Directiva, entrará en vigor a los 21 días de su publicación en el Diario Oficial de la UE (lo que a la hora de escribir el presente artículo aún no se había producido). A partir de su publicación en el DO de la UE, los Estados miembros tendrán 21 meses para incorporar el texto a su legislación nacional.

La publicación en el BOE se espera se produzca a finales de diciembre del 2022 o a primeros de enero del 2023.

El objetivo de esta legislación es la obtención de forma común en toda la Unión, de un alto nivel de ciberseguridad, mejorando la resiliencia y las capacidades de respuesta a incidentes tanto del sector público como del privado y de la UE en su conjunto, a través de sus actores esenciales (operadores esenciales e importantes).

En esta actualización de la hasta ahora vigente NIS, se incorporan una serie de mejoras (en algunos casos concreciones en aras a la armonización de su aplicación entre los diferentes estados miembros) y refuerzos de requerimientos, encaminados a obtener el objetivo antes indicado. Entre las novedades está la exigencia de la involucración de la alta dirección de los actores esenciales en el Gobierno de la Ciberseguridad de sus empresas; de ahí el llamativo titular en la prensa económica española: <<La UE obliga a las empresas a garantizar la ciberseguridad>>.

## ¿Por qué ahora la Ciberseguridad se va a sentar en el comité de dirección?

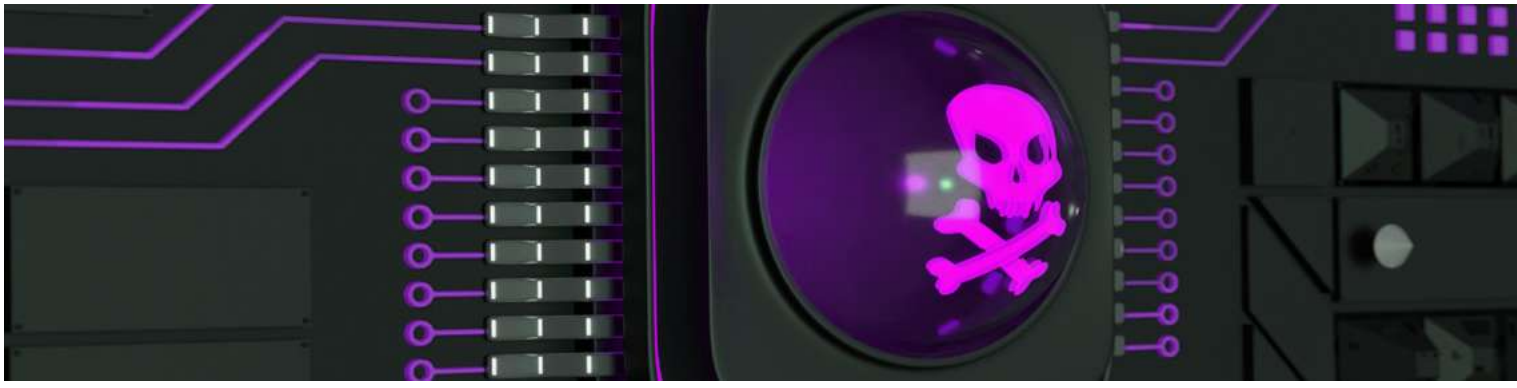
Para responder a esta pregunta, primero debemos mirar a nuestro alrededor y tomar consciencia real de que la tecnología a las empresas les hace ser más eficientes, más eficaces, les facilita crecer y mantenerse, pero también les hace más, mucho más, vulnerables y por tanto, a través de ese conocimiento claro y reflexivo de la realidad, decidir incorporar la Ciberseguridad a sus procesos, como parte inherente a todos ellos.

Los principales factores que facilitan conocimiento son:

- El uso cotidiano, amplio, omnipresente de las Tecnologías de la información y las Comunicaciones (por sus siglas, y en adelante, TIC) en las empresas y sociedad.
- La variedad y complejidad del entorno TIC.
- La mayor dependencia de la cadena de suministro; lo que tecnológicamente genera un nuevo paradigma: “las vulnerabilidades de mi cadena de suministro son mis vulnerabilidades”.
- La exigencia de tiempos de comercialización cortos, con el habitual sacrificio de la seguridad en aras de ese “time to market”.
- En entornos industriales (muy relacionados con Infraestructuras Críticas) la dificultad o la contradicción aun no adecuadamente resuelta, de cómo incoporar a los conceptos tradicionales Safety y Security (el elemento o proceso es seguro si no se mueve de lo certificado) la Ciberseguridad (actualizarse constantemente para ser seguro).
- De todo lo anterior se infiere una probabilidad muy alta de difuminar las responsabilidades para tratar las causas de los ciber-riesgos.
- El efecto llamada que representa para los delincuentes la provisión de servicios tales como RaaS (ransonware como servicio) y modelos de negocio alrededor del delito telemático que “democratizan” el acceso a herramientas y soporte, haciendo posible que un tarugo informático pase, por sus resultados, como un habilidoso hacker.
- Consecuentemente con todo lo anterior, la cada vez mayor materialización de las amenazas sobre las TIC, con el consiguiente impacto para personas, empresas, sociedades y estados.
- Las ciber-amenazas con capacidades “país” como consecuencia de tensiones e intereses geopolíticos; tales como las derivadas de la guerra de Rusia con Ucrania, la cual, si bien se está desarrollando en el plano físico, nos augura un futuro de amenazas hibridas; donde la destrucción de infraestructuras críticas y servicios esenciales podrá darse con especial intensidad a través de ciberataques, combinados con físicos.
- La presencia cada vez más habitual en los medios de comunicación de titulares y noticias de brechas y sanciones.
- Las obligaciones legales derivadas de la regulación europea (RGPD, Infraestructuras Críticas y Servicios esenciales, por citar las más importantes) así como de las iniciativas legislativas nacionales (como en España es el caso del Esquema Nacional de Seguridad), que requieren de capacidades técnicas y materiales que deben ser proporcionadas por las empresas.

**Según datos del Parlamento Europeo [1], El 28 de noviembre de 2022, el Consejo de la Unión Europea ha aprobado la NIS2, que sustituirá a la actual directiva NIS sobre seguridad y sistemas de información**

Del entendimiento que frente a estos riesgos, amenazas e impactos y la vulnerabilidad de nuestro entorno se requiere de un concepto más amplio que el que hasta el presente dábamos a la Seguridad de la Información, se desarrolla la Ciberseguridad. Así, la práctica de la ciberseguridad debe ser entendida no sólo como la protección de la Información y de los sistemas que tratan esa información, sino como la protección y reacción frente a los riesgos que, a través la información, amenazan a las operaciones de las compañías, su continuidad, su crecimiento y lo que para el conjunto de un Estado es más grave: los servicios básicos sobre los que se sustentan la forma de vida de las »



La Directiva NIS establecía la obligación de fijar unos requisitos respecto a la seguridad y notificación de incidentes en los operadores de servicios esenciales (OSE) y proveedores de servicios digitales (PSD), y el mandato de designar a autoridades nacionales competentes en esta materia

» sociedades modernas e incluso a la integridad y vidas de los ciudadanos

En la nota de prensa de la UE de la aprobación de la NIS2, Ivan Bartoš, Viceprimer ministro checo de Digitalización y ministro de Desarrollo Regional expresaba:

«No hay duda de que la ciberseguridad seguirá siendo un desafío clave en los próximos años. Lo que está en juego para nuestras economías y nuestros ciudadanos es enorme. Hoy, dimos otro paso para mejorar nuestra capacidad para contrarrestar esta amenaza».

En mi opinión el horizonte temporal de "los próximos años" se antoja corto; pues, en lenguaje empresarial: la Ciberseguridad no es un proyecto (con un horizonte temporal de finalización) sino una activad, la cual está inexorablemente ligada al uso de las tecnologías de la información y las comunicaciones (más concretamente al riesgo por el uso y/o posesión de dichas tecnologías) y la importancia de esa práctica vendrá dada por la dependencia cada vez mayor de la sociedad con las tecnologías.

Debemos saber que la Ciberseguridad no son solo "cacharros". Los controles de Ciberseguridad, los cuales reducen el riesgo (mediante la disminución de la probabilidad de que se produzca un incidente y/o mediante la disminución de su impacto, en caso de producirse) son de tipo organizativos, procedimentales (de forma más genérica: de desarrollo del marco normativo) y de recursos (humanos y técnicos).

Centrándonos en las empresas podemos resumir todo lo anterior en:

- Para garantizar el mantenimiento de las operaciones y crecimiento de las empresas es imprescindible tener un adecuado nivel de Ciberseguridad.
- La Ciberseguridad debe estar presente en todo proceso y actividad de la empresa en la que se trate información digital; es decir, en casi todos (por no decir en todos) los procesos de Negocio (siendo parte de ellos).
- Existe una probabilidad muy alta de difuminar la responsabilidad y consecuentemente de no ejercer un liderazgo capaz de imponer la acción.
- Los controles de Ciberseguridad son Organizativos, de desarrollo normativo y de recursos humanos y técnicos. Requiere de estrategia, objetivos, presupuesto y prioridades.
- La ciberseguridad, como proceso y actividad crítica debe ser gestionada.
- La cultura de ciberseguridad es básica para alcanzar un adecuado nivel de ciberseguridad en la empresa. La cultura debe ser impulsada por la Alta Dirección.

Con todo este conocimiento y de forma reflexiva deberíamos alcanzar la determinación de que la Estrategia de la Ciberseguridad, su respaldo, impulso y soporte para la consecución de sus objetivos es una cuestión de la Alta Dirección.

La razón del por qué del ahora, lo encontramos bien porque el sentido común nos dice que a la vista de todo lo anterior: "ya estamos tardando" y/o bien porque la legislación, para

determinados actores (que no para todas las empresas) les está señalando que ha llegado el momento.

Muy probablemente cuando pasen los años, cuando la Ciberseguridad haya sido totalmente adoptada en los procesos de negocio, paradójicamente no se requerirá que se personalice en un miembro del comité de dirección la responsabilidad de la Ciberseguridad, pero hoy en día es una buena noticia que desde la UE se establezca esa obligación.

## Antecedentes

La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (conocida como "Directiva NIS"), se aprobada en julio de 2016.

El alcance subjetivo, los sujetos obligados, son las entidades públicas y empresas designadas como operadores esenciales; es decir no todas las empresas sino específicamente aquellas que han sido designadas.

La Directiva NIS establecía la obligación de fijar unos requisitos respecto a la seguridad y notificación de incidentes en los operadores de servicios esenciales (OSE) y proveedores de servicios digitales (PSD), y el mandato de designar a autoridades nacionales competentes en esta materia.

A tal fin la Directiva:

**a)** establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información;

**b)** crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;

**c)** crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, «red de CSIRT», por sus siglas en inglés de «computer security incident response teams») con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;

**d)** establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales;

**e)** establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información

Con cuatro meses de retraso respecto a la fecha máxima en la que se debería haber transpuesto al ordenamiento jurídico nacional, se publicó el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Posteriormente, en enero del 2021 se aprobó el Real Decreto 43/2021 por el que se desarrolla el citado RD 12/2018.

En el RD 12/2018 se establecen las obligaciones del Operador

- Debe designar un responsable de Seguridad de la Información
- Debe establecer y desarrollar medidas de seguridad
- Debe establecer y desarrollar la Gestión y Notificación de incidentes de seguridad, entre otras obligaciones.

En la trasposición se incorporaba (no estaba presente en la Directiva NIS) la obligación de designar por parte del Operador un Responsable de la Seguridad de la Información, a fin de garantizar que las obligaciones de seguridad se llevaran a cabo y verdaderamente se mejorara el nivel de seguridad y resiliencia del operador. Así, el artículo 16 del RD 12/2018, dice:

"Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella" »

**Figura 1.**

Artículo 9. *Autoridades competentes.*

1. Son autoridades competentes en materia de seguridad de las redes y sistemas de información las siguientes:

a) Para los operadores de servicios esenciales:

1.º En el caso de que éstos sean, además, designados como operadores críticos conforme a la Ley 8/2011, de 28 de abril, y su normativa de desarrollo, con independencia del sector estratégico en que se realice tal designación: la Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

2.º En el caso de que no sean operadores críticos: la autoridad sectorial correspondiente por razón de la materia, según se determine reglamentariamente.

b) Para los proveedores de servicios digitales: la Secretaría de Estado para el Avance Digital, del Ministerio de Economía y Empresa.

c) Para los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos se encuentren comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público: el Ministerio de Defensa, a través del Centro Criptológico Nacional.

2. El Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, establecerá los mecanismos necesarios para la coordinación de las actuaciones de las autoridades competentes.

» Es importante destacar que frente a los sectores que la NIS identificaba en su alcance, la transposición española incluyó adicionalmente otros sectores. En España, se igualaron a los sectores ya contemplados en nuestra ley de Infraestructuras Críticas.

La NIS2 prácticamente tiene en su ámbito los sectores que en España que ya están en la transposición por lo que el numero de Operadores Esenciales en España será prácticamente el mismo que en la actualidad (pasando de 420 a una previsión de 450).

Originalmente la NIS contemplaba los Sectores de Energía (Electricidad, Crudo, Gas), Transporte (Aéreo, ferrocarril, Marítimo y Fluvial, Carretera), Banca, Infraestructuras de los mercados financieros, Sector Sanitario, Suministro y distribución de Agua potable e Infraestructura Digital (IXP, DNS,Reg. Nombres) y servicios digitales ( Mercado en línea, Motor de búsqueda en línea y Servicios de computación en nube).

La trasposición española incorporó a los sectores de Administración, Espacio, Industria Nuclear, Industria Química, Instalaciones de Investigación, TIC y Alimentación

Y en la trasposición nacional se identificaban para su ámbito nacional las autoridades de control; artículo 9 del RD 12/2018: *(Figura 1)*

En la práctica en España la principal autoridad competente es la secretaría de estado de seguridad, la cual inicialmente ejercía la competencia a través de su Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), tal y como podemos ver en el artículo 9. En la actualidad es la Oficina de Coordinación de Ciberseguridad (OCC), antes dependiente del CNPIC. El cambio se produjo como consecuencia de una modificación Organizativa en la secretaría (que respondía a la necesidad de dar entidad propia a la Ciberseguridad, independizándose del CNPIC).

## La necesidad de avanzar hacia una nueva NIS.

El 16 de diciembre de 2020, la Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad presentaron en Bruselas, la nueva Estrategia de Ciberseguridad de la UE. Con ella se pretende reforzar la resiliencia colectiva europea contra las ciber amenazas, así como ayudar a los ciudadanos y empresas para que pudieran beneficiarse de unos servicios digitales de confianza.

Con la experiencia de cuatro años de aplicación de la NIS y con una implantación no homogénea de la misma en los distintos países miembros, así como con un incremento de las amenazas en volumen, intensidad y peligrosidad sobre la UE, la Comisión propuso reformar las norma sobre seguridad de las redes y sistemas de información, a través de una Directiva NIS renovada (NIS 2.0) que aumentase el nivel de ciber resiliencia en los sectores críticos, tanto públicos como privados y que revisara los sectores sobre los que era necesario regular a fin de aumentar la resiliencia digital de la UE.

Tal y como ya hemos comentado: la NIS2 incorpora más sectores esenciales que la NIS. Si bien, si comparamos los sectores esenciales de la nueva directiva con los que ya están en el alcance de la trasposición

española de la NIS, observaremos que serán pocos los nuevos sectores que en España se incorporarán; por ejemplo, uno nuevo en el alcance será el sector de aguas residuales.

Pero, si en lugar de los sectores esenciales (único alcance en la NIS), comparamos los dos alcances (el de la NIS2 y el de la transposición española de la NIS) si habrá una importante ampliación del alcance de la NIS2; la que vendrá de la mano de un nuevo conjunto de sectores: los denominados sectores importantes.

## ¿Qué principales novedades nos trae la NIS2?

Las principales novedades son:

- La incorporación de nuevos sujetos obligados a través de la incorporación de un nuevo concepto de sectores importantes, así como de la ampliación del concepto de servicios esenciales. Son sectores importantes: servicios postales y de mensajería; gestión de desechos; fabricación, producción y distribución de productos químicos; producción, procesamiento y distribución de alimentos; fabricación y proveedores digitales.

  Se ha evaluado en que probablemente a nivel europeo sean en torno a 60.000 los operadores importantes, de los que en España serían alrededor de 1000.

- Responsabilidad de la dirección de la empresa en la Ciberseguridad: gracias a esta actualización, la responsabilidad del cumplimiento de las medidas de ciberseguridad recae en los propios órganos directivos de la empresa.

- Se introducirán en unos casos y en otros se reforzarán los requisitos de seguridad con una lista de medidas, inculcando la necesaria concienciación sobre la privacidad desde el diseño y por defecto, la obligación de cifrado, la respuesta a incidentes, la certificación de servicios, sistemas y/o productos bajo el paraguas de esquemas europeos de certificación, así como la gestión de crisis, la gestión de vulnerabilidades y pruebas de ciberseguridad

- Se reforzará la ciberseguridad de la cadena de suministro

- Se establecerá formalmente la Red Europea de Organización de Enlace para Crisis Cibernéticas, (EU-CyCLONe).

- Disposiciones más precisas sobre el proceso de notificación, contenido y plazos en las obligaciones de notificación de incidentes

- Incremento de las atribuciones de Supervisión a la autoridad de control, entre otras novedades.

## Responsabilidad de la dirección en el cumplimiento de las medidas de gestión de riesgos de ciberseguridad.

### NIS2: Articulo 17, Gobernanza

1. Los Estados miembros se asegurarán de que los órganos de dirección de las entidades esenciales e importantes aprueben las medidas de gestión de los riesgos de ciberseguridad adoptadas por dichas entidades para cumplir con el artículo 18, supervisen su aplicación y puedan ser considerados responsables del incumplimiento por parte de las entidades de las obligaciones previstas en este artículo.

2. Los Estados miembros se asegurarán de que los miembros del órgano de dirección de las entidades esenciales e importantes estén obligados a seguir una formación, y alentarán a las entidades esenciales e importantes a ofrecer una formación similar a todos los empleados de forma periódica, para que adquieran los conocimientos y habilidades suficientes para aprehender y evaluar los riesgos de ciberseguridad y las prácticas de gestión y su impacto en los servicios prestados por la entidad.” »

La nueva Directiva NIS, la NIS2, viene a incrementar la exigencia en la seguridad de las redes y sistemas de información a los estados miembros de la UE y particularmente a sus operadores esenciales e importantes sobre los que descansan los servicios esenciales

» **Artículo 29, supervisión y ejecución de las entidades esenciales**

" (..)

**5.** Cuando las medidas de ejecución adoptadas con arreglo a las letras a) a d) y f) del apartado 4 resulten ineficaces, los Estados miembros velarán por que las autoridades competentes estén facultadas para establecer un plazo en el que se solicite a la entidad esencial que adopte las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de dichas autoridades. Si la acción solicitada no se lleva a cabo en el plazo establecido, los Estados miembros se asegurarán de que las autoridades competentes estén facultadas para:

- suspender temporalmente o solicitar a un organismo de certificación o autorización o a los tribunales, de acuerdo con la legislación nacional, la suspensión temporal de una certificación o autorización relativa a una parte o a todos los servicios o actividades pertinentes prestados por una entidad esencial;

- solicitar la imposición por parte de los organismos o tribunales competentes, de conformidad con la legislación nacional, de una prohibición temporal contra cualquier persona que ejerza responsabilidades directivas a nivel de director general o representante legal en esa entidad esencial, de ejercer funciones directivas en dicha entidad."

Con una salvedad a la hora de aplicar estas sanciones: las administraciones públicas.

## Aumento de la Supervisión

La experiencia práctica de un operador español es que las autoridades de control han buscado principalmente la colaboración con los OSE, ejerciendo poco, muy poco, la supervisión; el aumento del nivel de seguridad de los OSE se ha producido (en los casos que se haya producido) por pura autoexigencia.

La nueva NIS establece unas obligaciones/competencias concretas de supervisión a las autoridades de control:

**"**Los Estados miembros se asegurarán de que las autoridades competentes, cuando ejerzan sus funciones de supervisión en relación con las entidades esenciales, sigan un enfoque basado en el riesgo y estén facultadas para someter a dichas entidades, como mínimo, a:

**(a) i**nspecciones in situ y supervisión fuera de las instalaciones, incluidos los controles aleatorios;

**(b)** auditorías periódicas de seguridad;

**(c)** auditorías de seguridad específicas basadas en evaluaciones de riesgo o en la información disponible relacionada con el riesgo;

**(d)** escaneos de seguridad basados en criterios de evaluación de riesgos objetivos, no discriminatorios, justos y transparentes, cuando sea necesario por razones técnicas, con la cooperación de la entidad en cuestión;

**(e)** solicitudes de información necesaria para evaluar las medidas de ciberseguridad adoptadas por la entidad, incluidas las políticas de ciberseguridad documentadas;

**(f)** solicitudes de acceso a datos, documentos o cualquier información necesaria para el desempeño de sus tareas de supervisión;

**(g)** solicitudes de pruebas de la aplicación de las políticas de ciberseguridad, como los resultados de las auditorías de seguridad realizadas por un auditor cualificado y las respectivas pruebas subyacentes.**"**

Las autoridades competentes podrán emitir: advertencias sobre el incumplimiento de obligaciones, emitir instrucciones vinculantes u órdenes para subsanar deficiencias, ordenar cesar conductas que incumplan la Directiva, ordenar que el operador ajuste sus medidas de seguridad a su riesgo, informar a las personas físicas o jurídicas a las que presten servicio sobre la potencial amenaza o las medidas de protección que pueden seguir.

Podrán establecer plazos para cumplir con las órdenes.

Imponer o solicitar la imposición de sanciones Administrativas pudiendo ser estar multas y/o retirada de autorización para la provisión del servicio y/o prohibiciones temporales de ejercer funciones directivas.

Lógicamente a la autoridad española para llevar a cabo todas estas funciones se le debería dotar de un notable incremento de sus actuales y exiguos recursos.

## Cadena de suministro

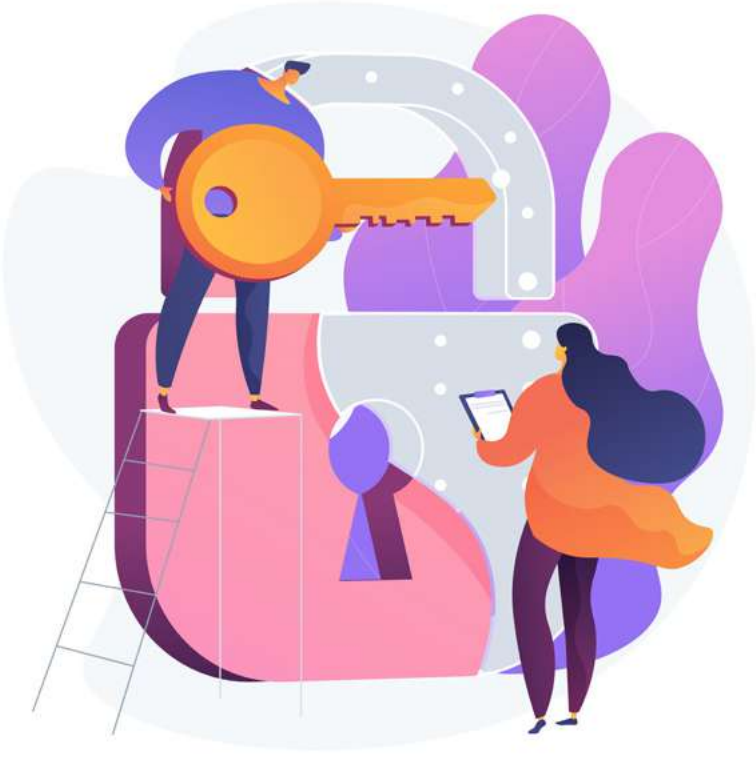
Es obvio que un operador no podrá disponer de un elevado nivel de seguridad si su cadena de suministro (sus proveedores y los proveedores de estos) para

sus servicios y productos de red y sistemas de información, no disponen de un nivel adecuado. La redacción de la NIS2 contempla desde varios planos que se debe exigir al respecto:

- **Artículo 5 Obligaciones estrategia nacional:** una política que aborde la ciberseguridad en la cadena de suministro de productos y servicios de TIC utilizados por las entidades para la prestación de sus servicios;

- **Artículo 18, medidas de seguridad:** la seguridad de la cadena de suministro, incluidos los aspectos relacionados con la seguridad de las relaciones entre cada entidad y sus proveedores directos o proveedores de servicios; tales como los proveedores de servicios de almacenamiento y procesamiento de datos o los servicios de seguridad gestionados;

- **Artículo 19, evaluaciones de riesgo coordinadas por la UE** (Cooperación, Comisión y ENISA) de cadenas de suministro TIC críticos específicos.



## Reflexiones finales.

La nueva Directiva NIS, la NIS2, viene a incrementar la exigencia en la seguridad de las redes y sistemas de información a los estados miembros de la UE y particularmente a sus operadores esenciales e importantes sobre los que descansan los servicios esenciales.

Su influencia se espera que sea mucho mayor que la de su predecesora, no tanto por las medidas de seguridad que impone a los operadores, las cuales para una organización con una madurez básica en ciberseguridad no representan una exigencia mayor que la que ya se autoimponen, sino por su mayor alcance y por la responsabilidad directa que los comités de dirección de los operadores tienen sobre la Ciberseguridad y sus resultados.

El mayor alcance como hemos visto viene tanto por la inclusión de nuevos sectores a los esenciales como por la extensión a un nuevo colectivo de sectores; los sectores importantes, así como por las exigencias que operadores, estados y UE deben ejercer sobre sus cadenas de suministro.

En cuanto a la futura transposición española, más allá de la predicción cierta que se publicará en el límite temporal, cuando no fuera de su plazo de 21 meses (así somos los españoles) y que el volumen de nuevos operadores esenciales será bajo, por las razones ya explicadas, habrá que estar atentos a una serie de cuestiones. Entre ellas:

- ¿Cómo compatibilizar las responsabilidades del CISO que el RD 43/2021 detalla con la nueva obligación de que un miembro del comité ostente la responsabilidad de la Ciberseguridad?. Su encaje debería ser simple y con una redacción abierta debería permitir que el CISO fuera o bien ese miembro del comité (muy muy pocas son las empresas hoy en día lo contemplan) o bien, que el CISO dependiera directamente de ese miembro del Comité de Dirección (lo que cada vez es más habitual).

- ¿Qué autoridad competente tendrán los nuevos operadores importantes? Al no ser estos también operadores críticos, la OCC no será su autoridad. A priori hay dos opciones, que cada sector tenga la suya ( el Ministerio/secretaría de estado correspondiente) o que haya una única autoridad .

  En realidad, la dispersión o no de las autoridades de control es una cuestión trascendental no sólo para los nuevos sectores importantes sino para el conjunto de operadores bajo la NIS. En la actualidad son 19 las autoridades, si bien la OCC es la principal. Las opciones como hemos comentado son: incrementar las autoridades de control (pasando de 19 a cerca de 35) o bien concentrar la responsabilidad en un único Ministerio/secretaría o mejor aún, hacer lo que otros países han hecho: crear una Agencia Nacional de Ciberseguridad.

- ¿Se dotará con los recursos necesarios a la autoridad/autoridades?

- ¿Cómo se concretarán en el correspondiente reglamento de desarrollo los requerimientos a la cadena de suministro?

# Ciberseguridad: La eterna amenaza para todo tipo de organizaciones

MARTINIANO MALLAVIBARRENA

Global head of incident response
**Telefónica Tech**

Contacta:

www.linkedin.com/in/mmallavibarrena/

**Desde los inicios del uso generalizado de la tecnología en empresas y organismos públicos en la segunda mitad del pasado siglo, la amenaza de "acciones maliciosas" estuvo presente. Si bien es cierto que entonces tanto las motivaciones como su impacto hacían de aquellos primeros incidentes algo casi romántico o divertido.**

A medida que este siglo XXI comenzó a ser una realidad, comprendimos que el mundo de la tecnología había cambiado de forma sustancial. Un cambio que provocó que ese famoso "perímetro de seguridad" (la universal metáfora de los muros de un castillo) se difuminara entre dispositivos móviles, personal itinerante y servicios en la nube. En esta época nuestros activos tecnológicos y nuestros datos están ubicados en lugares distintos y cambiantes, y a veces fuera de nuestras fronteras.

Todas las organizaciones y empresas del mundo tienen claro que el ciberespacio es un océano de oportunidades, pero también es un nuevo mundo de riesgos globales de los que no siempre sabemos protegernos.

## Amenazas globales, cada vez más profesionales

Este nuevo escenario global de amenazas desde Internet representa para las organizaciones con dispositivos móviles, servicios en la nube y subcontratistas y socios un nuevo paradigma donde hay algunos puntos que recordar:

- Los actores maliciosos se han profesionalizado siendo asumida su actividad por grupos de delincuencia organizada internacional.
  - Muchos grupos de actores "alquilan" sus herramientas de ataque y cifrado en modelos de afiliados donde delincuentes de menor nivel de preparación tienen ahora una gran potencia de ataque a cambio de compartir sus beneficios dentro del "contrato de afiliación".
- Actores maliciosos que trabajan por encargo para terceros.
- Al mismo tiempo que la tecnología que nos protege ha evolucionado y los


servicios en la nube se han desarrollado, los actores maliciosos han realizado sus esfuerzos paralelos para estar "a la última" y seguir siendo un problema para todos.

- En el terreno jurídico, algunos asuntos clave siguen sin resolverse de forma satisfactoria pese a los esfuerzos de las autoridades. Uno de ellos es el de la imposibilidad práctica de realizar atribuciones delictivas en ciertas zonas de Internet como TOR en la dark web. Ello da una relativa impunidad a esos actores.

Más allá de los estereotipos de los "hackers malos", que realmente no se ponen capucha para atacar ni teclean a oscuras en portátiles llenos de pegatinas, las principales amenazas que tiene ahora mismo una organización que está conectada con Internet se podrían resumir en estos grupos:

- **Ransomware:** Ataques destructivos que cifran los datos de la organización y exigen rescate para dar las herramientas y las claves secretas que permiten su recuperación.

## El ciberespacio es un océano de oportunidades, pero también es un nuevo mundo de riesgos globales de los que no siempre sabemos protegerno

- **Denegación de servicio:** Ataques muy dirigidos a detener o deteriorar los sitios web o sistemas. Pueden ser por activismo, por encargo, por recompensa, etc. Se sobrecarga artificialmente el entorno hasta que deja de funcionar o lo hace de forma muy pobre.

- **Ataques relacionados con correo electrónico y suplantación de identidad**: Multitud de fraudes son habituales hoy en día utilizando como vía de entrada una infección inicial al pulsar un enlace o abrir un fichero incluido en un mensaje "engañoso" (phishing se traduciría en inglés como "pescando") o mediante el robo de la identidad en una red social. Una vez logrado, intentan abonar facturas o nóminas en cuentas bancarias distintas a las habituales.

- **Robo de datos:** Por encargo o para pedir recompensa, en estos casos los actores se apoderan de gran cantidad de datos de la organización y los exfiltran (posiblemente utilizando los propios mecanismos legítimos de la empresa) para ser vendidos, subastados, etc.

- **Malware:** Otras familias de software malicioso son utilizadas con

Todas las organizaciones modernas deben tener un plan de seguridad concreto y unas medidas implantadas

» frecuencia para perjudicar los sistemas (virus), espiar (puertas traseras, grabadores de pulsaciones de teclado, etc.) o para sacar beneficio. Por ejemplo, los "mineros" son programas que minan criptomonedas en la infraestructura sin ser la empresa consciente, generando beneficios económicos para el actor malicioso.

- **Insiders:** En ocasiones se tiene al "enemigo en casa" y son empleados o colaboradores que actúan por venganza o para obtener beneficio económico.

Recordemos para completar esta foto panorámica que los actores maliciosos suelen ser grupos de delincuencia organizada internacional, lo que se debe tener en cuenta a la hora de realizar denuncias a los cuerpos policiales o agencias de protección de datos.

## El impacto real es multidimensional

Este tipo de incidentes de seguridad pueden llegar a tener impactos realmente serios en las organizaciones: operacionales, económicos, laborales y reputacionales. Por ello es rigurosamente necesario tener siempre en mente una valoración de riesgos, un plan de dirección y mantener una actitud defensiva en todos los empleados y colaboradores.

- **Problemas operacionales:** Muchos incidentes de seguridad y sobre todo los de tipo DDOS (denegación de servicio) o basados en ransomware generan automáticamente la indisponibilidad de los sistemas afectados, lo que puede llevar al colapso de las operaciones o a generar una degradación de servicios importante.

- **Problemas económicos:** Tanto por lucro cesante como por sanciones o multas relacionadas con incumplimiento de contratos o cancelación de pedidos, las pérdidas económicas suelen ser siempre una constante en estas situaciones.

- **Impacto legal:** Además de posibles problemas con agencias de protección de datos, hay otros riesgos; por ejemplo, si un cliente o socio cree que ha existido negligencia. Muchos de estos incidentes resultan en denuncias mercantiles, administrativas e incluso penales.

- **Reputación:** Si se sufre un incidente grave de ciberseguridad es más que probable que el mercado sea consciente (caso de una universidad donde sus entornos online dejan de funcionar en época de matriculación o exámenes finales) y ello afectará de alguna manera a la reputación de la organización. En caso de fugas de datos o ransomware, los datos de las plataformas (de clientes, socios, empleados) pueden acabar subastados en un mercado negro de la internet profunda y accesibles al mejor postor.

## ¿Qué podemos hacer?

Todas las organizaciones modernas deben tener un plan de seguridad concreto y unas medidas implantadas. En los casos más complejos, de multinacionales de gran tamaño, se debe contar con equipos propios y empresas especializadas para ayudarles. En los casos más sencillos (trabajadores autónomos, pequeñas y medianas empresas) se dispondrá de algunos servicios básicos empaquetados (posiblemente del proveedor de Telecomunicaciones) y un software antivirus. En todos los casos, la cultura de la seguridad juega un papel fundamental.

Si se trata de un gran conjunto de empresas, invirtiendo millones de euros al año en productos y servicios de tecnología de ciberseguridad, pero los empleados (propios o externos) siguen utilizando pendrives "encontrados" en la cafetería o abriendo ficheros PDF adjuntos de un mail algo extraño, seguirá habiendo un alto riesgo de incidente grave.

Las principales áreas de actuación se pueden agrupar de la siguiente manera:

- Tener un plan director de seguridad (empresas grandes, organismos con cumplimiento obligatorio) y una serie de medidas activas de ciberseguridad que necesariamente deben cubrir -entre otros bloques- la gestión de identidades, la protección perimetral (cortafuegos y otros sistemas), la detección y respuesta (los sistemas de tipo EDR/XDR son

especialmente útiles para ataques complejos como los que utilizan ransomware), la Ciberinteligencia (aportan información accionable de amenazas regionales o sectoriales) y siempre que sea posible, la seguridad ofensiva (los famosos hackers éticos que "atacan por contrato" descubriendo los puntos débiles, vulnerabilidades, etc.)

- Contar con socios tecnológicos y de servicios acorde al tamaño, complejidad y huella geográfica. Si se tiene presencia internacional, complejidad de sistemas, servicios críticos en la nube, etc. no se deben tomar decisiones en cuanto a proveedores o fabricantes con el factor "precio" como principal indicador de valor. Se debe valorar muy bien la ratio coste-beneficio de esta decisión (¿cuánto cuesta no estar operativo 48 horas?).

- Conocernos como organización: El peor momento para comprobar si se tiene el inventario de activos o diagramas de conectividad actualizados es en mitad de la noche por un incidente ransomware. Se debe conocer como organización digital, los activos, contratos con terceros, comunicaciones, presencia en Internet, etc. El delegado de protección de datos (DPD) debe ser consciente (y utilizar información siempre actualizada) de todos estos activos, sobre todo en cuanto a datos personales se refiere.

- Sólo la práctica lleva a la perfección: El sector de la ciberseguridad sigue una evolución frenética donde unos y otros intentan hacer un uso táctico de la tecnología a su favor: o para atacar o para defender (caso de la inteligencia artificial, en uso constante por ambos mandos). Es un error pensar que por contratar a un gran proveedor de servicios de ciberseguridad se puede bajar la guardia. Hay que seguir realizando labores de concienciación con los empleados, ejercicios de hacking ético o simulaciones de crisis para estar preparados siempre.

Una vez terminado el trabajo de la respuesta a incidentes es el momento de hacer recapitulación de las lecciones aprendidas en esta actividad y mejorar la postura de seguridad antes de que comience un nuevo incidente

En el caso de Telefónica Tech, nuestro portafolio de servicios se puede contratar a nivel internacional y obtener el beneficio de una inteligencia compartida por más de 3.000 profesionales en varios países. Nuestras plataformas de inteligencia permiten que nuestros clientes tengan una atención mucho más precisa al estar compartiendo información de amenazas de muy reciente adquisición (un ataque por la mañana en Europa se puede producir por la tarde en USA y al atenderlo, aportamos un conocimiento reciente del actor y sus técnicas de actuación).

La mayoría de los servicios de ciberseguridad se deben establecer en modo 24x7 y tener muy claro cómo "conectar" a los proveedores con nuestro equipo IT/Seguridad interno y con el DPD, en muchos casos.

En este contexto en el que no existe 100% seguridad, la gran pregunta es: ¿qué se debe hacer en caso de sufrir un incidente grave de seguridad?

1. **Valoración rápida del nivel de daño y de impacto en negocio.**

2. **Verificar si se tiene claro el guión (playbook) para este caso y aclarar los roles de la organización que deben involucrarse (y en qué momento).**

3. **Comprobar si se cuenta con un equipo de respuesta a incidentes listo para activarse (propio, ajeno, mixto) o contactar con proveedores reputados como Telefónica Tech de forma que en cuestión de minutos podamos organizar un equipo extendido de respuesta para trabajar hasta que la amenaza haya sido erradicada y los sistemas recuperados.**

Una vez terminado el trabajo de la respuesta a incidentes es el momento de hacer recapitulación de las lecciones aprendidas en esta actividad y mejorar la postura de seguridad antes de que comience un nuevo incidente.

# Confianza en la Ciberseguridad *con soluciones basadas en la experiencia*


BORIS DELGADO
Director de Soluciones de Digitalización y Tecnología
**AENOR**
Contacta:
linkedin.com/in/borisdelgadoriss

CARLOS MANUEL FERNÁNDEZ
Asesor Estratégico de TI
**AENOR**
Contacta:
linkedin.com/in/carlosmfs

**Son tiempos convulsos. Son tiempos inestables. Convivimos con multitud de riesgos y amenazas que impactan negativamente en nuestras organizaciones. Es el caso de la invasión de Rusia a Ucrania, con un modelo de guerra híbrida (física y virtual), que ha traído consigo una crisis económica y energética de profundo calado. Una crisis que se suma a las consecuencias de la alerta sanitaria global provocada por el COVID-19 que ha dejado huellas permanentes en la sociedad, los gobiernos y las empresas; cambiando nuestra forma de trabajar y de relacionarnos entre organizaciones y personas.**

Son tiempos convulsos y para gestionarlos es imprescindible avanzar en la transformación digital que muchas organizaciones ya iniciaron antes de la pandemia, con especial consideración a la ciberseguridad. En palabras de Félix Barrio, CEO de INCIBE (Instituto Nacional de Ciberseguridad): "La ciberseguridad es ya una palanca de competitividad, de continuidad y de resiliencia para nuestra sociedad"

Sabemos de la potencia de computación actual, que permite la ejecución de modelos de inteligencia artificial,

machine learning y deep Learning. Nos empezamos a familiarizar con tecnologías disruptivas como Blockchain, o con nuevos paradigmas como Edge-Computing, Metaverso, Web3, Data Mesh o la computación cuántica.

Muchas de ellas son necesarias para la transformación y modernización empresarial, si bien requieren de nuevas herramientas e instrumentos actualizados que hagan frente a las nuevas ciberamenazas y ciberriesgos de la actual sociedad digital.

Por todos es conocido el importante esfuerzo por parte de todas las administraciones de cada país; como son los fondos de recuperación europeos y nacionales que consideran la digitalización y la ciberseguridad prioritarias en sus estrategias de ayuda. Es la transformación digital uno de los ejes principales muy presente en los fondos Next Generation EU, el instrumento con el que se apoya la recuperación económica tras la crisis provocada por el COVID-19.

## Retos y cuestiones en los comités de dirección

Los analistas de IDC Research, han estimado que en 2023 el mercado de la ciberseguridad retomará la senda del crecimiento a un ritmo del 7,7% para hacer frente al incremento exponencial de los ciberataques a las organizaciones públicas y privadas.

Son por tanto, la ciberseguridad junto con la privacidad de los sistemas y los datos, los retos más prioritarios en los comités de dirección de las organizaciones, para que la transformación digital en ellas sea una realidad. Y es que es habitual encontrar en su orden del día tres cuestiones fundamentales:

- ¿Se conocen y gestionan los ciberriesgos y las ciberamenazas que puedan afectar a su organización en la actual era digital?
- ¿Se es capaz de detectar y gestionar un incidente de seguridad, informando de forma adecuada a sus *stakeholders* y valorando el impacto en su organización?
- ¿Se sabe si los datos o sistemas de información corporativos han sido comprometidos en los últimos seis meses?

**Son tiempos convulsos y para gestionarlos es imprescindible avanzar en la transformación digital que muchas organizaciones ya iniciaron antes de la pandemia, con especial consideración a la ciberseguridad**

Para dar respuesta a estas cuestiones a nivel internacional, ISO a través de su comité técnico ISO/IEC JTC 1/SC 27, tomó cartas en el asunto y en febrero de 2022 publicó la actualización de uno de sus estándares técnicos más reconocidos y utilizados: *la ISO/IEC 27002 - Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de Seguridad de la Información.*

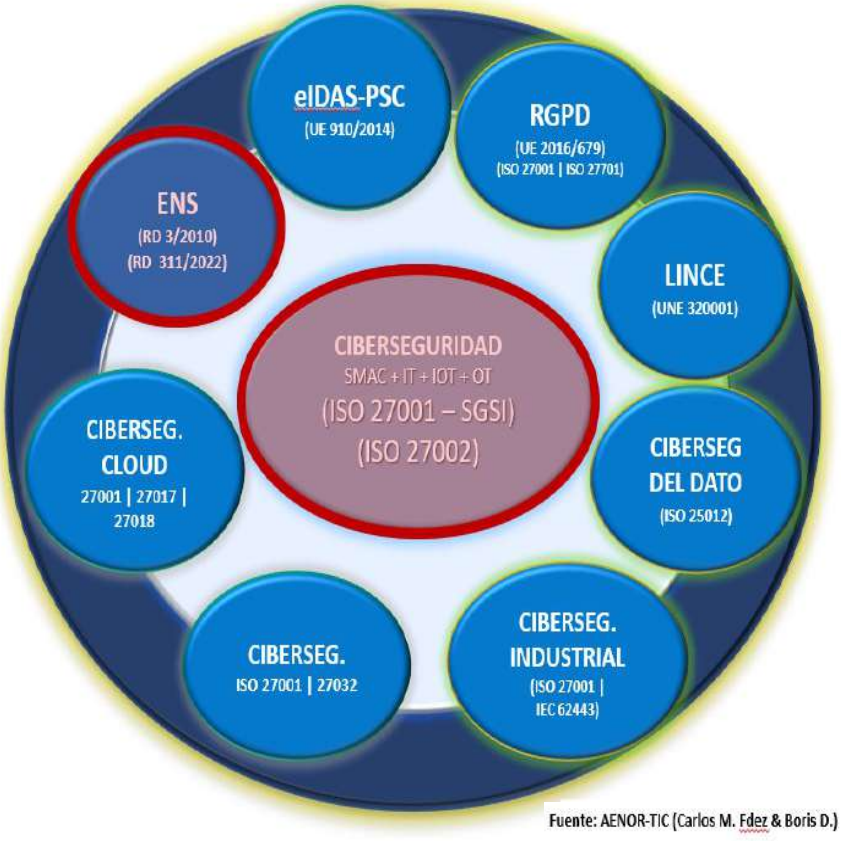
También a nivel nacional, en España los responsables del Esquema Nacional de Seguridad, agilizaron la actualización de su RD 3/2010, viendo la luz el nuevo RD 311/2022 el pasado 4 de Mayo de 2022.

Sin duda, el colofón a estas actualizaciones fue la publicación el pasado 25 de octubre del estándar de referencia *ISO/IEC 27001 - Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información – Requisitos.*

Así, teniendo en cuenta el escenario y retos anteriores, AENOR, fiel a su propósito de aportar soluciones que generen confianza entre organizaciones y personas, diseñó la plataforma de confianza: ***"Proteger la Seguridad y Privacidad de los datos"***. Una respuesta ante los escenarios tecnológicos anteriormente presentados.

Esta plataforma se apoya en el modelo de ciberseguridad y privacidad de AENOR basado en estándares internacionales ISO, tomando como pilares fundamentales la ISO/IEC 27001 e ISO/IEC 27002 junto con el estado del arte de las actuales y futuras ISO. Asimismo, de las leyes y reglamentaciones españolas y europeas en materia de Ciberseguridad; como es ya el nuevo »

**Figura 1. Modelo de Ciberseguridad & Privacidad**




Fuente: AENOR-TIC (Carlos M. Fdez & Boris D.)

Esta plataforma de confianza propone un modelo eficaz, eficiente y dinámico, actualizado constantemente, que está basado en las mejores prácticas: los estándares ISO

» Esquema Nacional de Seguridad, el actual Reglamento General de Protección de Datos Personales, el RD 7/2022 sobre Seguridad 5G, la recién publicada Directiva NIS2, la regulación DORA, o Cybersecurity/ Cyberesiliency Act, etc.

Es decir, esta plataforma de confianza propone un modelo eficaz, eficiente y dinámico, actualizado constantemente, que está basado en las mejores prácticas: los estándares ISO que han sido consensuados por 155 expertos de 155 países, y dotan de una mayor visión y capacidad de reacción a la ciberseguridad. *(Figura 1)*

Soluciones consolidadas: aspectos clave en las nuevas ISO 27001, ISO 27002 y el nuevo ENS.

Con más de 15 años de historia, la ISO/IEC 27002 es una norma no certificable. Es una guía de implantación de controles de seguridad de la información que ahora se ha actualizado para mitigar los riesgos y amenazas de la actual era digital.

Estos controles de seguridad se incluyen en el Anexo A de la ISO/IEC 27001 - Sistema de Gestión de Seguridad de la Información (SGSI), que sí es certificable, como la de aquellos que hay que aplicar, según el análisis de riesgos de los procesos/servicios de la organización y conforme a la mejora continua.

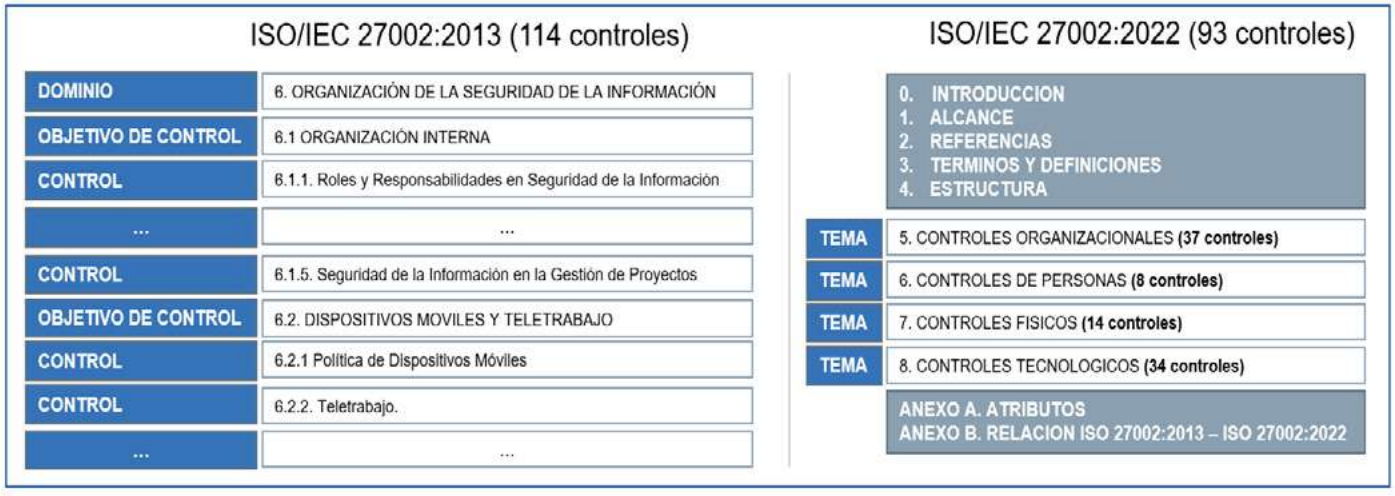
La buena noticia es que ISO/IEC 27001, ha mantenido prácticamente intactos sus requisitos y su índice sigue alineado a la estructura de alto nivel que otras normas ISO mantienen (apartados del 4 al 10).

Pero si ha actualizado su Anexo A, conforme a la nueva ISO/IEC 27002 que es la que ha actualizado buena parte de su estructura y contenido.

Principalmente nos encontramos aclaraciones en la redacción y un nuevo apartado:

- **Apartado 4.4,** se sustituye norma internacional por documento, y hace mención a “incluir procesos necesarios y sus interacciones”.
- **Apartado 5.3**, donde de forma explícita menciona que la comunicación en la organización sea interna.
- **Apartado 6.1.3,** donde se referencia al Anexo A de controles.
- **Apartado 6.2**, donde se explicita que los objetivos de seguridad se supervisan y documentan.

Figura 2. Comparativa de la anterior y actual versión de ISO/IEC 27002




- **(nuevo) Apartado 6.3 – Planificación de los cambios.** Se incorpora este apartado, con el fin de planificar los cambios del SGSI en general, donde se puede considerar la propia adaptación del sistema de gestión de la versión de 2017 a la actual.

La ISO/IEC 27002 proporciona un conjunto de controles generales de seguridad de la información, contemplando para cada uno de ellos una guía de implementación.

Se ha diseñado para ser utilizada por las organizaciones públicas y privadas de tres posibles formas:

1. en el contexto de un SGSI basado en la norma ISO/IEC 27001 (en su Anexo A de controles para actualizar los 114 a 93 controles);

2. para implementar controles de seguridad de la información basados en las mejores prácticas reconocidas internacionalmente;

3. para desarrollar sus propias directrices de gestión de la seguridad de la información;

Esta nueva versión de ISO/IEC 27002 ha realizado cambios, principalmente en la estructura de la norma/estándar, y son:

1. **Cambio de nombre** del comité técnico de ISO que lo desarrolla y el nombre del estándar.

## La nueva versión de ISO/IEC 27002 ha realizado cambios, principalmente en la estructura de la norma/estándar

2. **Nueva estructura, considerando "temas"** de seguridad de la información.

3. **Nueva estructura, considerando "atributos"** de los controles.

4. **Nuevos controles e integración de otros,** desde la anterior versión de ISO/IEC27002:2013. (se pasan de 114 a 93 controles) *(Figura 2)*

Para completar las referencias que nos ayudan en la reorganización de la ciberseguridad, el nuevo RD 311/2022 actualiza al anterior RD 3/2010 – ENS y a su posterior modificación RD 951/2015.

Esta versión vigente de ENS establece la política de seguridad para la protección adecuada de la información tratada y los servicios prestados a través de un planteamiento común de **principios básicos (7), requisitos mínimos (15), medidas de seguridad** y mecanismos de conformidad y monitorización para la Administración Pública, así como para los proveedores tecnológicos del sector privado que colaboran con la Administración.

Recordemos el hito conseguido por todas las organizaciones que han confiado desde hace años en las certificaciones ISO/IEC 27001: en el último informe de ISO, España se sitúa en el top ten de países del mundo por número de certificaciones

Entre las novedades del nuevo ENS se encuentran:

- **Evolución de los principios básicos:** prevención, detección, respuesta y conservación, incluyendo el principio de vigilancia continua.
- **Modificación de la terminología:** de la seguridad por defecto a Mínimo privilegio.
- **Actualización de los controles/medidas de seguridad.** Muchas de ellas se mantienen, otras han incrementado su exigencia, y otras se han simplificado o eliminado. En definitiva, de 75 medidas se actualizan a 73.
  - Marco Organizativo (se mantienen 4)
  - Marco Operacional (de 31 a 33). Hay que destacar la incorporación de controles en entornos cloud (nube).
  - Marco de Protección (de 40 a 36)
- la incorporación de la figura del **perfil de cumplimiento,** cuyo objetivo es alcanzar una adaptación al Esquema más eficaz y eficiente.
- el establecimiento de un **protocolo de actuación** ante ciberincidentes, donde se establecen las condiciones de notificación al CCN-CERT.
- un nuevo sistema de codificación de los requisitos de las medidas de seguridad (refuerzos), cuyo objeto es facilitar de manera proporcionada la seguridad de los sistemas de información, su implantación y su auditoría

## Confianza en la ciberseguridad a través de las normas y estandares ISO.

Recordemos el hito conseguido por todas las organizaciones que han confiado desde hace años en las certificaciones ISO/IEC 27001: en el último informe de ISO, España se sitúa en el *top* ten de países del mundo por número de certificaciones; AENOR, con más del 50% de estas.

Por último, no debemos olvidar que los estándares de ciberseguridad deben aportar soluciones a las organizaciones que las implantan y certifican, y considerar los desafíos que ya están sobre la mesa: *blockchain*, BigData, Edge-computing, Data Mesh, etc. y su relación con la Inteligencia Artificial, modelos matemáticos, datos y algoritmos que tomarán decisiones en la actual sociedad digital.

NIPPON GASES
The Gas Professionals

Juntos somos
**"The Gas Professionals"**
y todos tenemos
el mismo objetivo:
**"Making life better through gas technology".**


nippongases.com

# Sistemas y Plataformas Aeroespaciales Seguras

ANGEL L. LÓPEZ ZABALLOS

Cyber Defence Architect
**Airbus Defence & Space**

**Contacta:**

www.linkedin.com/in/angellopezzaballos/

En los últimos años la ciberseguridad ha pasado de ser un área de conocimiento y especialización exclusiva de profesionales del sector tecnológico, a un área conocida por el público en general.

Los continuos ciberataques a organismos públicos han puesto en alerta a la clase política y a todos los cuerpos encargados de velar por la seguridad y el bienestar de la población. Asimismo, la reciente guerra de Ucrania ha traído consigo un mayor grado de atención a la ciberseguridad a nivel nacional, intensificando la preocupación por la ciberdefensa en el espacio europeo y a nivel mundial.

Como resultado de ello, desde Europa se han lanzado multitud de iniciativas e instrumentos de financiación relacionados con la ciberseguridad, centrándose inicialmente en la regulación de productos y procesos. Sin embargo, queda todavía un largo recorrido para implementar soluciones destinadas a la protección de ciberamenazas en el área de Infraestructuras Críticas.

Por otro lado, la creciente convergencia entre Tecnologías de la Información (IT) y Tecnologías de Operaciones (OT), así como los largos ciclos de vida involucrados, conducen a mayores riesgos cibernéticos, incluida la posibilidad de ataques cibernéticos exitosos. Por tanto, es crucial considerar la ciberseguridad en cada etapa del proceso de diseño de los sistemas y las plataformas. .

## Metodología de Ciberseguridad Integral

La ciberseguridad requiere de una metodología que incluya un enfoque único de "seguridad por diseño", necesaria para abordar problemas de diseño fundamentales y encontrar nuevas formas de protegerse contra los ataques cibernéticos más peligrosos, combinando evaluaciones de vulnerabilidades técnicas tradicionales y un enfoque centrado en las personas como elemento fundamental del sistema. En esta metodología se incluyen procesos de mejora continua que abarcan el diseño y desarrollo, la arquitectura e integración, la puesta en servicio y mantenimiento, así como el desmantelamiento seguro de los sistemas y plataformas. (*Figura 1)*

Figura 1. Metodología de Ciberseguridad Integral


## Sector Aeronáutico y Espacial

La complejidad de los sistemas informáticos integrados en aeronaves, satélites y otras plataformas aeronáuticas y espaciales siguen aumentando vertiginosamente.

La ciberseguridad en el sector aeronáutico requiere de una integración de las nuevas plataformas, junto con la mejora de la seguridad digital de los aviones que ya están en servicio. Esto es aplicable tanto al sector comercial como a los diferentes programas militares y plataformas multipropósito, lo que implica un profundo conocimiento de la ciberseguridad de los sistemas de misión y de soluciones de gestión de tráfico aéreo para los actuales y nuevos sistemas, plataformas aéreas no tripuladas y sensores de ciberdefensa a bordo. (*Figura 2)*

Figura 2. Sector Aeronáutico y Espacial


## Nuevos retos y desafíos

El sector espacial se encuentra igualmente ante nuevos desafíos de seguridad en las comunicaciones por satélite, incluida la reconfiguración en órbita, las radios definidas por software localizadas en el espacio y los segmentos terrestres del usuario. Todo ello requerirá de nuevos enfoques de innovación, incluyendo líneas de investigación en torno a la computación cuántica, para llevar a cabo la seguridad integral de las mega-constelaciones en órbita terrestre baja (LEO), aplicando y manteniendo la protección de los sistemas de navegación y comunicaciones en el espacio y todos los satélites de observación de la Tierra.


# El factor humano en la Ciberseguridad

GERARDO SARMIENTO FERNÁNDEZ

CISO / Jefe de la Oficina de Ciberseguridad

**ENAIRE**

Contacta:

www.linkedin.com/in/gerardosarmiento/

La navegación aérea es, sin lugar a dudas, uno de los sectores en los que la seguridad adquiere un mayor protagonismo. No en vano, a pesar de la gran complejidad de sus operaciones y los sistemas que las sustentan, las cifras lo avalan como el medio de transporte más seguro del mundo.

En **ENAIRE**, Operador de Servicios Esenciales y principal proveedor de servicios de navegación aérea a nivel nacional, consideramos a la seguridad en su conjunto y a la **ciberseguridad** en particular como elementos nucleares y estratégicos. Así lo reflejan explícitamente tanto nuestros valores, estableciendo la seguridad como nuestra **máxima prioridad** y el **pilar** en el que descansa nuestro servicio y el bienestar de las personas, como nuestros objetivos estratégicos, priorizando el refuerzo continuo de la seguridad y prestando especial atención a la cultura de ciberseguridad ante nuevos riesgos emergentes.

Esta visión y compromiso se vertebran a través de nuestro Sistema de Gestión de la Seguridad de la Información (SGSI), quedando a su vez evidenciados mediante sendos Certificados de Conformidad con el Esquema Nacional de Seguridad, tanto en Categoría Media -relativa a los sistemas de gestión empresarial y apoyo- como en Categoría Alta, abarcando todos los sistemas operacionales críticos, directamente involucrados en la prestación de los servicios de navegación aérea. Adicionalmente, el hecho de haber sido el

**primer Operador Crítico y de Servicios Esenciales en haber logrado dicha certificación en su categoría más exigente, no hace sino refrendar tal convencimiento.**

En este contexto, además de las herramientas, equipamiento y recursos necesarios, un elemento singularmente relevante para nosotros es el factor humano, **las personas**. Nada de lo anterior es viable si no cuenta con el respaldo de un equipo multidisciplinar experto, altamente cualificado y actualizado, capaz de ejecutar las tareas encomendadas de forma ágil y eficaz.

Esta consideración es, de hecho, aplicable a toda nuestra plantilla. Iniciativas como la formación, concienciación y sensibilización son claves en la consecución y mantenimiento de los más altos niveles de seguridad. Así queda recogido en nuestro **Plan Estratégico de Ciberseguridad** 2020-2025 (PROTEGE), aprobado y promovido por la Dirección General de la compañía.

En ENAIRE tenemos muy presente este compromiso y lo abordamos, además, tratando de acercar el lado más humano y amable de la ciberseguridad a cada una de las personas que componen nuestro equipo, procurando que se sientan reflejadas en sus actividades cotidianas, tanto profesionales como personales, de modo que puedan asimilar fácilmente los contenidos e interiorizar mejor las recomendaciones.

Si hay algo que diferencia a la ciberseguridad frente a otras áreas es que, dada su presencia y relevancia en nuestras propias vidas, resulta indisociable la vertiente personal de la profesional. No porque convivan tecnologías o sistemas, sino por el factor común que une todos los puntos: **la persona**. Si hasta ahora ya teníamos una estrecha relación con las nuevas tecnologías, en este nuevo escenario de teletrabajo la dependencia tecnológica es total y la ciberseguridad adquiere un papel protagonista a todos los niveles: videollamadas, compras por internet, bulos, estafas bancarias, suplantación de identidad… No se trata de algo que se circunscriba a un entorno específico, horario o actividad concreta. Por el contrario, abarca toda nuestra vida digital y de ahí la necesidad de difundir conocimiento e interiorizar buenas prácticas a título personal.

Iniciativas como la formación, concienciación y sensibilización son claves en la consecución y mantenimiento de los más altos niveles de seguridad. Así queda recogido en nuestro Plan Estratégico de Ciberseguridad 2020-2025 (PROTEGE), aprobado y promovido por la Dirección General de la compañía

Por todo ello, en ENAIRE dedicamos un gran esfuerzo en promover cualquier iniciativa que redunde en una mayor y mejor formación, concienciación y sensibilización de todo el personal. En este sentido, elaboramos cursos de ciberseguridad, difundimos alertas y noticias, publicamos artículos, disponemos de un portal web específico actualizado con novedades y recomendaciones, desarrollamos iniciativas gamificadas e interactivas, así como valoramos y promovemos cualquier actividad divulgativa que revierta en una mejor capacitación de todos.

Fruto de este esfuerzo, ENAIRE ha sido recientemente galardonada con el **Premio al Programa de Formación Cultura Cibersegura,** concedido por Entelgy, reconociéndonos como referente de concienciación en ciberseguridad y de éxito colaborativo entre las áreas técnicas, comunicación y personas, a través de nuestra Oficina de Ciberseguridad, Dirección de Sistemas y Campus ENAIRE.

Este reconocimiento viene a reforzar y confirmar un valor fundamental en ENAIRE, por encima de cuestiones técnicas y más allá de complejas arquitecturas tecnológicas, sobre el que se cimienta la seguridad, ya sea operacional, física o ciberseguridad: somos un solo y gran equipo gracias a l**a colaboración y participación de todos.**

# La acreditación, al servicio de la ciberseguridad

JOSÉ LUIS BORREGO

Jefe del departamento de laboratorios y certificación de producto

**ENAC**

**Contacta:**

https://www.linkedin.com/in/jos%C3%A9-luis-borrego-nadal-47b090155/?originalSubdomain=es

**La información, uno de los principales activos de las compañías, ha convertido al espacio digital en su principal medio natural. Una esfera con novedosas tecnologías (el blockchain, la inteligencia artificial, la robótica, el big y smart data...), que exige una interconexión constante volviéndonos más dependientes de las infraestructuras que hacen posible el ciberespacio y más vulnerables a acciones hostiles contra dichas infraestructuras. Así, en los últimos años, se ha presentado la ciberseguridad como un elemento de especial importancia para todos los sectores, con requisitos cada vez más exigentes.**

En este ámbito, las actividades de evaluación y control tienen un gran protagonismo, ya que ayudan a garantizar la seguridad, funcionalidad, operatividad y resiliencia de productos, procesos, sistemas y servicios digitales de comunicación; la seguridad, confidencialidad, integridad y disponibilidad de información y la protección de los usuarios, y a impulsar, en definitiva, un uso seguro del ciberespacio.

Sin embargo, el valor que pueden aportar estas evaluaciones a las empresas depende del buen hacer y la competencia de las entidades que las realizan. La acreditación es la herramienta que, a nivel internacional, aporta esa confianza y credibilidad, ya que solo las entidades acreditadas han demostrado a un tercero independiente, la Entidad Nacional de Acreditación en España (ENAC), mediante rigurosos procesos de evaluación, que disponen de la necesaria competencia técnica para realizar su actividad.

En este sentido, el mercado español cuenta ya con más de 50 entidades acreditadas por ENAC, que han demostrado su competencia técnica para evaluar productos y servicios relacionados con la seguridad de la información.

## Ciberseguridad, clave en Europa

La importancia de la ciberseguridad ha continuado en aumento tanto a nivel europeo como en las agendas de la mayoría de los Gobiernos, ya que, en ocasiones, puede llegar a afectar a la seguridad nacional. Así, el Reglamento (UE) 2019/881, más conocido como “Cybersecurity Act”, que tiene el objetivo de reforzar la lucha contra las amenazas y ataques en materia de ciberseguridad, otorga un papel central a la acreditación para asegurar la fiabilidad y comparabilidad de las certificaciones concedidas por las diferentes entidades que operan en toda Europa y garantizar, así, la robustez del sistema y la consecución de sus objetivos. Por ello, el reglamento exige la acreditación de todas las entidades que operen en los esquemas europeos en materia de ciberseguridad con

independencia de que estos sean organizaciones privadas o la propia Administración.

Dicho de otro modo, se ratifica la confianza del Parlamento y la Comisión Europea en la acreditación, herramienta a la que recurren cada vez con mayor frecuencia para aportar garantías a las actividades de evaluación de conformidad en la UE.

Una confianza también visible en los tres nuevos esquemas europeos que la Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha comenzado a desarrollar en el marco del Cybersecurity Act: el Esquema de Certificación de Ciberseguridad Europeo basado en Common Criteria (EUCC), el Esquema de Certificación Europeo de Ciberseguridad en Servicios en la Nube (EUCS) y el esquema de certificación de la ciberseguridad de la UE para las redes 5G.

El primero de estos esquemas, EUCC, el más avanzado en su desarrollo ya que sustituirá al actual acuerdo europeo SOG-IS (Senior Officers Group Information Systems Security), permite el reconocimiento de certificados de seguridad de productos a los más altos niveles de exigencia en el ámbito de la Unión Europea.

## Más de 50 entidades acreditadas por ENAC han demostrado su competencia técnica para evaluar productos y servicios relacionados con la seguridad de la información

En este caso, ENAC ha participado, en representación de la organización europea de acreditadores (EA), en el grupo de trabajo de ENISA que desarrolla la propuesta sobre cuáles deberán ser los requisitos de acreditación, tanto para los laboratorios de ensayo como para las entidades de certificación que realizan evaluaciones de productos dentro del esquema EUCC.

### Más apoyo a las políticas públicas

Además de la mencionada Cybersecurity Act, la acreditación ha venido siendo usada desde hace tiempo en el ámbito de la ciberseguridad, como, por ejemplo, con la certificación de los sistemas de gestión de la seguridad de la información, ensayos y certificaciones de seguridad de los productos y sistemas de tecnologías de la información de acuerdo con estándares como Common Criteria o Lince, que evalúan la capacidad de un producto TIC para tratar la información de forma segura.

Asimismo, el Reglamento (UE) nº910/2014, eIDAS, para la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, ha establecido la acreditación para asegurar la competencia técnica, la operatividad e imparcialidad de los organismos que auditan y certifican a los proveedores de servicios de identificación electrónica.

A nivel nacional, el Esquema Nacional de Seguridad (ENS) fija los requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración Pública y en los servicios que los operadores privados presten a entidades públicas. Para aportar las máximas garantías, las entidades de certificación que quieran actuar en el marco de dicho esquema deben contar con la acreditación de ENAC.

# La inteligencia artificial en la cyber defensa

LAURA BAUS
Cyber Defence Manager
**Vodafone**

Contacta:
www.linkedin.com/in/laurabauslerma/

"Lo que es pues de gran trascendencia en la guerra es desbaratar la estrategia del enemigo"
*Sun Tzu*

**Los profesionales de ciberseguridad se enfrentan a riesgos que serán significativamente influenciados por las denominadas tecnologías disruptivas o emergentes estas, van a suponer un antes y un después en el cibercrimen. La estrategia de los atacantes, sin duda, se verá fuertemente marcada por el apoyo en estas tecnologías. Con ello, los profesionales de ciberseguridad se enfrentarán a amenazas que serán significativamente influenciadas por las mismas a lo largo de los próximos años. Es por esto que, abordar su estudio, es crucial para adaptar y anticipar las defensas de seguridad.**

De dichas tecnologías disruptivas, la Inteligencia Artificial presenta, actualmente, mayor evolución y crecimiento, las estimaciones valoran que el gasto global en Inteligencia Artificial se estimó en $ 37.5 mil millones en 2019, y se prevé que alcance los $ 97.9 mil millones en 2023.

En este contexto, la Inteligencia Artificial ya ha comenzado a incorporarse en las técnicas de ataque y, en consecuencia, en la defensa. Se espera, por lo tanto, que se convierta a lo largo de los próximos años en uno de los grandes motores del cibercrimen, así como de una defensa exitosa.

Esto se deberá principalmente a la creciente complejidad del manejo de datos; a la escasez de talento en el sector que propicia la necesidad de automatizar procesos a un ritmo más rápido; y a la complejidad operativa, en la actualidad, la proliferación de relaciones entre terceras y cuartas partes (famosos third and fourth parties), así como la hiper-conectividad de estas requieren una fuerte capacidad analítica, así como rapidez en la gestión y respuesta que puede ser provista por sistemas de Inteligencia Artificial.

Desde el punto de vista de las dinámicas ofensivas, destaca la capacidad de la tecnología para mejorar la calidad y ejecución existente en los ataques gracias al aprendizaje automático. Es adaptativa, lo que significa que puede aprender, volverse creativa, y generar ideas en las que los atacantes no necesariamente habrían pensado. Todo ello resulta en crecientes niveles de sofisticación, escalabilidad y rapidez que propiciarán los ataques y operaciones de los criminales favoreciendo actividades relacionadas con el reconocimiento, el acceso inicial y la ejecución. Las aplicaciones en phishing y malware potenciadas por Inteligencia Artificial continúan evolucionando como grandes ámbitos de la utilización a fin de evadir la detección y la eliminación, potenciando con ello la persistencia de los atacantes, así como fortaleciendo las capacidades de evasión. En relación a la escalada de privilegios, la Inteligencia Artificial sería capaz de obtener información y datos disponibles en la red, crear listados de palabras clave en base a la información interceptada, crear contraseñas potenciales y conseguir irrumpir en otros dispositivos; en relación a su capacidad para llevar a cabo movimientos laterales, está tecnología es capaz de recopilar de forma autónoma cuentas y credenciales y calcular la ruta óptima para llegar al objetivo del atacante; finalmente, en su papel para exfiltrar información, la Inteligencia Artificial es capaz de identificar y decidir qué material es relevante en base al contexto, reduciendo los volúmenes de transferencia de datos y dotando de mayor sigilo a las operaciones de robo de datos. Sería capaz además de llevar a cabo estas actividades en períodos de alta actividad para mezclarse con el ruido de la red, sin levantar alertas.

La Inteligencia Artificial en la ofensiva ofrece un amplio abanico de posibilidades, que, si bien solo podemos detallar por la corta extensión de este artículo, nos da una idea del gran potencial que podemos esperar de los ataques venideros

La Inteligencia Artificial en la ofensiva ofrece un amplio abanico de posibilidades, que, si bien solo podemos detallar por la corta extensión de este artículo, nos da una idea del gran potencial que podemos esperar de los ataques venideros.

En relación a la defensa, la Inteligencia Artificial aporta una capacidad única para la Identificación de riesgos. Es posible identificar e incluso predecir el crimen cibernético a través del análisis de big data en las redes sociales y el aprendizaje automático. También ofrece innovación en la protección. Los avances en velocidad y aprendizaje continuos podrían ayudar a aumentar la velocidad de los defensores para automatizar los procesos de razonamiento detrás de la detección de vulnerabilidades y parchear de forma dinámica y automática. En términos de defensa proactiva, dado el potencial para la generación automática de nuevas rutas »

La tecnología de Inteligencia Artificial permite favorecer las prácticas de ataque y defensa, pero también impulsar muchos de los procesos de negocio. Es por esto por lo que se espera que esta tecnología sea incorporada de manera creciente en la toma de decisiones de los mismos »

de red y activos falsos por parte de la Inteligencia Artificial, permitiría una evolución constante del entorno percibido por el atacante. Esto entorpecería y obstaculizaría el ataque. En cuanto a la proyección a futuro, la industria considera la creación de software inteligente que pueda aprender tanto de las redes como de los procesos de una organización, y en el caso de verse comprometida puede restablecer una nueva instancia en un corto período de tiempo. Esta tecnología puede fortalecer la capacidad de un sistema para resistir y tolerar un ataque al facilitar la detección de amenazas y anomalías. Los agentes de Inteligencia Artificial pueden también responder automáticamente para interrumpir y contener ataques a gran velocidad o facilitar la respuesta a través del suministro de información enriquecida a los analistas. Cabe destacar la capacidad de la Inteligencia Artificial para reconocer patrones a partir de grandes cantidades de datos y clasificar información. Esto sugiere su utilidad potencial en los análisis que sustentan la atribución cibernética.

La tecnología de Inteligencia Artificial permite favorecer las prácticas de ataque y defensa, pero también impulsar muchos de los procesos de negocio. Es por esto por lo que se espera que esta tecnología sea incorporada de manera creciente en la toma de decisiones de los mismos. Ha de ser, por tanto, protegida. Y se debe proteger desde una triple perspectiva: datos, algoritmos y resultados. Los datos han de protegerse pues son utilizados para el entrenamiento de la tecnología y para su explotación. Es necesario procurar por el desarrollo de algoritmos seguros y defendibles, además de aplicar medidas de seguridad que los protejan contra la manipulación adversa y las técnicas de interrupción, asegurando los resultados.

El desarrollo de las tecnologías y técnicas de ataque se ve propiciado e impulsado por el negocio lucrativo del cibercrimen. Los grupos criminales operan con grandes inversiones que permiten la evolución de los ataques, técnicas y tecnologías, volviéndose cada vez más organizados y altamente sofisticados. Esta evolución podrá ser gestionada en el corto plazo, evolucionando y madurando las capacidades de la defensa, adoptando innovaciones tecnológicas como la Inteligencia Artificial. Esta tecnología, a diferencia de la Inteligencia Natural, es capaz de tomar decisiones y actuar en milisegundos, procesar grandes cantidades de datos y operar 24x7. Es imprescindible, en consecuencia, formar a expertos en seguridad en Inteligencia Artificial para que puedan explotar el potencial de esta tecnología. No obstante, a medio y largo plazo, si la tendencia de desarrollo de capacidades ofensivas continúa evolucionando de acuerdo con lo expuesto, manteniendo altos niveles de rentabilidad e inversión en desarrollo y suponiendo un coste cada vez mayor para las organizaciones, es de esperar que las capacidades criminales diverjan en gran medida con respecto a los atacantes. Se trata de una amenaza acrecentada por el peligro de un riesgo sistémico debido a la interconectividad e interdependencia de los ecosistemas, antes mencionada.

Esta situación necesitará una respuesta colectiva por parte de la sociedad, el gobierno, las organizaciones y la academia. Solo a través de un enfoque coordinado se podrá cambiar el rumbo de esta amenaza, y comenzar por la coordinación y colaboración en materia de Inteligencia Artificial parece el paso más natural, debido, como se ha mencionado al avance de la investigación, del desarrollo y de la adopción de esta.

Entre otras acciones, la colaboración podría promover la adopción de las capacidades de inteligencia artificial en las tecnologías defensivas; favorecer la comunicación público-privada permitiría compartir proactivamente información acerca de las nuevas técnicas, tácticas y tecnologías influenciadas por la Inteligencia Artificial. También es fundamental trabajar conjuntamente estableciendo prácticas y requisitos de desarrollo seguro y promoviendo su adopción, procurando perseguir la estandarización y adhesión global. Así como fortalecer la gestión de los datos y el cumplimiento de las políticas relacionadas ya que los datos son cada vez más valiosos para los atacantes y las implicaciones de su mal uso son cada vez más graves.

Se requiere sin duda de una respuesta conjunta para hacer frente a una amenaza global. Pues como se citaba al inicio del artículo, ***"lo que es pues de gran trascendencia en la guerra es desbaratar la estrategia del enemigo"***.


thalesgroup.com
THALES
Building a future we can all trust
8.000 millones
de pasajeros se benefician de las
tecnologías de Thales cada año
Síguenos: Thalesgroup
PublicisLMA & Madras Global - ©Getty images

# Cuando la ciberseguridad depende de nosotros

JOSÉ MARÍA HERNÁNDEZ FEU

Information Security Manager
**Johnson & Johnson**

Contacta:

www.linkedin.com/in/jmhernandezfeu

**Ahora, más que nunca, la ciberseguridad se ha convertido en un tema candente y de actualidad. Todos somos conocedores de que existen riesgos cibernéticos que nos pueden afectar de alguna forma. Pero, ¿realmente le estamos prestando la atención que se merece? ¿Hacemos nuestros deberes para evitar lo que puede desencadenar un gran perjuicio personal?**

Comienzo a escribir estas líneas mientras viajo en el vagón de un tren (sería similar en la cabina de un avión), donde la distancia con nuestros compañeros de viaje es cada vez menor. Esta corta distancia me permite leer sin dificultad el correo electrónico de la persona que está a mi lado, que tiene su portátil abierto, pero también el de quien viaja en el asiento de delante, en diagonal con respecto a mí. Ahora sé cómo se llaman, para qué empresa trabajan, a qué se dedican, cuáles son los correos de sus jefes e, incluso, los nombres de sus parejas y algún que otro teléfono móvil. Así comienza mi aventura por la ingeniería social, que usada malintencionadamente permitiría entablar conversación con esos individuos y, quién sabe, si finalmente captar más información personal o las credenciales para acceder a su cuenta de empresa.

El de al lado recibe una llamada de alguien que le ofrece comprar un cachivache en una página web. Le entra el ansia de conseguirlo cuanto antes y se pone a pedir dicho cachivache en línea. Como no está registrado, introduce sus datos personales para darse de alta y acepta (sin leer) el aviso legal y la política de privacidad. Es lo fácil, pero no es lo correcto si queremos evitar sorpresas. Ahí no queda todo. Lo mejor viene cuando realiza el pago, para lo cual pone encima de la mesita del tren su tarjeta de crédito, primero por un lado y después por el otro. Sí, el banco le obliga a usar un segundo factor de autenticación, pidiéndole que inserte una contraseña por el teléfono móvil. ¡Es el nombre de su pareja! Ya lo tengo todo. De ahí a la estafa, la extorsión y el quebradero de cabeza solo hay un paso. ¿Es muy complicado? En absoluto.

Estos señores han confiado equivocadamente en la aparente bondad de las personas que les rodean y en su fingido despiste. Ojalá fueran reales esa bondad y ese despiste, pero la realidad es otra. Una parte importante de la población (algunos por ignorancia, la mayoría por dejadez) no tiene en cuenta las serias consecuencias que pueden acarrear sus despreocupados comportamientos con la tecnología. Sin embargo, aunque algunas prácticas son farragosas y más propias de gurús hipertecnológicos o de profesionales

del sector, muchas de ellas son sencillísimas y pueden prevenir y evitar algún que otro susto. Veamos algunas. He elegido las diez que me han parecido más básicas y fáciles de poner en práctica, pero no son las únicas:

1. **Usa contraseñas complejas y largas.** No es difícil en absoluto acordarse de la serie de caracteres "MiPuebloEstáA13kmDeVillabotijo DeAbajo", que contiene atributos de todo tipo, y nada más y nada menos que una longitud de 38 caracteres. Harían falta cientos, si no miles, de años para que una máquina pudiera adivinar esta contraseña por un ataque de fuerza bruta, es decir, por prueba y error de los millones de combinaciones posibles.

2. **No compartas tu contraseña**. No seas ingenuo compartiéndola o la acabará conociendo todo tu entorno y toda la fortaleza que le has asignado al establecer unos criterios fuertes de complejidad y longitud no te habrá valido para nada.

3. **No uses la misma contraseña en diferentes sitios**. No es un capricho. La razón detrás de esto es que si el sistema al que accedes se viera comprometido y las contraseñas llegaran a poderse usar malintencionadamente por un atacante, éste tendría acceso, no sólo al sistema atacado, sino a todos aquéllos donde tuvieras credenciales comunes.

4. **Tapa tu PIN cuando lo insertes en comercios**. Desconfía de la persona que está en la caja, pero también de otros clientes que tengas a tu alrededor. No pasa nada por tapar con la mano el visor y ser discreto. Lo debemos hacer todos por costumbre.

5. **Activa el doble factor de autenticación**. En aquellos sitios donde accedas a información sensible y te dé esta opción, actívala. Normalmente se trata de un código adicional que te enviarán por SMS al teléfono móvil, pero puede ser una aplicación en la que se muestra ese código o en la que activas temporalmente alguna opción, un rasgo biométrico o un certificado digital. Así, si alguien llegara a conocer tu contraseña e hiciera mal uso de ella, te llegaría a ti la petición para permitir el acceso con el segundo factor.

6. **Usa antivirus y mantenlo actualizado.** Los hay buenos y baratos, incluso gratuitos. Es recomendable tener uno que detecte lo que técnicamente se conoce como Troyano, Gusano, Spyware, etc. Configúralo para que se actualice regularmente y detecte los nuevos virus que van apareciendo.

7. **Protege tus datos personales.** Introduce el mínimo imprescindible. Si no hace falta un correo electrónico o un número de teléfono móvil, no lo des. Y si quieres saber para qué se recogen tus datos y qué van a hacer con ellos, echa un ojo a la política de privacidad, ese largo documento que seguramente marcas como que has leído, aunque no lo hayas hecho ni por asomo.

8. **Estate atento a la ingeniería social.** Se trata de un ataque mediante el engaño a una persona haciéndose pasar por quien no es. Detrás de las aparentemente buenas personas a las que no conoces, y por muy legítima que sea esa apariencia, pueden esconderse intenciones maliciosas. Si te llama o escribe alguien desconocido, no des ningún dato tuyo ni de nadie que conozcas. Escondido en el anonimato de una voz agradable al teléfono, puede haber alguien captando información tuya, que luego usarán posiblemente para engañar a su vez a alguien cercano a ti.

9. **No caigas en el *phishing.*** Ten cuidado con los correos de alguien que no esperas y que llevan enlaces o documentos adjuntos. Podrían estar instalándote algo o abriendo una página web casi igual a la real y tú posiblemente no te darás ni cuenta. Algunas pistas para detectar rápidamente el phishing son: dirección del remitente desconocida o incorrecta, faltas de ortografía, mensaje dirigido a un destinatario genérico (o sea, no dirigido a ti con tu nombre), sentido de urgencia en la respuesta, dinero u otros bienes demasiado fáciles de conseguir, enlace que va a un sitio desconocido (se ve pasando el ratón por encima sin hacer clic) o que te dirige de un país que no te da confianza, etc.

10. **Realiza copias de seguridad.** Haz periódicamente una copia de seguridad de los datos importantes que tengas y que no te gustaría perder bajo ningún concepto. En caso de que le ocurra algo a tu dispositivo, cualquiera que éste sea, podrás recuperar esa información. Imagina que se te rompe ese dispositivo donde tienes la información que más aprecias, se te pierde o incluso que te instalan un Ransomware y la información de tu ordenador resulta cifrada y te piden un rescate por descifrártelo. En estos casos, recuperar la información a partir de la última copia de seguridad sería un mal menor.

Todo esto te puede parecer una exageración o incluso una excentricidad. Pues bien, que sepas que este artículo se basa en diferentes hechos reales que he presenciado y que todos estamos expuestos a los riesgos aquí descritos, riesgos que están ahí y que nos pueden suponer un quebradero de cabeza, pero que tienen fácil solución si nos esforzamos un mínimo por evitarlos.

Dejo de lado para otro momento otros riesgos de ciberseguridad que afectan mayoritariamente a las empresas y no a las personas, como, por ejemplo, los ataques a las infraestructuras críticas o los riesgos operacionales en la fabricación, almacenamiento y distribución de bienes y, en general, de toda la cadena de suministro.

A partir de ahora, fíjate a tu alrededor cuando viajes en tren o en avión. Te darás cuenta de lo poco precavidas que son algunas personas y de los riesgos a los que están expuestas.

# Cómo convertir la práctica de ciberseguridad en un socio del negocio en tiempos de transformación

GABRIEL MOLINÉ
CISO
Leroy Merlin
Contacta:
linkedin.com/in/gmolinesosa

CÉSAR COLADO
CIO
Leroy Merlin
Contacta:
linkedin.com/in/cesarcolado

**¿Cuánto inviertes en ciberseguridad? Seguramente, no suficiente. Probablemente estés en el sector de banca, en telco, en la administración… Nosotros estamos en la industria del retail, venta minorista. Probablemente los retos a los que nos estamos enfrentando no sean tan diferentes entre nuestras industrias y nuestro enfoque te pueda aportar alguna idea.**

No cabe duda de que nos encontramos en un momento de transformación digital y en el caso de Leroy Merlin, nos hemos centrado en desarrollar nuestras capacidades logísticas para atender cada día mejor a nuestros clientes. Los clientes demandan una experiencia coherente a través de los canales físicos y también los canales digitales. Esperan poder ver el catálogo en la web, llamar por teléfono o por videoconferencia para resolver algunas dudas, pasarse por una de nuestras tiendas para tocar el producto y tomar una decisión de cuándo le viene mejor y a través de qué canal realizarla compra y, por supuesto, compartir con sus conocidos lo que ha hecho o va a hacer con ese nuevo taladro que ha comprado.

Todo el esfuerzo que estamos poniendo en nuestra transformación y aprendizaje para proporcionar una mejor experiencia a nuestros clientes genera rápidamente una huella digital enorme. En una multinacional, se desarrollan servicios de forma distribuida y se utilizan servicios desarrollados en el grupo que se ejecutan en diferentes partes del mundo. Además, como nos ha pasado a todos, el COVID ha traído el trabajo híbrido para quedarse, el 60% de la gente con la que trabajamos está en remoto y el 18% de ellos no volverán nunca a la oficina (Attack Surface Expansion by Pete Shoard - Gartner). A esto sumemos el hecho de que el *cloud* también es real y nuestros despliegues de todo lo nuevo los hacemos en el *cloud* y la mayor parte de nuestro *legacy*,

sigue *on prem,* junto con software desarrollado *in-house*, utilización de librerías open source, aplicaciones SaaS y sistemas IoT en nuestras tiendas y almacenes no simplifican la ecuación.

Nadie discute que la ciberseguridad es clave porque a todos nos aterra tener problemas. Pero lo cierto es que el presupuesto no es infinito y la exposición es cada vez mayor. ¿Te suena?

¿Cómo priorizamos? ¿qué protegemos? ¿cuánto? ¿cómo? Si las preguntas son las buenas, tenemos que priorizar y eso significa renunciar. Debemos identificar los riesgos asociados a las tecnologías utilizadas, datos personales y requerimientos regulatorios. Y todo ello, por supuesto, manteniendo. la experiencia porque dos factores de autenticación pueden suponer una reducción en la tasa de conversión, con la presión que ello genera para nuestro negocio. Se trata siempre de encontrar un equilibrio, pero es necesario poner cierto orden y método.

Nosotros utilizamos el concepto de **ciber-exposición,** como nuestra torre de control en la cual ponderamos conceptos como la obsolescencia tecnológica, vulnerabilidades conocidas, criticidad de los servicios implicados, tipos de datos personales, el histórico de incidencias o el modelo de exposición del servicio, permitiéndonos clasificar y priorizar el riesgo tecnológico asociado a los procesos de negocio y con ello establecer el grado, tipo y el nivel de controles de seguridad que deberán ser aplicados en la implantación de los sistemas o servicios de información de nuestra compañía.

## Ciber-exposición

### Principales elementos

Para el cálculo de la ciber-exposición tenemos en cuenta los siguientes aspectos:

1. **Naturaleza del activo:** se realiza un BIA (Business Impact Analysis) además de valorar el riesgo en función de la naturaleza del activo, del tipo de datos que gestiona, del histórico de incidencias de seguridad asociadas al activo, de los resultados de las auditorías y revisiones realizadas.

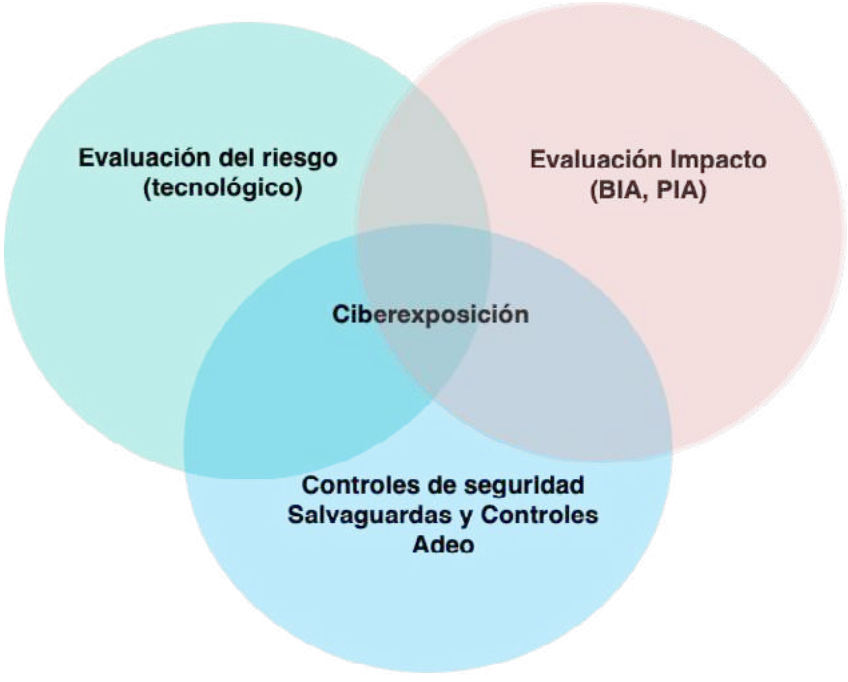
2. **Gestión de vulnerabilidades:** en este apartado nos basamos en la priorización para optimizar el despliegue de mejoras o actualizaciones que el mayor número de riesgos en base a los criterios de tipos de servicios que presta la solución y las tecnologías que la soportan.

3. **Información de vigilancia digital** como las credenciales comprometidas, monitorización de nuevas amenazas o vectores de ataque, importancia relativa para los ciberdelincuentes (suplantaciones de identidad o phishing detectados)

4. **Riesgos asociados a las personas** que usan esos activos tecnológicos: el nivel de formación y concienciación en ciberseguridad de los usuarios de los activos tecnológicos es muy importante a la hora de determinar el riesgo. En ese sentido se ha de tener muy en cuenta los VAP (Very Attack Persons) que son aquellas personas de la organización que o bien por su nivel jerárquico (por ejemplo son los miembros del Comité de Dirección) o bien por su exposición pública (por ejemplo personas que participan en eventos o realizan tareas clave) son más susceptibles de sufrir ciberataques.

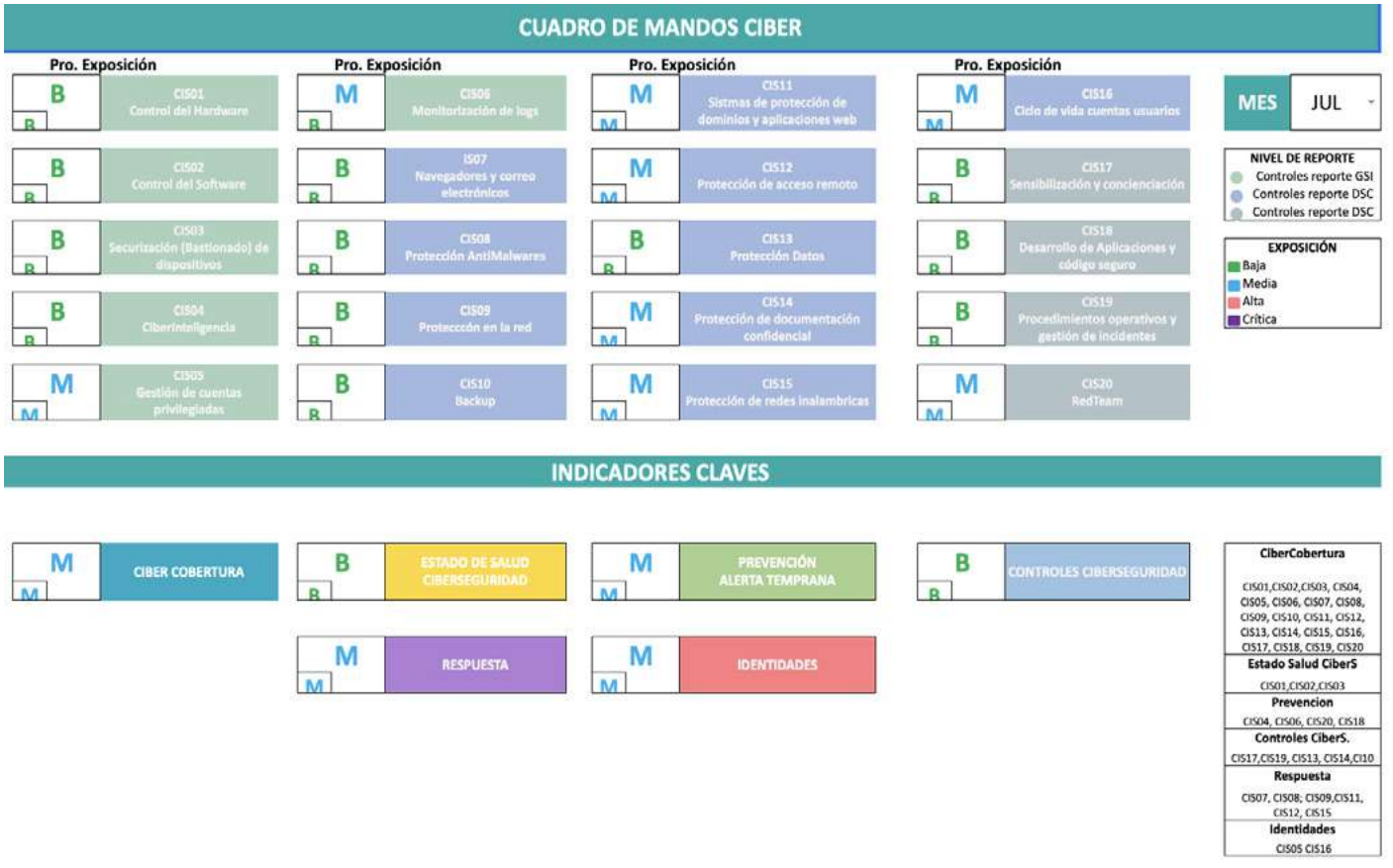
5. **Riesgos asociados a los proveedores y socios** que colaboran en el soporte y desarrollo de esos activos tecnológicos. *(Figura 1)*

Figura 1. Parámetros de prioridad de vulnerabilidades




Este proceso nos permite tener una **visión clara y objetiva** de los activos tecnológicos que presentan un mayor riesgo y nos facilitan la tarea a la hora de determinar los controles y las necesidades de inversión en ciberseguridad. Nos permite alinearnos con el negocio y explicar claramente las prioridades para la práctica y cuánto más se puede hacer con cada incremento en nuestro esfuerzo. »

Figura 2.




## Controles o ciber-cobertura

Si bien la ciber-exposición nos permite identificar los principales riesgos de ciberseguridad y una estrategia para su mitigación, el modelo no estaría completo sin un inventario de controles proporcionales, efectivos y que puedan ser implantados en nuestro ecosistema. Para ello, hemos definido un conjunto de controles basados en la estrategia CIS en la cual, desde el diseño servicio, definimos un conjunto mínimo de controles obligatorios para todas las aplicaciones y servicios involucrados en el proceso, como definición de roles acceso y perfiles, medios de autenticación robusta, controles de software maliciosos, almacenamiento y gestión de logs, y diferenciación de entornos, entre otros. Además, en función de los criterios de ciberexposición implantamos controles específicos como análisis de código, test de penetración, controles DLP, IAM o MFA. *(Figura 2)*

## Conclusiones

En el mundo del comercio minorista basado en el cambio continuo de la oferta de productos y donde los canales digitales se entrecruzan con los canales físicos para interactuar con nuestros clientes, es fundamental contar con visibilidad continua de los riesgos de ciberseguridad con el objeto de transmitir una percepción de seguridad a nuestros clientes y garantizar la aplicación de controles proporcionales, mitigantes de las necesidades regulatorias y garantía de la continuidad de los servicios tecnológicos, por ello es fundamental el diseño de una estrategia de ciberseguridad relacionada con la organización, las capacidades y el modelo de servicio. Pudiendo mediante la presentación y la discusión con el negocio de la ciber-exposición, priorizar y decidir sobre las acciones para garantizar la cobertura que como compañía consideremos aceptable o suficiente.

Medallia

# La Plataforma #1 de Experiencias

# ESG y Ciberseguridad: *la pareja más moderna del presente y del futuro*

MARTA FERNÁNDEZ NÚÑEZ

Delegada de Protección de Datos
**Grupo BNP Paribas en España**

**Contacta:**

https://www.linkedin.com/in/marta-fern%C3%A1ndez-n%C3%BA%C3%B1ez-ab84321b9/

**Desde hace más de diez años el Grupo BNP Paribas ha puesto foco en materia de sostenibilidad y en particular, en relación a los indicadores denominados ESG, cuyo acrónimo anglosajón describe los tres pilares sobre los que se asienta: (Environmental, Social, Governance). La ciberseguridad y sus parámetros se han incluido por la Value Reporting Foundation, en agosto de 2022, en el pilar de la Gobernanza. Además, la entrada en aplicación del Reglamento Europeo de Protección de Datos el 25 de mayo de 2018 obligó a las empresas a reforzar la seguridad informática y la securización de los datos de carácter personal que tratan en sus negocios. Nuevas amenazas aparecen y así, el robo de datos de carácter personal por parte de las nuevas formas de ciberdelincuencia han reforzado de forma significativa los sistemas informáticos, con herramientas que blindan a las empresas frente al robo de lo que se ha denominado, en referencia a los datos de carácter personal, "el petróleo del siglo XXI". En este escenario; ¿En qué lugar queda la ciberseguridad respecto a los indicadores ESG? ¿Cuáles son los retos actuales que tienen que afrontar las empresas para ser ciberseguras a la vez que sostenibles?**

Históricamente la protección de datos y la ciberseguridad no han sido considerados conceptos ESG, pero en los últimos tiempos hay una tendencia a incluir la protección de datos y la ciberseguridad en el reporte y en la clasificación de las empresas cuando las grandes agencias de calificación financiera se refieren a indicadores de sostenibilidad. Los profesionales que se dedican a la protección de datos y a la ciberseguridad trabajan con los equipos que se dedican a los temas de sostenibilidad para demostrar cómo las organizaciones abordan los retos de privacidad, creando un impacto social positivo.

La ciberseguridad cobra una importancia crucial en las empresas, pues no es únicamente un concepto que incluye la defensa de los datos estructurados sino también a los datos no estructurados, frente a amenazas de la ciberdelincuencia.

Un fallo en la ciberseguridad de una empresa puede comprometer seriamente su continuidad, siendo el riesgo financiero el más inmediato, por lo que los Consejos de Administración integran cada vez más la ciberseguridad en la gobernanza de las compañías. Las empresas

son conscientes de que si sus terceros no están protegidos, y no garantizan dicha protección en materia de ciberseguridad, pueden poner en riesgo a la propia empresa.

Las empresas que apuestan por la sostenibilidad en sus negocios son generadoras de confianza en inversores que buscan la seguridad no sólo de sus activos, sino en materiade seguridad informática y en cómo dichas empresas se defienden frente a ataques devastadores de ciberdelincuentes.

Los indicadores ESG ¿Cómo intervienen en el proceso de inversión? Ahora mismo se incluyen en los procesos de diligencia debida y cuando se integran en el negocio, mejoran el portfolio de las compañías al incrementar las inversiones en negocios inclusivos y sostenibles.

Tradicionalmente la privacidad ha sido encasillada en el apartado "Social" de la ESG, sin embargo el panorama está cambiando ya que la privacidad y la ciberseguridad, taly cómo está estructurado el sistema en la compañía, forman parte ahora del pilar "Gobernanza", pues incluyen elementos de un programa de privacidad.

Por esta razón los profesionales de la privacidad, de la seguridad informática y de la ciberseguridad han tenido que trabajar conjuntamente en equipo y comprender a fondo este nuevo marco de esta alianza y cómo las métricas de privacidad y protección de datos pueden ser utilizadas para abordar la metodología del scoring en ESG. Dentro de este ámbito, la privacidad se convierte en un imperativo de gobernanza para el negocio que va más allá del cumplimiento normativo y que aparece como una parte esencial de la confianza que deposita el cliente en la empresa.

Como resultado de lo anterior, el perfil de la privacidad y de la protección de datos en la empresa aparece como un indicador estratégico de la empresa, que la coloca en los primeros puestos si cuenta con las mejores políticas de ciberseguridad y de privacidad.

## En el Grupo BNP Paribas seguimos avanzando: hacia un negocio cada vez más sostenible, inclusivo y seguro para nuestros clientes

El pasado 1 de agosto de 2022 entraban en aplicación los indicadores ESG de la Value Reporting Foundation (Normas SASB- consolidadas en la Fundación NIIF), creando la primera Junta Internacional de Normas de Sostenibilidad (ISSB). En dichas normas se incluyen por primera vez indicadores relacionados con la seguridad de la información y de datos de carácter personal, subrayando la importancia en dichos indicadores, de que las empresas deben contar con unos procedimientos adecuados en materia de gestión de los datos estructurados y no estructurados cuando se diseñan políticas de ciberseguridad y de seguridad informática.

Son muchos los elementos que los indicadores van a tener en cuenta a la hora de hacer el rating de la empresa: el volumen de brechas de datos de carácter personal y de seguridad, no establecer procedimientos robustos en ciberseguridad y contar con un alto volumen de pérdidas en el negocio por no garantizar sistemas y entorno IT seguros, ser sancionado por reguladores de protección de datos y otros reguladores por no cumplir con la regulación nacional y/o de la Unión Europea en materia de ciberseguridad, no contar con sistemas que permitan al cliente controlar cómo quiere que se traten sus datos de carácter personal, básicamente mediante su consentimiento expreso, son sólo algunos ejemplos.

Dentro de estos indicadores más recientes ESG (bajo el marco del GRI 418) y a la hora de realizar el informe ESG sobre los datos personales de los clientes, se establece que para proteger la privacidad de los clientes, se espera que una organización limite su recopilación de datos personales, recopile datos por medios legales y sea transparente sobre cómo se recopilan, utilizan y garantizan la securización de los datos.

También se espera que la organización no revele o utilice información personal del cliente para fines distintos de los convenidos, y que comunique directamente a los clientes cualquier cambio en las políticas o medidas de protección de datos.

Por esta razón se incluyen como elementos fundamentales para ser evaluados por dichos indicadores, las denuncias fundamentadas relativas a violaciones de los datos de carácter personal de los clientes y las pérdidas de datos de carácter personal del cliente.

Además se comunicará el total de reclamaciones fundamentadas recibidas en relación con violaciones de los datos de carácter personal del cliente, clasificadas en: reclamaciones recibidas de terceros y justificadas por la organización y reclamaciones presentadas en organismos reguladores, el número total de fugas de datos de carácter personal y robos o pérdidas de datos de carácter personal de clientes. Si la organización no ha identificado ninguna reclamación justificada, basta con una breve exposición de este hecho.

Al compilar la información especificada en el indicador 418-1, la organización deberá indicar si un número considerable de esas infracciones se refieren a acontecimientos ocurridos en años anteriores.

Como conclusión, no podemos dejar de subrayar la importancia de los indicadores ESG en las empresas, pues los mismos obligan a avanzar y a invertir en cambios inclusivos y sostenibles sobre todo en tecnología, en especial en ciberseguridad, por lo que una empresa será puntera cuando tenga estos conceptos claramente definidos e interiorizados en la gobernanza de la compañía. En el Grupo BNP Paribas así es desde hace más de diez años y en ello seguimos avanzando: hacia un negocio cada vez más sostenible, inclusivo y seguro para nuestros clientes.

CAROLINA GONZÁLEZ

National Leader de Claire Joster Executive
**Eurofirms Group**

**Contacta:**

linkedin.com/in/carolinagonzalezpoza


# *La creciente demanda de perfiles de ciberseguridad en el convulso mercado tecnológico*

**Si la demanda de perfiles tecnológicos aumenta día a día, todavía podemos observar un crecimiento más elevado en los perfiles enfocados al ámbito de la ciberseguridad. Con la irrupción de la pandemia y la normalización del teletrabajo, las brechas de seguridad en las compañías se disparan y la necesidad de crear equipos sólidos que frenen estos ataques se incrementa, pero la realidad es que la diferencia entre la oferta y la demanda de este tipo de profesionales se acrecienta cada día.**

**Desde Eurofirms Group hemos realizado un estudio para intentar arrojar luz sobre la realidad del mercado tecnológico: convulso, cambiante y claramente dominado por los candidatos. ¿Qué buscan y valoran estos perfiles? ¿Existe realmente inflación en el sector? ¿Cuáles son las áreas con más potencial de crecimiento?**

Llevamos ya años viendo cómo la demanda de los profesionales del ámbito tecnológico crece a un ritmo mucho más alto que el de la oferta de candidatos y cómo nuestros modelos educativos no nos permiten abarcar la realidad que el mercado necesita.

Con la irrupción de la pandemia fueron muchas las empresas que tuvieron que adaptar su tecnología para permitir que sus empleados pudieran trabajar desde sus casas. Ahora, el teletrabajo es una realidad con la que convivimos y que ha creado nuevas oportunidades y retos para las compañías. Uno de estos retos es la creciente demanda de perfiles de ciberseguridad.

## Perfiles más demandados en ciberseguridad

Entre las posiciones más demandadas cabe destacar la figura del CISO (Chief Information Security Officer), cada vez más estratégica para las compañías. El CISO es el máximo responsable en lo que a seguridad se refiere y es la persona encargada de definir la estrategia global, crear los equipos necesarios o seleccionar a los partners adecuados. Un proceso de selección con estándares de calidad muy altos es clave en la búsqueda de este perfil para cualquier organización que quiera evitar ser vulnerable ante posibles ataques. Las competencias que adquieren una mayor relevancia en esta posición son visión estratégica, capacidad de adaptación, poseer un perfil resolutivo y una fuerte orientación a la calidad, ya que un error en esta área puede ser absolutamente crítico para la compañía.

Desde hace algunos meses estamos percibiendo una tendencia importante a internalizar los departamentos de ciberseguridad que, históricamente tendían a externalizarse con equipos externos. Para reforzar estas áreas las empresas necesitan perfiles más técnicos que puedan implementar de manera correcta las directrices en materia de seguridad. Entre los perfiles más demandados están analista de Ciberseguridad, ingeniero SOC y Pentester o hacker ético. Y cada vez son más las compañías que piden certificaciones específicas y herramientas concretas. A la hora de seleccionar a estos candidatos se debe tener muy en cuenta la competencia de la orientación al detalle ya que en numerosas ocasiones se enfrentan a retos muy complejos y en los que el margen de error debe ser mínimo.

## Inflación en los salarios del sector

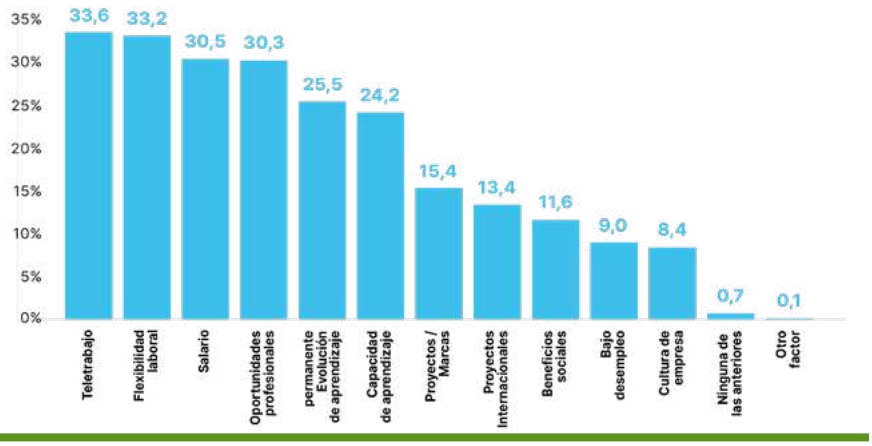
Pero el crecimiento en la demanda de estos perfiles no ha ido acompañado de un aumento homogéneo en la oferta de candidatos. Uno de los efectos más inmediatos cuando la demanda de una disciplina se dispara es la inflación y no iba a ser menos con la ciberseguridad. En el estudio que hemos realizado se pone de manifiesto que estos candidatos tienen un salario superior a la media en todas las comunidades autónomas de España. Un perfil junior, con experiencia de uno o dos años puede tener un salario bruto anual de más de 30.000 euros. Para profesionales con algo más de experiencia, el salario pude estar en torno a los 50.000 euros brutos anuales.

Si hablamos de la figura del CISO la franja salarial varía mucho en función del tipo de perfil y de compañía, pero puede partir en torno a los 80.000 euros de salario bruto

anual en algunas empresas de tamaño medio y llegar a alcanzar cifras superiores a los 200.000 euros en función del sector, el tamaño de la compañía y la responsabilidad.

En el propio estudio hemos preguntado a los profesionales si consideran que existe una inflación en el mercado tecnológico y su respuesta es muy clara: el 45% de los encuestados afirman ser conscientes de que la realidad es que existe una sobrevaloración salarial para este tipo de perfiles. Esta tendencia inflacionista que llevamos experimentando desde hace años parece acentuarse en algunas categorías y una de las más fuertes en este sentido es la de la ciberseguridad.

Figura 1: Aspectos mejor valorados




Nuestro estudio demuestra que se trata de un sector muy nuevo y en consolidación. El 45% de los profesionales encuestados tiene menos de 5 años de experiencia y tan solo el 32,4% posee más de 10 años de trayectoria en este tipo de posiciones. Un dato que por sí solo nos dice bastante, pero que, unido a la alta rotación, -ya que el 64% de los encuestados ha trabajado entre 2 y 5 empresas-, nos hace darnos cuenta de que los paradigmas del mercado de empleo tradicionales no sirven para abordar a colectivo de perfiles.

Si nos referimos el ámbito de la ciberseguridad, el estudio de Eurofirms concluye que, a pesar de ser una de las áreas en las que tenemos menos profesionales con experiencia, es la disciplina con mayor potencial de crecimiento. El 44% de los encuestados considera que es la que más futuro tiene, superando incluso a la inteligencia artificial o a la robótica.

Por tanto, cuando tengamos que invertir en formación, sin duda la ciberseguridad es una apuesta al alza. Como hemos comentado y tal y como nuestro estudio confirma, el sistema educativo actual no cubre la demanda de estos perfiles. Uno de los datos que observamos es que solo el 33,1% de los encuestados han llegado a su posición a través de una formación reglada específica del área. El 20,4% ha evolucionado desde otras áreas de conocimiento y el 16,4% ha llegado a su puesto actual a través de autoaprendizaje.

Si el salario y la formación continua son claves en una propuesta de valor atractiva para estos profesionales, no son suficientes para ser competitivo en un mercado tan convulso como el tecnológico. En las encuestas realizadas para el estudio les hemos preguntado por lo que más valoran y lo que hace atractivo el sector para ellos.

## Aspectos más valorados por los profesionales del sector

Las respuestas que nos han dado nos permiten sacar conclusiones muy interesantes. Entre los aspectos más valorados están el teletrabajo, con un 33,6% y la flexibilidad laboral con un 33,2%. En tercer lugar, situarían el salario, con 30,5%. De hecho, 6 de cada 10 encuestados afirma estar dispuesto a renunciar a una parte salarial por tener más tiempo libre. La sociedad evoluciona, los modelos de trabajo también y las necesidades y prioridades de estos profesionales cambian con esta evolución. Como empresa debemos ser atractivos para estos perfiles, entender sus inquietudes y realizar una propuesta de valor siempre coherente con nuestra filosofía, pero lo más completa posible en todos los ámbitos. *(Figura 1)*

## El reto de la incorporación del talento femenino

Pero si hablamos del reto de la selección y fidelización de estos perfiles, no podemos olvidarnos del doble reto que vive el sector y es el de la incorporación de la mujer en estas posiciones. Cuando hemos preguntado por los aspectos a mejorar dentro del sector, el 60% de los encuestados nos dicen que el principal es la inclusión de la mujer en el sector tecnológico.

Dentro de las carreras de ámbito STEM tenemos un gran déficit de mujeres. Si bien el 55,3% de las matriculaciones universitarias son de mujeres, en el caso de disciplinas más técnicas como matemáticas, ciencias o ingenierías, la cifra cae hasta el 35%.

En el estudio realizado por Eurofirms podemos ver, además, el detalle de mujeres en cada disciplina. De las 21 categorías analizadas solo existe un mayor porcentaje de mujeres que de hombres en marketing digital, bases de datos, producto, diseño y desarrollo de negocio. A medida que vamos abordando disciplinas mucho más técnicas el porcentaje de mujeres va cayendo, y el de la ciberseguridad es el ámbito con una mayor caída. La diferencia entre hombres y mujeres trabajando en áreas de ciberseguridad es de 6 puntos.

La realidad es que el mercado tecnológico evoluciona cada día a un ritmo frenético y la clave para garantizar el éxito de demandas tan crecientes como la de la ciberseguridad es estar muy cerca de los candidatos, entender sus necesidades, escucharlos y crear propuestas de valor globales que sean atractivas para ellos.


# *Ciberseguridad:* La otra cara de la digitalización

EDDY THÉSÉE

Vicepresidente de Ciberseguridad

**Alstom**

Contacta:

linkedin.com/in/eddythesee

**Para gestionar un sistema de movilidad seguro y sostenible en el momento actual, es fundamental contar con una estrategia de ciberseguridad eficaz en el sector ferroviario, cada vez más digitalizado.**

El ferrocarril ha experimentado una gran transformación en la última década. Gracias a la tecnología moderna, los trenes ofrecen mayor capacidad, velocidad y comodidad, se adaptan a su entorno, se comunican entre sí e incluso predicen cuándo será necesario el mantenimiento. Pero, igualmente, cuanto más se conectan los trenes en los entornos digitales, más vulnerables son a los ciberataques.

Por eso la ciberseguridad es clave. Los sistemas actuales necesitan un enfoque moderno para garantizar la seguridad de la información y de las infraestructuras, tanto embarcadas como en vía. En el ferrocarril encontramos tres niveles de digitalización, cada uno de ellos con sus propios retos en materia de ciberseguridad.

En primer lugar, nos encontramos con la señalización, los sistemas de gestión y control del tráfico, diseñados para regular el tráfico y garantizar la seguridad de las operaciones ferroviarias. Las comunicaciones electrónicas y las tecnologías en la nube son, por su parte, cada vez más importantes a la hora de mejorar la eficiencia de la operación, su fiabilidad y puntualidad. Para ello, se necesitan conexiones seguras y sistemas avanzados de protección de datos. Y, por último, nos encontramos con la parte corporativa del negocio, que depende en gran medida de que los clientes interactúen de forma segura con los servidores centrales.

La digitalización ofrece numerosos beneficios en estos tres niveles, y su interdependencia entre sí es fundamental para garantizar su correcto funcionamiento. Ninguna de ellas opera de forma independiente, ni su estrategia cibernética puede funcionar de forma aislada.

Como en otros sectores, la automatización representa una oportunidad para gestionar la red ferroviaria de forma segura y eficiente, siendo también un ejemplo de cómo una operación cada vez más digitalizada tiene implicaciones significativas en ciberseguridad.

Las innovadoras soluciones de señalización de Alstom están revolucionando las comunicaciones ferroviarias, reduciendo la infraestructura en vía e incorporando cada vez más "inteligencia" y funcionalidad al material rodante. Los equipos que permanecen en la infraestructura también son tecnológicamente más avanzados.

La digitalización también está impulsando un mantenimiento cada vez más predictivo, permitiendo que el software identifique los equipos defectuosos antes de que éstos fallen. El mantenimiento así es más eficiente, tanto a nivel de personal dedicado como de tiempo de inmovilización de los trenes.

Todas estas innovaciones deben ir acompañadas de estrategias de ciberseguridad que protejan los datos, el software, la conectividad y el hardware que los procesa y gestiona. Más digitalización significa más componentes digitales e interconexiones entre sistemas, lo que conlleva más áreas expuestas.

## Una infraestructura crítica

La clasificación del ferrocarril como "infraestructura crítica" ha acelerado la adopción de soluciones de ciberseguridad estandarizadas. Los nuevos protocolos y otras iniciativas normativas están empujando al sector a ser aún más ciberseguro. En paralelo, los operadores tienen que anticiparse a los ataques, por lo que solicitan una supervisión y alerta periódica de las vulnerabilidades de sus productos y sistemas.

Para responder a esta creciente demanda, Alstom está ampliando rápidamente su experiencia en ciberseguridad, con más de 200 expertos en ciberseguridad que trabajan en 110 proyectos. Una red de expertos globales y locales dan respuesta a las necesidades en materia de ciberseguridad de los clientes en todo el mundo

> La ciberseguridad para una movilidad segura requiere que los sistemas y activos, tanto nuevos como heredados, se incluyan en una estrategia integral de ciberseguridad

Cada nuevo vehículo ferroviario que fabricamos ya incluye el control de seguridad requerido por las especificaciones del cliente. La cuestión ahora se traslada a la base instalada: todo el material rodante, la infraestructura y los sistemas de señalización entregados antes de que la ciberseguridad entrara en nuestra "agenda" diaria. Mejorar la seguridad de las flotas, la señalización y las infraestructuras existentes es un verdadero reto en el que los clientes tendrán que decidir qué nivel de protección quieren alcanzar para sus infraestructuras críticas.

Para mantenerse a la vanguardia, las medidas de protección deben evolucionar constantemente, con la misma rapidez con la que lo hacen las nuevas amenazas. Alstom colabora con diferentes socios, como Airbus o Cylus, para establecer las mejores prácticas y las normas de referencia. Situar la ciberseguridad en el centro de la cultura de excelencia de una empresa ferroviaria implica impulsar la formación y la cultura de ciberseguridad, alineando los equipos de ciberseguridad y de operaciones ferroviarias.

Además de liderar la definición y el despliegue de normas y reglamentos, es necesario abordar todo el ciclo de vida de la ciberseguridad con un enfoque global. En Alstom estamos comprometidos en este objetivo, y así se manifiesta en las numerosas acreditaciones con las que contamos: ISO 27001 para la seguridad de la información, IEC 62443 para los sistemas de automatización y control industrial, así como la normativa específica del sector ferroviario, CENELEC TS50701, basada en gran parte en IEC 62443. »


Resulta clave la adopción de soluciones estandarizadas de ciberseguridad centradas en el ferrocarril, que protejan los datos, el software, la conectividad y el hardware que procesa y gestiona los sistemas ferroviarios

## » La ciberseguridad, en el centro del negocio

En los próximos años habrá una demanda de soluciones digitales que permitirán a los operadores ferroviarios hacer más con menos. Hoy, los operadores saben que necesitan proteger sus sistemas y buscan incansablemente soluciones que puedan integrarse de forma holística en ecosistemas complejos.

Con más de 70 años de experiencia en proyectos complejos en el sector ferroviario y con más de 110 proyectos de ciberseguridad desarrollados en todo el mundo, el diseño de todos los nuevos proyectos de Alstom da prioridad a la ciberseguridad, junto con las consideraciones tradicionales de ingeniería y seguridad.

Todo el desarrollo de productos de Alstom se lleva a cabo con la premisa "diseño seguro", comenzando con un análisis de riesgos exhaustivo y una arquitectura centrada en la integración de la ciberseguridad.

Esto también se aplica a los proveedores. A través del "programa de gestión de proveedores" de Alstom, se evalúa la capacidad de cada proveedor en materia de ciberseguridad.

Todos los sistemas desarrollados, desplegados y mantenidos por Alstom están equipados para salvaguardar las operaciones contra las ciber-amenazas. Esto incluye la implementación de sistemas con características de diseño que proporcionan a los operadores la flexibilidad para realizar modificaciones relativamente fáciles y asequibles en línea con las futuras necesidades de seguridad.

Aunque la ciberseguridad sea una prioridad en todo el ecosistema ferroviario, no podemos subestimar los retos que tenemos por delante: los cambios culturales necesarios, el largo ciclo de vida de los productos ferroviarios y la creciente complejidad de los sistemas ferroviarios, por nombrar algunos.

Los retos no son menores: un mal diseño que no proteja contra las amenazas cibernéticas en evolución puede comprometer la seguridad y la respuesta operativa de redes enteras. La necesidad de que la ciberseguridad sea considerada desde el primer día en el desarrollo de cualquier proyecto es evidente. Las ciberamenazas evolucionan constantemente, y las estrategias para hacerles frente también deben hacerlo.

Los fabricantes y operadores ferroviarios no sólo deben seguir aplicando altos niveles de ciberseguridad, sino que deben hacerlo con soluciones que sean específicas para el ferrocarril y que cumplan las normas de seguridad tanto para los sistemas nuevos como para los heredados, tanto dentro como fuera de la vía.

TRIGO

Centro Especial de Empleo





## COMPROMETIDOS CON LA INTEGRACIÓN SOCIO-LABORAL DE LAS PERSONAS CON DISCAPACIDAD

- Inspección, control y verificación de calidad. Auditorías.
- Retrabajos, recuperaciones y montajes de componentes.
- Embalajes y empaquetados.
- Selección, integración y acompañamiento de personas con discapacidad.

## Consultoría en LGD y Discapacidad

www.cee-trigo.com
ceemadrid@trigo-group.com
Tlf: 660 677 039 - Avd. de las Provincias 33, Oficina 6, 28941 Fuenlabrada (Madrid)

# La Unión Europea avanza en su estrategia común en ciberseguridad con la Directiva Europea NIS2

MARTA MARTÍNEZ PÉREZ

Responsable Departamento Protección de Datos

**MAZ**

**Contacta:**

www.linkedin.com/in/marta-martinez-35a3595a/

**La Comisión Europea es consciente que ante el crecimiento exponencial de las ciberamenazas, ningún Estado miembro puede quedarse atrás en el diseño de su estrategia nacional de ciberseguridad. Para ello a través del proyecto de Directiva conocida como NIS2 ha pretendido el establecimiento de una estrategia básica única en ciberseguridad que permita el diseño de unas medidas de protección básicas como marco de la cultura de cumplimiento en ciberseguridad y el establecimiento de herramientas colaborativas que permitan establecer cauces para favorecer el flujo de información que facilite la gestión de incidentes.**

La Directiva (UE) 2016/1148 conocida como Directiva NIS, de sus siglas en inglés *Network and Information Security*, surgió con el objetivo de establecer un planteamiento global en la Unión que integrara requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales.

Sin embargo, la revolución tecnológica de esta era digital, y la evolución de las amenazas para la ciberseguridad así como el contexto socioeconómico surgido como consecuencia de la guerra de Rusia y la COVID-19 exigían que la ciberseguridad se convirtiera en un objetivo básico de refuerzo para la Unión. Era necesario dar un salto

cualitativo que permitiera desarrollar un marco jurídico básico común entre los Estado de la Unión, que forzara a alinear el diseño de las estrategias nacionales de ciberseguridad cuyo desarrollo era desigual en el territorio europeo.

La desigual sensibilidad en las estrategias de ciberseguridad nacionales era el caldo de cultivo ideal para alimentar vulnerabilidades y riesgos, lo que suponía una motivación más que suficiente para abordar el proyecto de Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad (NIS2) y que entronca con otros proyectos promovidos por la Comisión como el Reglamento DORA.

Las prescripciones establecidas por la Directiva serán aplicables tanto para medianas y grandes empresas de sectores definidos por la norma como importantes (por ejemplo: industria química, farmacéutica, proveedores de servicios digitales o servicios postales entre otros) pero también para la Administración. Para poder facilitar el encuadramiento en el ámbito subjetivo se identifica a las entidades esenciales en el anexo I y las entidades importantes en el anexo II.

En este sentido, destacar la creación del registro de entidades esenciales e importantes que permitirán establecer mecanismos de comunicación y contacto con las mismas. Se excluye del ámbito subjetivo de la Directiva: seguridad o defensa nacional, seguridad pública, policía. Aunque respecto a la gestión de ciberamenazas los Estados miembros deben permitir que las entidades excluidas del ámbito de aplicación puedan notificar voluntariamente ciberamenazas, cuasiincidentes e incidentes significativos.

Los principales aspectos que destacan de la Directiva son:

- Se refuerza la estrategia colaborativa mediante la coordinación en la gestión de incidentes de ciberseguridad mediante la EU-CyCLONe: creando una red de funcionarios de enlace que permita tanto la gestión coordinada como garantizar el intercambio de información regular entre Estados miembros y las instituciones de la UE así como la red CSIRT (cada Estado designará uno o varios) y se articulará como mecanismo colaborativo de intercambio de información en materia de ciberseguridad e incluso asistencia en incidentes transfronterizos. Así mismo, se establece un Grupo de Cooperación a fin de apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros en el ámbito de aplicación de la Directiva.

- Se promueve el establecimiento de medidas colaborativas publico privadas, a través de asociaciones publico privadas con el fin de prevenir, detectar, responder o mitigar incidentes.

- En cuanto a la definición y exigencia de requisitos técnicos de seguridad descritos en el artículo 18 de la Directiva, destacan en la gestión de riesgos en la cadena de suministro, la obligación de las entidades de evaluar y tener en cuenta la calidad general de los productos y las prácticas en materia de ciberseguridad de sus proveedores y prestadores de servicios como, por ejemplo, proveedores de servicios de almacenamiento y tratamiento de datos o servicios de seguridad administrada o, el cifrado de extremo a extremo, para los proveedores de tales servicios y redes de conformidad con los principios de seguridad y protección de la privacidad por defecto y desde el diseño.

- La cultura de ciberseguridad no será una opción, sino una obligación: Los Estados miembros deberán promover que los órganos de dirección de todas las entidades incluidas en el ámbito de aplicación aprueben las medidas de gestión de los riesgos de ciberseguridad adoptadas por las respectivas entidades y reciban formación específica relacionada con la ciberseguridad. Asimismo, deben velar por que las entidades notifiquen a las autoridades nacionales competentes o a los CSIRT cualquier incidente de ciberseguridad que tenga efectos significativos en la prestación de sus servicios.

- Habida cuenta de las dificultades que conlleva implementar la modificación de las políticas de gestión y el fomento de la cultura de cumplimiento, se podrán imponer sanciones en caso de incumplimiento siendo los Estados miembros los que deberán articular su régimen sancionador que deberá comunicarse a la Comisión en el plazo máximo de dos años de la entrada en vigor de la Directiva. Dentro de dicho régimen se prevé para impulsar el compromiso de los órganos directivos de las empresas, la posibilidad de establecer como sanción no sólo la suspensión de la actividad de la Entidad infractora sino también la inhabilitación al ejercicio de responsabilidades a nivel de director general o representante legal.

- Verificación y certificación, los Estados miembros podrán exigir a las entidades esenciales e importantes que certifiquen determinados productos, servicios y procesos de TIC en virtud de un esquema europeo de certificación de la ciberseguridad específico adoptado con arreglo al artículo 49 del Reglamento (UE) 2019/881.

> El contexto socioeconómico surgido como consecuencia de la guerra de Rusia y la COVID-19 exigían que la ciberseguridad se convirtiera en un objetivo básico de refuerzo para la Unión

Está prevista la inminente publicación de la Directiva en el Diario Oficial de la Unión, a partir del cual los Estados miembros dispondrán de 18 meses para la transposición de la norma.

# *Ciberseguridad como pilar fundamental para* La Fábrica del Futuro

BORJA IGLESIAS

Director General y Partner
**Kaizen Institute España**

Contacta:

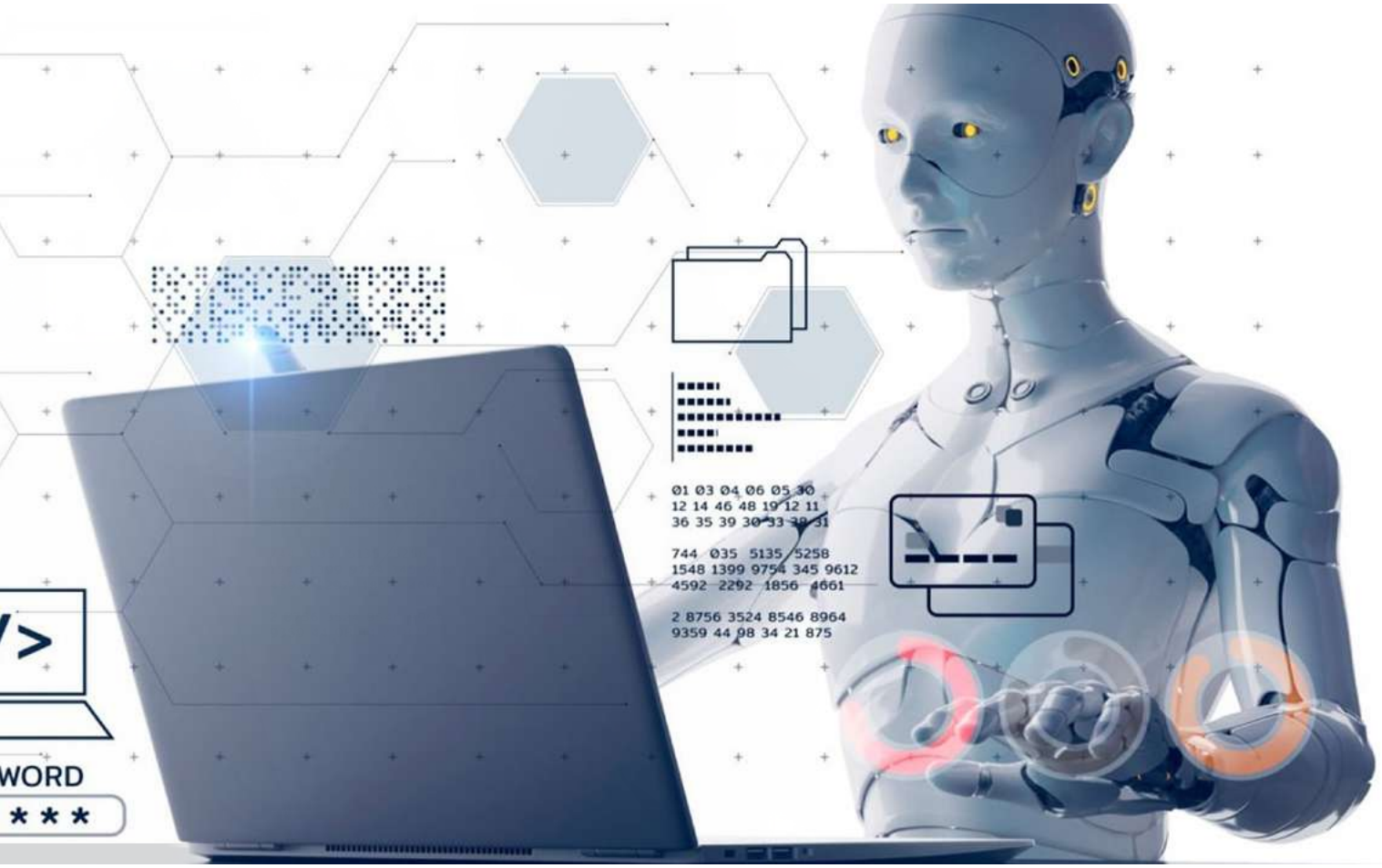
https://www.linkedin.com/in/borjai/

**Al contrario de lo que venía sucediendo hasta la cuarta revolución industrial en la que las empresas industriales venían buscando una mayor capacidad productiva para la fabricación de productos en masa a través de la construcción de grandes líneas de fabricación y optimización de estas. En la actualidad nos encontramos ante otro paradigma en la que las compañías requieren de una mayor flexibilidad y capacidad de adaptación a los requerimientos del mercado para seguir siendo competitivas.**

Estas necesidades llevan a su vez directamente a la implantación de nuevas tecnologías digitales, como el IoT (Internet de las cosas), que posibilitan a las empresas a conseguir esta adaptación de manera ágil sin renunciar a su eficiencia.

A partir de esta transformación tecnológica, las compañías son capaces de monitorizar todos sus procesos operativos en tiempo real y tomar decisiones acertadas basadas en datos. Por lo general estos datos no son únicamente utilizados por la propia compañía, sino que algunos son compartidos con clientes y proveedores para sacar un mayor provecho de estos y optimizar al completo la cadena de valor.

La implementación de estas tecnologías de la información en áreas productivas de la compañía que hasta hace poco funcionaban como cajas negras en las que únicamente contábamos con datos sobre el número de productos fabricados y materiales consumidos durante el día trae consigo enormes beneficios. Una monitorización de los procesos productivos en tiempo real posibilita atacar los problemas de planta con información clave sobre lo sucedido, anticiparnos a futuras averías, o replanificar y secuenciar la producción en minutos en caso de sufrir un imprevisto… entre otros. Así mismo, también trae consigo algunos inconvenientes, como un mayor vulnerabilidad ante ataques y la absoluta necesidad de contar con una estrategia de ciberseguridad bien definida e implementada.




Estos entornos OT (entornos de tecnología operacional) que hasta la fecha se consideraban de bajo riesgo ante ciberataques, debido a su desconexión o bajo grado de interacción con el resto de tecnologías IT(tecnologías de la información), son ahora una gran puerta de entrada para los ciberdelincuentes. Algunos estudios revelan que el 97% de estas compañías sufrió al menos una intrusión en sus sistemas durante el último año. Intrusiones que provocaron desde la perdida o filtración de datos valiosos, hasta en los peores casos, la necesidad de interrumpir las operaciones productivas de planta, con las grandes pérdidas económicas que ello conlleva.

La mayor parte de las vulnerabilidades utilizadas por estos delincuentes son ocasionadas por las conexiones e integraciones entre distintas tecnologías, que en el contexto actual no dejan de crecer. Este problema se agrava en compañías en las que contamos con tecnologías con varias décadas de antigüedad, que no han sido debidamente actualizadas para hacer frente a estos posibles ataques y que ahora se integran con los sistemas a partir de los cuales controlamos nuestras operaciones y gestionamos nuestros datos. Tecnologías que en muchos casos no son herramientas estándar, sino soluciones ad hoc, diseñadas por y para la propia compañía, que cumplen su función, pero no conocemos en profundidad.

> A partir de esta transformación tecnológica, las compañías son capaces de monitorizar todos sus procesos operativos en tiempo real y tomar decisiones acertadas basadas en datos

Algunos de las vulnerabilidades más típicas de las que podemos hablar son:

- Accesos directos inseguros: Pudiendo venir desde los propios equipos de los usuarios, en las que no se controlan si quiera las »

Es crítico contar con una gestión diaria robusta dentro de la compañía que nos ayude a identificar desviaciones en los comportamientos de los usuarios y corregirlos de manera inmediata antes de que constituyan un riesgo de seguridad

direcciones IP desde donde se originan las conexiones para determinar las reglas de acceso adecuadas.

- Equipos no controlados: Ordenadores o salas de control no vigilidas, sin control de accesos ni sistemas de bloqueo, que posibilitan a un atacante conectarse a los sistemas de la compañía.

- Software desactualizado: Implantado varios años atrás por la compañía sin estar diseñados teniendo en cuenta las posibles vulnerabilidades ante ciberataques.

- Softwares maliciosos: Por falta de concienciación y formación a los usuarios que abren archivos adjuntos de emails con emisores poco confiables o conectan a un puerto USB pinchos potencialmente infectados.

- Plan de Acción ante Ataques: Planes de respuesta poco desarrollados o inexistencia de los mismos que provoca el colapso de la organización ante una intrusión en sus sistemas informáticos.

Hemos visto distintas casuísticas que pueden facilitar un ciberataques, pero no podemos olvidarnos de la más importante, "El factor humano". La cual se estima que en 2021 fue el responsable del 95% de las infracciones de seguridad. Con esto, queda claro, que cualquier estrategia de ciberseguridad debería contemplar como una de sus líneas principales la concienciación y formación de las personas del equipo para el seguimiento de unos procedimientos y hábitos seguros, así como la detección de intentos de manipulación por agentes externos, la llamada "ingeniería social".

La ingeniería social es una técnica de manipulación utilizada por los ciberdelincuentes para hacer uso del error humano, con múltiples intenciones maliciosas, como el acceso a los datos críticos o sistemas de la compañía. Normalmente los atacantes se aprovechan especialmente de aquellas personas con escasos conocimientos digitales o que no son plenamente conscientes del valor de los datos que comparten o a los que dan acceso. Uno de los métodos más habituales utilizados en estos casos es el Pishing.

Ante esta situación, es crítico para cualquier empresa industrial el contar con estrategia de ciberseguridad que avance y se actualice en concordancia a la aparición de nuevas amenazas digitales. Para conseguir esta actualización constante, debemos contar con un proceso iterativo de desarrollo, en el que:

1. **Analizar nuestra situación inicial.** Mapeando el estado de nuestros sistemas OT e IT, procesos y personas, de cara a identificar los gaps principales de seguridad y darles solución.

2. **Diseñar una plan de mitigación para cada uno de los gaps identificados**. Manteniendo siempre en el foco el no perder agilidad y eficiencia de nuestros procesos. No generar procesos burocráticos innecesarios que compliquen en exceso nuestra dinámica, o que sean difícilmente afrontables por los usuarios finales.

3. **Ejecutar el plan e implementar las soluciones definidas.** Implementación de nuevas tecnologías, desarrollo de las ya existentes o formación y concienciación de los usuarios finales.

4. **Evaluar del impacto y buen funcionamiento de las soluciones implementadas,** para posteriormente volver al paso 1, y realizar de nuevo un análisis del punto de partida para seguir mejorando de manera iterativa.

Este tipo de despliegues conllevan grandes cambios a nivel conductual en las personas de la organización, qué en caso de no consolidarse, redundarán en un no funcionamiento del plan. Por esto es crítico contar con una gestión diaria robusta dentro de la compañía que nos ayude a identificar desviaciones en los comportamientos de los usuarios y corregirlos de manera inmediata antes de que constituyan un riesgo de seguridad.


**Brains International School Las Palmas de G.C.**
Pº Tomás Morales, 111 (Nursery)
C/ Pérez del Toro, 72 (Primary)
35004 Las Palmas de Gran Canaria
Tel.: 928 29 64 44

**Brains International School Telde**
Carretera de La Pardilla Km 1,7
35213 La Pardilla (Telde) Gran Canaria
Tel.: 928 50 61 14

**Brains International School Conde de Orgaz**
C/ Frascuelo, 2, 28043 Madrid
Tel.: 91 388 93 55

**Brains International School María Lombillo**
C/ María Lombillo, 5 y 9, 28027 Madrid
Tel.: 91 742 10 60

**Brains International School La Moraleja**
C/ Salvia, 48, 28109, Alcobendas, Madrid
Tel.: 91 650 43 00

**www.colegiobrains.com**

**RESERVA TU VISITA PERSONALIZADA**

# Ciberseguridad en los tiempos de Blockchain

GABRIELA CHANG VALDOVINOS

CSO y cofundadora
**EthicHub**

**Contacta:**

https://www.linkedin.com/in/gabriela-chang-valdovinos-76b34410/

**Para entender por qué se denomina a la tecnología Blockchain *la revolución industrial de Internet* es necesario partir de sus diferencias básicas: el registro de la información en Blockchain está replicado y distribuido en una red descentralizada que se actualiza constantemente, mientras que en Internet la información se almacena centralizada en grandes servidores.**

El almacenamiento centralizado conlleva riesgos de ataques físicos a los servidores (inundaciones, incendios) o hackeos que eliminan o alteran la base de datos a la que accedemos desde los ordenadores. La evolución de este modelo centralizado son las redes descentralizadas o distribuidas donde las bases de datos se replican para guardar copias idénticas en miles de puntos de almacenamiento (nodos), lo que las hace más resistentes a los ataques cibernéticos ya que se tendrían que modificar simultáneamente todas las réplicas almacenadas para alterar la información. Adicionalmente, al estar replicada y distribuida, aunque se destruyan algunas copias (nodos) la información se preserva en el resto de ellos. *(Figura 1)*

La potente capacidad de encriptación que ha dado lugar al desarrollo de la tecnología blockchain no ha surgido de la noche a la mañana. Es el resultado de más de cuarenta años de investigación. Dicen que cuando un programador ve el código de la blockchain reconoce las partes y se sorprende de que no se haya implementado antes.

La cadena de bloques (blockchain) se llama así porque la información se almacena encriptada en bloques que se completan en unidades de tiempo (por ejemplo, cada diez minutos) o por volumen (por ejemplo cada que se acumula 1Mb). Estos bloques se enlazan en orden consecutivo, quedando relacionados matemáticamente. Una blockchain pública guarda el registro de interacciones ocurridas, que pueden consultarse libremente en

un visualizador de bloques (por ejemplo ethers scan.io). Una vez que un bloque es validado y cerrado, no puede ser alterado, por eso se dice que la cadena es inmutable. El proceso para cerrar y validar bloques es distinto dependiendo de cada blockchain. En la blockchain de Bitcoin se llama minería y es la forma de incentivar la seguridad de su red: por medio de incentivos cripto económicos programables. *(Figura 2)*

Partiendo de la base de que la cadena de bloques o blockchain es la garantía de que los datos no han sido alterados, nos encontramos con un nuevo modelo en el que las interacciones entre particulares no requieren de la intermediación de un tercero de confianza para validar la información. Estas interacciones pueden ser, por ejemplo, el intercambio de archivos de valor. Es por ello que a la Blockchain también se le conoce como Contabilidad de triple entrada o Internet del Valor.

Y a partir de estos intercambios (y custodia) de archivos de valor, surgen nuevos paradigmas sobre la seguridad: por primera vez es posible prescindir de entes centrales para el depósito y custodia de unidades digitales de valor. Esta nueva autonomía en la custodia de los bienes repercute en retos de ciberseguridad para proteger a individuos y entidades de los ataques informáticos. Paradójicamente, la costumbre de haber requerido confiar en terceros para almacenar nuestros bienes es lo que nos hace vulnerables.

Para interactuar en la Web2 necesitábamos crear una cuenta en las plataformas de terceros, mientras que la Web3 nos permite interactuar con otros actores, sin intermediarios. Interactuar de forma segura requiere ser consciente de la responsabilidad de ser nuestros propios custodios. En el mundo blockchain se dice con frecuencia “no confíes, verifica” porque en cualquier intercambio de valor estamos expuestos a los fraudes o la mala fe de terceros.

El gran reto de la innovación es la adopción masiva, pero el desconocimiento genera desconfianza, por eso resulta clave informarnos adecuadamente de las ventajas y desventajas de las nuevas tecnologías antes de descalificar su enorme potencial por falta de conocimiento.

**Figura 1. Tipos de redes**

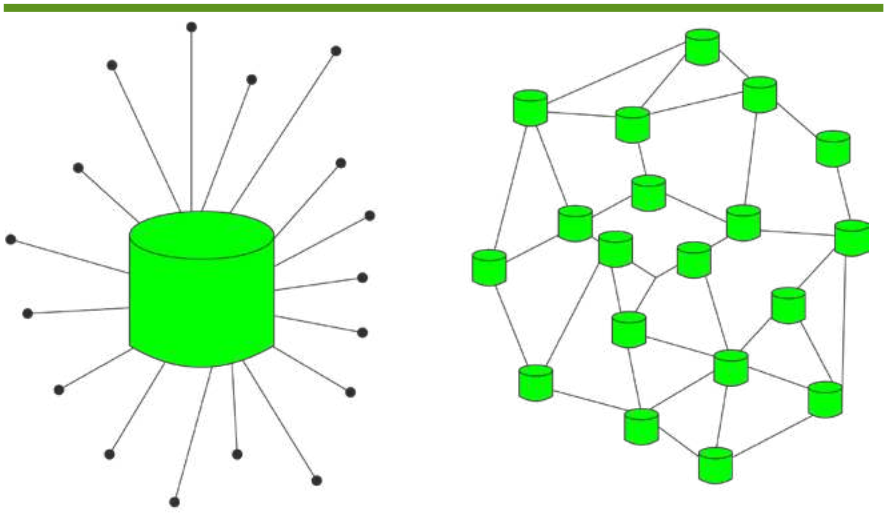
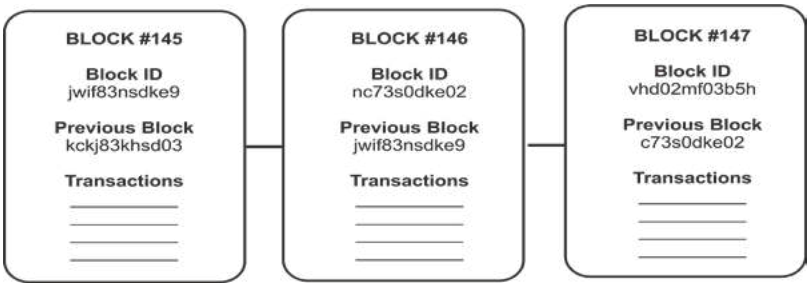


**Figura 2. Cadena de bloques**

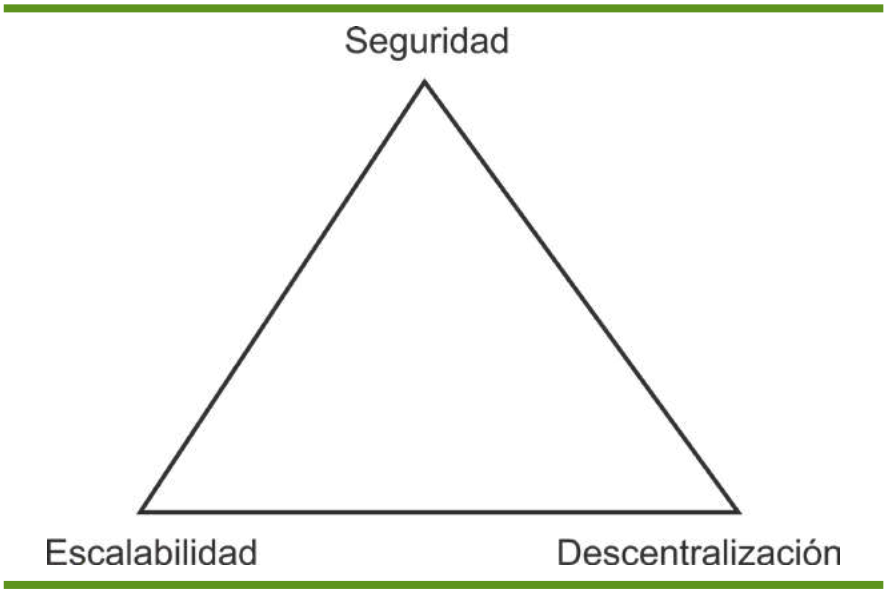



A nivel de seguridad es muy importante entender el trilema de la Blockchain que definió Vitalik Buterin, el fundador de Ethereum: cuando una Blockchain intenta ser mucho más rápida, escalable o útil, lo hace a costa de la seguridad o la descentralización que es una parte fundamental para que una cadena de bloques se mantenga inmutable y resistente a la censura en el tiempo. Para participar en una red social descentralizada y ganar puntos por los likes que otros usuarios dan al contenido, se necesita una blockchain muy escalable y barata de usar, mientras que para guardar los fondos de un plan de pensiones, deberá primar la seguridad sobre la velocidad o el coste. *(Figura 3)*

Mientras que en Internet y software tenemos estándares de s*(Figura 3)*guridad comúnmente adoptados que hacen que cualquier pasarela de pago, red social, ERP o CRM sean igualmente seguros, en Blockchain nos vemos obligados a entender los “Trade-Offs” que una blockchain o un protocolo construido sobre blockchain han implementado para

» Los retos de la seguridad evolucionan de preservar la integridad de la información hacia preservar la identidad de los usuarios para permitirles disfrutar de una privacidad con responsabilidades

Figura 3. Blockchain Trilemma




Estamos frente a un cambio de paradigma en la seguridad informática: si en la era Web2 (antes de Blockchain) la seguridad implicaba resguardar y proteger la información valiosa bajo siete candados, en la era Web3 la información se protege haciéndola pública y visible

conseguir una velocidad mayor o un coste de operación menor. Por eso EthicHub apoya el proyecto que lidera nuestro Security Advisor Luis A. Rodrigo Piqueras para construir un sistema de Rating Público que permita calificar la seguridad de los diferentes protocolos Web3.

En los inicios de Internet, los Estados desconfiaban de su utilidad y hoy en día en gran parte del mundo la declaración de la renta se hace online. Blockchain es una tecnología mucho más potente que Internet, y apenas estamos viviendo la fase temprana equivalente a la aparición del correo electrónico.

El mundo cambia cada vez más rápido y la tecnología modifica la manera en la que nos relacionamos. La identidad digital cobra mayor relevancia cuando las interacciones online aumentan día con día. Evolucionamos hacia una identidad que nos permitirá una privacidad responsable, donde un periodista podrá recibir el beneficio económico y el crédito por sus artículos, sin poner en riesgo su seguridad personal, donde la información compartida se limitará a la estrictamente necesaria y las bases de datos ya no almacenarán la información sensible de millones de usuarios sino cada uno de ellos será su propio custodio.

Finalmente, la tecnología es una herramienta, y de nosotros depende utilizarla para crear y construir, aunque en etapas tempranas de desarrollo de cualquier tecnología disruptiva, la especulación tiene un protagonismo desproporcionado tal y como pasó con la burbuja de las puntocom con Internet.

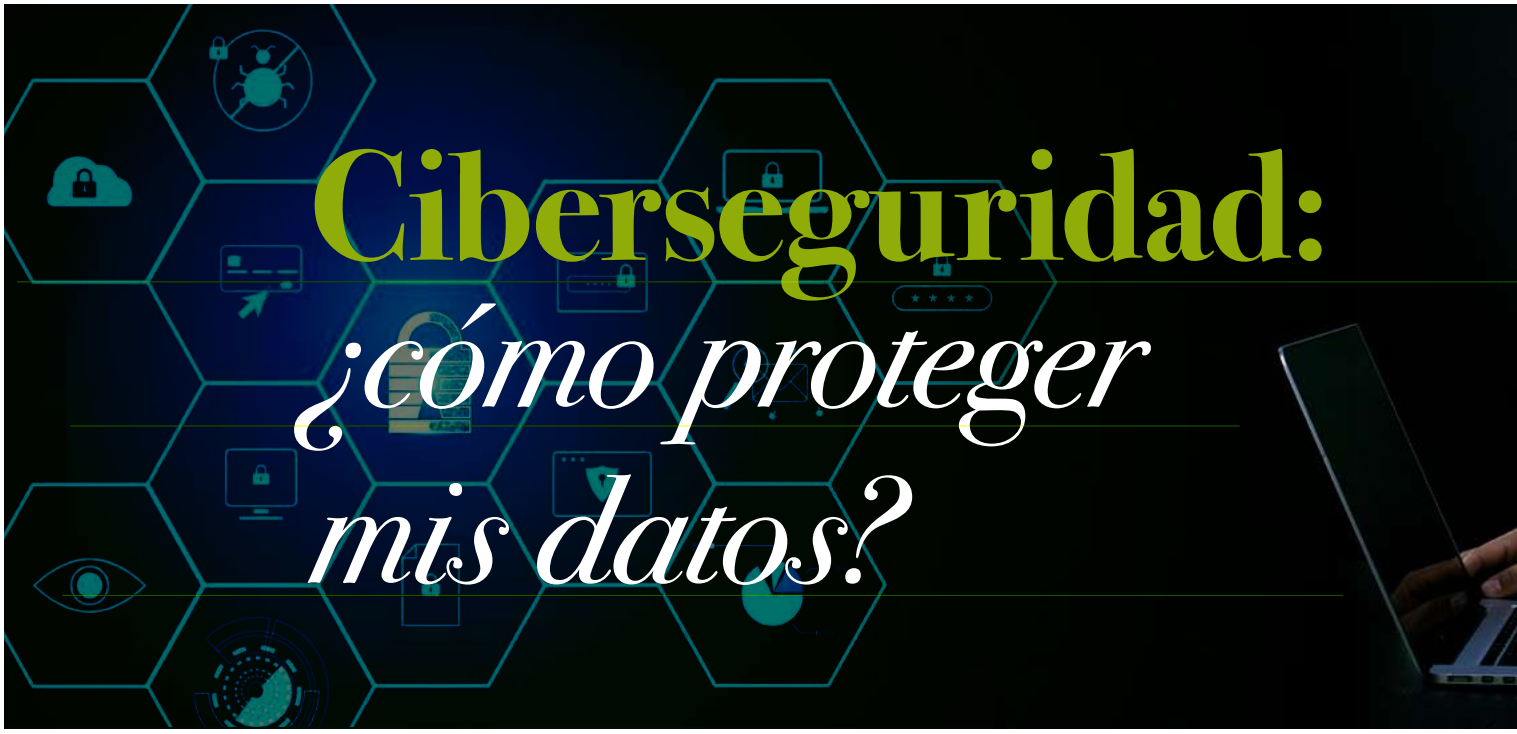
Desde junio del 2018, EthicHub utiliza la tecnología blockchain para conectar regiones económicas complementarias, resolviendo la falta de acceso al sistema financiero tradicional para los llamados *desbancarizados* (la cuarta parte de la población mundial según datos del Banco Mundial). Gracias a este internet del valor, personas de cualquier parte del mundo pueden enviar fondos a cooperativas agrícolas de pequeños agricultores en economías emergentes, para impulsar su crecimiento económico y social de una manera rentable para todos los participantes. La trazabilidad y transparencia en el manejo de los fondos aporta la capa de confianza necesaria para interactuar con personas del otro lado del mundo sin necesidad de intermediarios financieros cuyo coste haría inviable la operación para miles de familias que hoy se benefician con la blockchain.

El registro inmutable de los préstamos recibidos y de su devolución constituye un historial de reputación que permite a estos agricultores acceder a la financiación necesaria para sacar adelante sus actividades productivas.

Los *contratos inteligentes* inscritos sobre una blockchain pública actúan como un scrow para recibir la financiación colectiva de múltiples inversores y asignarla a la cuenta específica de la cooperativa. En sentido inverso, una vez que la cooperativa devuelve el préstamo bajo las condiciones estipuladas en el contrato inteligente, el principal más los intereses son distribuidos proporcionalmente entre los inversores participantes.

Dado que un *contrato inteligente* no puede modificarse una vez inscrito en la blockchain, es imprescindible auditarlo previamente. Estas y otras medidas de ciberseguridad logran que la interacción con la blockchain resulte mucho más segura y confiable.

La siguiente ola de innovación es la sostenibilidad: las empresas que no sean sostenibles dejarán de ser rentables. De nosotros depende prepararnos para surfear esta ola, adaptando nuestras empresas y modelos de negocio hacia un futuro más prometedor para todos.



# Ciberseguridad: ¿cómo proteger mis datos?

GABRIELA CONTRERAS

Ingeniero calidad, seguridad y medio ambiente

**BlueKanGo**

**Contacta:**

www.linkedin.com/in/gabriela-contreras-

JAVIER BULLÓN CARO

Country Manager - España

**BlueKanGo**

**Contacta:**

www.linkedin.com/in/javierbullon/

**La ciberseguridad es parte fundamental de la seguridad informática, un tema que cobró mayor relevancia con la pandemia por el Covid-19. A medida que las empresas han comenzado a acelerar su transformación digital, el número de ciberataques ha aumentado en paralelo. El objetivo es proteger los recursos de las organizaciones contra los ciberataques y todas las amenazas que pueden producirse por medio de la red. Según un estudio elaborado por Deloitte, en el 2021, el 94% de las empresas españolas sufrieron incidentes de ciberseguridad. Los datos de las organizaciones están en riesgo si no se establecen estrategias de prevención oportunas.**

## ¿Qué se trata con la ciberseguridad?

Siempre que pienso en el momento en que La ciberseguridad engloba desde la evaluación de riesgos, los procedimientos, las herramientas y toda acción que tiene como propósito proteger los activos informáticos, las redes y los datos de los ciberataques. Este tipo de ataques se utiliza para obtener acceso a los sistemas, interrumpir las operaciones, alterar y/o robar datos, incluso es empleado para extorsionar a las víctimas. Ocurre en diferentes sectores y es independiente del tamaño de la empresa, puede ocurrir tanto en grandes organizaciones como en pymes; de hecho, las pequeñas estructuras suelen estar menos preparadas para este tipo de ataques, estudios han indicado que el 40% de las pymes sufren problemas con sus sistemas.

En España, para el 2021, los sectores más impactados fueron los seguros, la banca, la fabricación, las telecomunicaciones, medios de comunicación y tecnología. Los mismos son un blanco para los cibercriminales, por lo que contar con un sistema maduro en materia de ciberseguridad se ha vuelto una gran necesidad.

Los daños para las organizaciones son enormes, ya que suelen provocar daños financieros, de reputación, causan fallas en la infraestructura informática, entre otros. Para proteger todos los recursos y datos necesitan de una política de ciberseguridad robusta y de herramientas digitales que sirvan de barrera.

## ¿Cómo prevenir los riesgos de ciberataques?

Como lo mencionamos anteriormente, hoy los riesgos son más altos, por lo que las organizaciones deben contar con un Plan de continuidad TIC (PCTIC), el cual hace parte del Plan de Continuidad del Negocio (PCN). Según el Instituto Nacional de Ciberseguridad, estos planes aseguran la

Los daños para las organizaciones son enormes, ya que suelen provocar daños financieros, de reputación, causan fallas en la infraestructura informática, entre otros. Para proteger todos los recursos y datos necesitan de una política de ciberseguridad robusta y de herramientas digitales que sirvan de barrera

continuidad de las actividades de la organización en caso de fallas del sistema.

Existen diversos tipos de ciberataques, los más comunes incluyen malware, ransomware, phishing y denegación de servicio. Un comportamiento riguroso puede ayudar a proteger tus datos, existen estrategias eficientes como buenas prácticas para tomar las precauciones necesarias. Los ejemplos más habituales o básicos son:

- **Contar con copias de seguridad de los datos**: es una de las acciones básicas a poner en marcha. En caso de pérdida de la información por un ciberataque, la empresa contará con un respaldo, lo cual no impactará la continuidad de la actividad.

- **Efectuar un control de acceso al sistema:** cuando una persona abandona la organización, se deben limitar sus accesos de manera inmediata.

- **Implementar herramientas de control:** existen software que detectan las amenazas a tiempo por medio de un monitoreo de seguridad continuo, por ejemplo la solución SIEM (Security Information and Event Management).

- **Aplicar procesos de concienciación y formación de los empleados**: lo ideal es hacer formaciones regulares sobre ciberseguridad, con el fin de dotar a los empleados de los conocimientos necesarios para proteger sus datos. Por ejemplo, evitar el intercambio de dispositivos USB, o abrir enlaces externos, utilizar un software antivirus, instalar una VPN, elegir contraseñas apropiadas “no usar 1234”

## Utilizar soluciones digitales seguras

Desde la crisis sanitaria la transformación digital se ha acelerado; lograr obtener la información al instante y compartir documentos a distancia son una de las multiples necesidades. A esto debemos sumar la seguridad de los datos, los accesos a las diferentes soluciones deben tener un acceso para cada usuario, garantizando solidez. ¿Cuál es la mejor solución que podemos emplear?

## Diferencia entre Cloud Computing “la nube” y un Software SaaS

Estamos lejos de ver cómo los avances en la tecnología informática deceleran, por lo cual es importante conocer cuál es la solución más segura y que se adapta a las necesidades de nuestra organización. Muchas son las preguntas con respecto a la solución mejor adaptada, hemos escuchado hablar sobre “la nube” y también sobre SaaS, pero, concretamente, ¿qué son? »


» El Cloud Computing incluye los tres siguientes componentes: Software como un servicio (SaaS), la infraestructura como servicio (IaaS) y la plataforma como servicio (PaaS).

La mayor parte de los productos SaaS funcionan por medio de un navegador web y se encuentran localizados en "la nube", no se alojan en los dispositivos (ordenador o móvil), lo que garantiza seguridad y disponibilidad. Desde el gran auge tecnológico de los 90 las aplicaciones SaaS han cobrado mayor fuerza, debido a que se requería de una herramienta de menor coste con una ubicación central. La realidad es que el modo SaaS tiene la particularidad de ver rápidamente el Retorno sobre la inversión, también llamado ROI.

## ¿Prefieres un apartamento vacío o amueblado?

Utilicemos un ejemplo para dar mayor claridad, cuando utilizas "la nube" compras un espacio de la máquina virtual, te dan una determinada cantidad de potencia de cálculo, memoria y almacenamiento, sin embargo, para poder utilizar todas las aplicaciones que necesites tendrás que comprar las licencias de software y configurarlas. El Software SaaS se adapta a tus necesidades, tienes todo listo para empezar a trabajar. Es como tener un apartamento vacío y uno amueblado.

## Ventajas de un software SaaS

Algunas de las mayores dificultades a la hora de utilizar un software es la instalación, mantenimiento y las actualizaciones, al utilizar un software SaaS todos estos inconvenientes desaparecen. El modo SaaS garantiza que trabajes siempre en la última versión, no debes preocuparte por instalar actualizaciones. Al mismo tiempo que el SaaS sigue creciendo y mejorando, lo hacen las ventajas que ofrece a los usuarios y su seguridad.

En caso de fallos en el sistema, los proveedores SaaS emplean sitios separados para la producción y las copias de seguridad. Cuando ocurre un incidente en un sitio, siempre será posible recuperarlos. Ellos emplean herramientas para revisar las diferentes bibliotecas de manera regular, en caso de fallo enviará alertas automáticas. Del mismo modo, emplean herramientas que analizan el código y notifican a los diferentes equipos.

Las soluciones SaaS son consideradas como un elemento de barrera contra posibles ciberataques. Los proveedores de este tipo de servicios deben garantizar la seguridad de sus datos por medio de un sistema de control, es por ello que debemos conocer cuáles son los factores a tener en cuenta a la hora de escoger el mejor proveedor.

Ahora la pregunta es saber ¿cuál es el mejor proveedor?

Es aquel que asegure tus datos y al mismo tiempo te permita trabajar de manera eficiente en tu día a día. El proveedor está en la obligación de asegurar que tus datos están almacenados en servidores seguros, por ejemplo, que se beneficien de herramientas como Microsoft Azure. Incluso, que cuenten con una certificación ISO 27001, lo cual, da garantía de que tienen un sistema de seguridad de la información robusto, donde los equipos están formados en buenas prácticas y se llevan a cabo auditorías de seguridad de manera regular.

Los ciberataques han aumentado en los últimos años, nadie es inmune a estos ataques, sin embargo, podemos poner en práctica acciones para reducir el riesgo y crear barreras y proteger los recursos de la organización. Para facilitar la puesta en marcha de estrategias de prevención existen soluciones digitales adaptadas y normas que podrán ayudarte a lo largo de este proceso.

# EthicHub, pioneros en Finanzas Regenerativas sobre Blockchain

Con más de **5 años en el mercado** y múltiples premios por inclusión financiera e impacto social, **EthicHub** es un referente en la aplicación de la tecnología blockchain para llegar de forma rentable a la población sin acceso al sistema financiero tradicional.

Democratizamos la **inversión de impacto** gracias a nuestra plataforma de crowdlending (app.ethichub.com) donde cualquier persona o entidad puede financiar proyectos agroalimentarios ubicados en regiones emergentes, obteniendo una **rentabilidad fija del 8%** anual mientras contribuye con impacto económico, social y medioambiental.

Todos los proyectos publicados están protegidos por nuestro innovador Sistema de Compensación que actúa como un "**blended finance**" contra el riesgo de impago, incentivando la inversión alineada con los **objetivos Objetivos de Desarrollo Sostenible (ODS)** de la ONU.

Visita nuestra web www.ethichub.com y súmate a la regeneración económica.

2022

**8%**
Rentabilidad media

**>$2,5M**
Volumen de financiación

**450**
Proyectos financiados

Retornado
**100%**

# Las claves de una organización ciberresiliente

IDOIA
URIARTE LETAMENDI

CISO
**Grupo MASMOVIL**

**Contacta:**

https://www.linkedin.com/in/iuriarteletamendi/

**Podemos definir la ciberresiliencia como la capacidad de un proceso, negocio, organización o nación para anticipar, resistir, recuperarse y evolucionar, no solo para recuperar su estado inicial, sino para mejorar sus capacidades de sobreponerse ante condiciones adversas, estrés o ataques a los recursos cibernéticos que necesita para funcionar. Uno de los objetivos que persigue es evolucionar en las capacidades ciber en todas sus dimensiones, con el fin de minimizar los impactos adversos de los ataques reales o previstos de los adversarios. Este objetivo debe alcanzarse en el contexto de los cambios en el entorno, y es el tema que trataremos en este artículo, analizando las tendencias observadas y su repercusión en el sistema de gestión de la seguridad de información implantado en el GRUPO MASMOVIL con el fin de mejorar en su capacidad de ciberresiliencia.**

Profundizando en el concepto de ciberresiliencia, podemos indicar que ésta persigue cuatro objetivos fundamentales:

- **Anticipar:** anticiparse es mantener un estado de preparación informado para prevenir que los atacantes consigan comprometer las funciones de la organización.
- **Resistir:** resistir es continuar con las funciones esenciales de la misión/negocio a pesar de un ataque por parte de un adversario.
- **Recuperar:** recuperar es restaurar las funciones de la misión/negocio lo antes posible tras la ejecución exitosa de un ataque por parte de un adversario.
- **Evolucionar:** evolucionar es cambiar las misiones/funciones empresariales y/o las ciber capacidades de apoyo, con el

fin de minimizar los impactos adversos de los ataques reales o previstos de los adversarios.

De acuerdo al informe publicado en noviembre de este año por ENISA, la agencia europea de ciberseguridad, las principales tendencias observadas en el último año en el escenario de ciberamenazas son las siguientes:

- El ransomware y los ataques contra la disponibilidad (ataques de denegación de servicio) se sitúan en el top de los ciberataques.
- Los actores de los ataques han utilizado exploits de día cero para lograr sus objetivos operacionales y estratégicos. Cuanto mayor es la madurez en ciberseguridad de las compañías, mayor es el coste para los atacantes, debiendo desarrollar o comprar exploits de día cero, ya que las estrategias de defensa en profundidad reducen la disponibilidad de vulnerabilidades explotables.
- La geopolítica continúa teniendo un impacto importante en las ciberoperaciones, y los ciberataques destructivos son un componente principal en las operaciones de los agentes estatales, como hemos podido observar en la guerra Rusia-Ucrania.
- El modelo de negocio del hacking como servicio ha ganado tracción, especialmente desde el año 2021.
- Se ha observado una nueva ola de hacktivismo, especialmente desde que empezó la guerra Rusia-Ucrania.
- El phishing es, una vez más, el vector de ataque más utilizado. Se han detectado nuevas técnicas más sofisticadas, fatiga en los usuarios y phishing dirigido y basado en el contexto como principales elementos del incremento que ha sufrido.
- Las técnicas de extorsión están evolucionando, con el uso de ciertos sitios de leaks que han ganado en popularidad.
- El malware ha vuelto a aumentar después de la disminución que se notó y se vinculó con la pandemia.


El phishing es el vector de ataque más utilizado. Se han detectado nuevas técnicas más sofisticadas, fatiga en los usuarios y phishing dirigido y basado en el contexto como principales elementos del incremento que ha sufrido

- El compromiso de los datos se incrementa año a año dado el papel central que ocupan los datos en nuestra sociedad.
- Los ataques DDOS se están haciendo más grandes y complejos, y se están moviendo hacia las redes móviles e Internet of Things (IoT).
- Los grupos atacantes tienen un mayor interés en la cadena de suministro.
- La desinformación es una herramienta en la guerra cibernética.

De acuerdo a dichas tendencias, hay dos actores que resultan fundamentales para tener una organización ciberresiliente: las personas que forman la compañía y los proveedores. Una compañía será ciber-resiliente en la medida en que todas las personas que trabajan en la misma y sus proveedores lo sean.

Para ello es necesario empoderar a los usuarios, haciéndoles partícipes de la responsabilidad que tienen, dotándoles de las herramientas y soporte necesarios para hacer


El Grupo MASMOVIL es un referente de transformación e integración digital, ejemplo de crecimiento orgánico e inorgánico en un sector que permite la transformación digital de la sociedad, y lo ha hecho de forma compatible y equilibrada con ser una organización ciberresiliente

frente a la ingeniería social, phishing, smishing, vishing y todas las modalidades que intentan engañar y conseguir credenciales de acceso, información de la compañía....

Como indicábamos, tenemos que prestar atención especial a la cadena de suministro, clasificando el nivel de riesgo de los proveedores, estableciendo las medidas de seguridad que tienen que cumplir a nivel contractual, reforzando las previamente definidas, y asegurando el cumplimiento de las mismas, mediante los assesments y evidencias necesarias. También resulta necesario profundizar en los procedimientos de gestión y respuesta ante incidencias en la cadena de suministro, para ejecutar las acciones necesarias de contención y recuperación con el menor impacto al negocio, y de forma coordinada. Esto también obliga a reconsiderar la arquitectura/conectividad y forma de trabajo con determinados proveedores, con el fin de asegurar que un posible incidente en un proveedor no se propague a nuestra organización y que el impacto sea el menor posible.

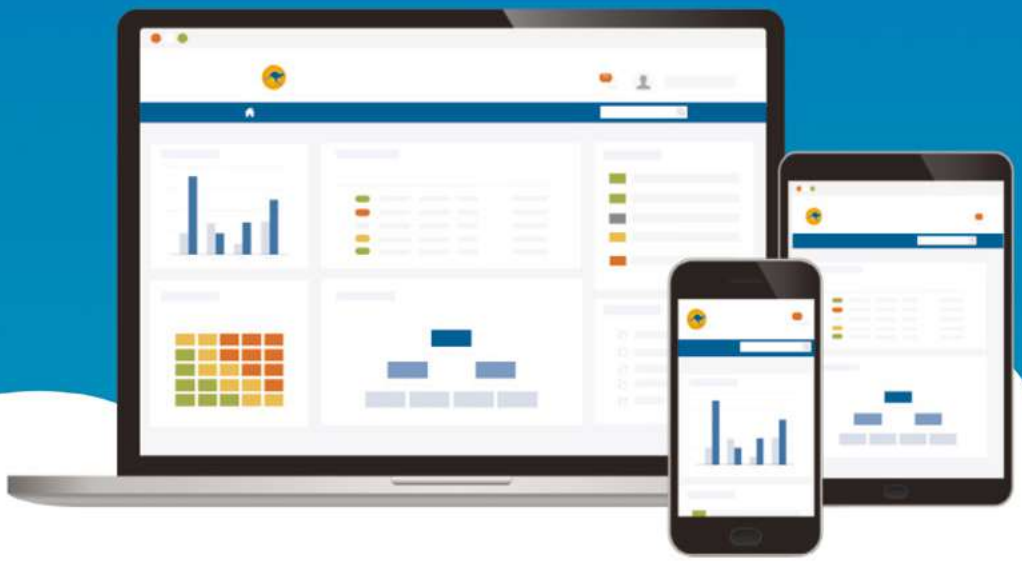
Por otro lado, teniendo en cuenta las tendencias observadas en cuanto a tipo de ataques, resulta necesario revisar, y mejorar las capacidades de los sistemas anti-DDOS, más aún teniendo en cuenta nuestro papel como operadores de telecomunicaciones y prestador de servicios digitales, así como las medidas anti-ransomware, anti-malware y de gestión de vulnerabilidades implantadas para anticiparnos y resistir a posibles incidentes. Esto implica disponer de la última tecnología implantada para hacer frente a estas amenazas y reforzar los procesos existentes, para la monitorización de eventos, detección y resolución de incidencias, gestión de KRIs… Surgen aquí, por tanto, los dos pilares básicos para la ciberresiliencia, la tecnología y los procesos, ambos necesarios para prevenir, detectar y remediar posibles incidentes. Todo ello, acompañado de la necesaria vigilancia digital con el fin de detectar información publicada que resulte de nuestro interés, posibles amenazas adicionales...

Personas, proveedores, tecnología y procesos son los actores y pilares clave que se recogen en el sistema de gestión de la información del Grupo MASMOVIL, en el que, a partir del análisis de los riesgos existentes con los activos, información y servicios que prestamos, determinamos qué salvaguardas tenemos implantadas, qué nivel de riesgo consideramos o no aceptable y qué tratamientos del riesgo consideramos necesario, todo ello, en sucesivos ciclos de mejora continua. Los servicios, datos, infraestructuras y equipamientos están cada vez más distribuidos (en la nube, en el datacenter, en la oficina, en la calle, en casa…), por lo que es necesario trabajar de forma transversal en los ámbitos arriba indicados y de forma continuada en el tiempo, para que el nivel de riesgo sea cada vez menor, en un escenario global en el que la extorsión informática, el robo de información y otros delitos cibernéticos son una realidad creciente.

Y para finalizar, creo que el Grupo MASMOVIL es un referente de transformación e integración digital, ejemplo de crecimiento orgánico e inorgánico en un sector que permite la transformación digital de la sociedad, y lo ha hecho de forma compatible y equilibrada con ser una organización ciberresiliente.

BlueKanGo

# LA PLATAFORMA BPM TODO EN UNO DE CALIDAD, MEDIOAMBIENTE, PREVENCIÓN, RSE 100% CONFIGURABLE



- La infraestructura más potente y segura.
- Acceso nominativo e ilimitado (empleados y partes interesadas).
- Acompañamiento por expertos en todo momento.
- Taller de creación de aplicaciones No-Code, para que puedas tener tus propias aplicaciones. Amplio catálogo.
- Plan de acción global, Gestor Documental, estadísticas, módulo API, módulo de autoevaluación.

WWW.BLUEKANGO.COM

# Riesgos de ciberseguridad en la transformación de los servicios financieros

ALEXANDRA NAVARRO LAHOZ
CISO
**Ibercaja Banco**

**Contacta:**
https://www.linkedin.com/in/alexandra-navarro-lahoz-01a1006/

**En los últimos tiempos, el sector de banca ha estado trabajando en evolucionar cada vez más hacia un modelo más digital y con mayor presencia en Internet. De esta forma, se consigue que sea menos necesario realizar trámites y transacciones de manera presencial, permitiendo a los clientes tener una inmediatez y comodidad superior a los modelos tradicionales y donde, además, se reducen los costes operativos.**

Este nuevo paradigma conlleva que ahora las entidades financieras estén expuestas a nuevas y más complejas amenazas en materia de ciberseguridad incrementando el nivel de exposición a los riesgos de ciberseguridad y fraude digital. En los comienzos de Internet, había un número reducido de expertos de seguridad que se dedicaban, por ejemplo, a tratar de comprometer sistemas por fallos de seguridad informática, en muchos de los casos únicamente con fin didáctico. Ahora, en cambio, hay bandas criminales totalmente profesionalizadas y organizadas que se dedican única y exclusivamente a lucrarse y obtener el mayor rendimiento económico posible aprovechándose de fallos de seguridad de los sistemas, robando información o secuestrándola, estafando a los usuarios usando medios tecnológicos, etc. Para el delincuente, el cibercrimen acarrea mucho menos riesgo que un modelo de delincuencia tradicional, ya que es más anónimo y silencioso, y permite realizar estos ataques desde cualquier parte del mundo y a cualquier objetivo con presencia digital.

Por tanto, las entidades financieras, para disminuir los riesgos, deben disponer de una buena estrategia de seguridad que se revise constantemente y que se vaya adaptando a las nuevas amenazas que evolucionan con muchísima rapidez.

Las principales amenazas a las que está expuesto el sector financiero en la actualidad son de distintos tipos:

## Cadena de suministro

Las entidades financieras colaboran con muchos proveedores de todo tipo. Esto conlleva un riesgo ya que, depende del modelo de colaboración, si el proveedor tiene un fallo de seguridad y sus sistemas son comprometidos, puede acabar afectando también a la seguridad de la entidad. Los métodos de propagación son diversos, por ejemplo, que los propios correos enviados por el proveedor tuvieran contenido malicioso y por ser remitidos por dichos usuarios, los empleados de la entidad confiaran en ellos. Otro método es que, si hay algún tipo de conectividad entre ambas compañías, el atacante, una vez comprometidos los sistemas y la red del proveedor, tratará de saltar a los de la entidad. También que el proveedor disponga de datos confidenciales de la entidad, y estos sean sustraídos directamente de sus sistemas, etc.

Para disminuir el riesgo de esta amenaza se hace necesario llevar a cabo revisiones de las medidas de seguridad de dicho proveedor que cubran todos los aspectos, como si se tratara de una extensión de la entidad: auditorías periódicas de sus sistemas, correcta gestión de vulnerabilidades y obsolescencia, procedimientos de respuesta ante incidentes de seguridad, sistemas antimalware, etc. Debe haber también un buen protocolo de comunicación en el que el proveedor pueda notificar en tiempo y forma si sufren un incidente de seguridad para poder tomar medidas, como pueda ser cortar las comunicaciones con dicho proveedor de manera preventiva y temporal hasta que el problema se solucione.

## Ataques ransomware

Consisten en comprometer los sistemas de la empresa por medio de distintos vectores de entrada para después cifrar sus datos. Por ejemplo, el envío de correos maliciosos a los empleados, para comprometer el PC de un usuario, con el fin de moverse lateralmente por los

sistemas, hasta tener el control y permisos suficientes para cifrar los datos afectando a la disponibilidad de la información. Posteriormente, los delincuentes piden un rescate económico por los datos.

Este tipo de amenazas es de las más complicadas en prevenir y gestionar, ya que implica muchos posibles fallos de seguridad diferentes. Por lo tanto, la estrategia en estos casos debe cubrir la seguridad de muchas capas diferentes. Algunas de las medidas de prevención son: una buena concienciación de usuarios para disminuir el riesgo de que ejecuten documentos o programas maliciosos en los PC; un buen filtrado de la navegación y los correos analizando si son confiables y si no bloquearlos; sistemas antimalware avanzados o EDRs (Endpoint Detection and Response) en los sistemas que nos permitan prevenir, pero también responder ante cualquier anomalía; una correcta gestión de vulnerabilidades y parcheado; segmentación de redes; monitorización 24x7 por un SOC (Security Operations Center); una buena gestión de usuarios privilegiados y separar las capas de administración de los sistemas, etc.

Ninguna de estas medidas es infalible y es por eso que se debe incluir también un plan de contingencia y recuperación para, en caso de ser afectados, ser capaces de restablecer el servicio lo antes posible. Se debe disponer de un buen sistema de copias de seguridad que nunca pueda ser afectado por el cifrado de información, y debe haber procedimientos de los pasos a seguir para que la recuperación no tenga fallos y sea lo más rápida posible. Dicho sistema y procedimientos deben ser probados de manera periódica.

## Hacktivismo

Otra de las amenazas es el hacktivismo, que consiste en que por diversos motivos (por ejemplo, un conflicto geopolítico o una causa social) pueda haber interés en afectar negativamente a la seguridad. En estos casos, es muy común que haya grupos que se organicen para tratar de impactar a la disponibilidad de una entidad o varias realizando ataques de denegación de servicio sobre los sistemas de la banca electrónica consiguiendo interrumpir su servicio. Generalmente, consisten en enviar grandes volúmenes de tráfico hacia un sistema o varios, en muchas ocasiones de manera distribuida (desde muchos puntos diferentes en simultaneo), saturando los sistemas o la red de los mismos.

Para este tipo de amenazas es importante tener contratados servicios de inteligencia que nos puedan alertar de si la entidad puede estar siendo objetivo de este tipo de ataques a corto plazo. También se debe disponer de medidas específicas ante los posibles ataques que este tipo de actividades suelen realizar, por ejemplo, medidas de monitorización ante anomalías de tráfico que sean capaces de bloquear el tráfico de los ataques de denegación de servicio. Este tipo de soluciones es recomendable que estén lo más cerca posible del origen, es decir, no únicamente en el CPD de la entidad sino situándolo, por ejemplo, en las líneas de conexión a Internet del proveedor o pudiendo desviar el tráfico a otro proveedor intermedio que realice este servicio de limpieza antes de llegar a la infraestructura de la entidad. De este modo, se evita el riesgo de que la denegación de servicio no se produzca ni por la saturación de los sistemas ni por la saturación del ancho de banda de la línea de internet contratada.

## Vulnerabilidades de seguridad

Las vulnerabilidades de seguridad en los sistemas de información son también una amenaza muy relevante ya que suelen estar implicadas en casi todos los tipos de ciberataques. Suele aprovecharse un fallo de seguridad provocado por una vulnerabilidad, por ejemplo, de un sistema o de una aplicación. Debido al gran volumen de sistemas de información de los que dispone una entidad financiera, es muy complejo y costoso mantener todos los sistemas libres de dichos fallos, ya que la cantidad de nuevas vulnerabilidades que aparecen cada día es muy elevada, y esto se multiplica por el número de activos a proteger. Adicionalmente, se suma el problema de que, a veces, por requerimientos de negocio u operativos, se hace necesario mantener sistemas que ya están fuera de soporte, para los que puede no haber parches de seguridad que solucionen las vulnerabilidades que vayan apareciendo.

Para mitigar el riesgo derivado de estas amenazas se hace necesario tener un procedimiento ágil y robusto de identificación de vulnerabilidades, usando tanto herramientas automáticas que verifiquen la existencia de vulnerabilidades como la contratación de auditorías técnicas de seguridad (pen testing) más exhaustivas. Debido al volumen de vulnerabilidades a gestionar, es muy recomendable disponer de una buena herramienta de gestión integral de todas las vulnerabilidades para controlar que las mismas sean gestionadas adecuadamente en los tiempos establecidos según su riesgo. También se debe disponer de un plan de parcheado periódico, y de obsolescencia para actualizar los sistemas o aplicaciones antes de quedarse fuera de soporte.

## Fraude

El fraude en el sector financiero se basa fundamentalmente en aprovecharse del eslabón más débil de la cadena, que suele ser el usuario final (en este caso, el cliente de la entidad financiera) para obtener un beneficio económico. A través de diversos mecanismos, se busca engañar a los usuarios para que, a través de la banca electrónica u otros canales, faciliten datos privados y credenciales o que directamente autoricen realizar transacciones para sustraerles el dinero de sus cuentas corrientes. Existen muchos métodos; desde el clásico “phishing”, que consiste en enviarle al cliente un enlace con una web fraudulenta que simula ser la de banco, para que este introduzca las claves, a otras como puedan ser las siguientes: smishing, que consiste en lo mismo que el phishing, pero se envía por SMS; vishing, donde el engaño se produce por una llamada de teléfono simulando ser la entidad financiera para conseguir que el cliente de sus datos; SIM-swap, que consiste en solicitar un duplicado de la tarjeta SIM de la víctima sin que este lo autorice, permitiendo al atacante acceder a los mensajes de autenticación que se reciben para autorizar operaciones. También es común utilizar malware instalado en el dispositivo del usuario.

En general, esta amenaza es complicada de mitigar ya que interviene sobre todo la seguridad de los propios clientes y sus conocimientos en materia de prevención. Por lo tanto, es importante implantar una estrategia integral. Tiene que existir la concienciación de los clientes para que estén prevenidos sobre este tipo de engaños y actuar ante estas amenazas, y deben existir suficientes medidas de control que los clientes conozcan y sepan utilizar correctamente. También se debe disponer de medidas de monitorización que puedan detectar transacciones potencialmente sospechosas para bloquearlas antes de que el dinero sea sustraído y no pueda recuperarse..

# La Digitalización:

## *Un enfoque puramente técnico (Parte II)*

**Antonio Moreno Calvo**

Vicepresidente de la Comisión Consultiva de la **AEC**

Presidente del Comité de Metrología del **Instituto de la Ingeniería de España**

**Álvaro Santamaría Enebral**

Vicepresidente de la Comunidad de la Calidad de la **AEC**

Jefe de Calidad de la **Fabrica Nacional de Moneda y Timbre**

www.linkedin.com/in/alvaro-santamaria-enebral-88474243/

**A finales de 2020 presentamos a la AEC una contribución a la Revista Calidad y tuvimos el honor de que fuera publicada en el primer número del año 2021, dedicado a la Digitalización.**

**La contribución se llamaba LA DIGITALIZACIÓN: Un enfoque puramente técnico.**

**Todo lo expresado en esa contribución lo mantenemos. Posteriormente hemos sido conscientes de algún aspecto, entonces no contemplado, y que consideramos interesante difundir.**

En el artículo de 2021 decíamos que la Digitalización es un proceso por el cual se pasa de un mundo analógico (en el sentido de continuo) a otro obtenido por observaciones distanciadas en el tiempo o en el espacio. En el caso de que las observaciones estén distanciadas en el tiempo, se podría entender, de acuerdo a Leonard Susskind (uno de los padres de la teoría de cuerdas), que se trata de observaciones estroboscópicas.

Decíamos que ese era un proceso puramente técnico, y que al obtener una imagen digitalizada del mundo en el que vivimos, teníamos a nuestra disposición una herramienta muy potente.

Herramienta muy potente porque el tratamiento digital de señales permite obtener e inferir resultados que, o no son posibles de obtener a partir de datos analógicos, o su obtención es extremadamente difícil o costosa.

Pues bien, en ocasión de la celebración del Día Mundial de la Metrología de 2022, uno de nosotros fue invitado a acudir al acto conmemorativo en el Centro Español de Metrología.

El acto, como era de esperar, fue extremadamente interesante, pero su narración no es el objeto de este artículo.

Lo que sí fue digno de destacar, desde el punto de vista de esta colaboración, es la explicación que Federico Grasso Toro, doctor Ingeniero, actualmente en el Instituto Nacional de Metrología de Suiza (METAS) dio acerca de la palabra española Digitalización.

Como no podía ser de otra manera, coincidió con nuestras apreciaciones acerca del paso del mundo continuo al mundo cuantificado (no le llamó estroboscópico), y añadió que la palabra "digitalización" también se emplea para referirse a todas las transformaciones o aplicaciones que hacen uso de la imagen digital de la versión real.

Por lo tanto, la palabra digitalización se emplea con dos significados distintos. Este tipo de palabras son llamadas polisémicas, y hay muchas en nuestra lengua.

Un ejemplo, la palabra "falda" puede significar lo que usted está pensando en estos momentos. La RAE, en su acepción 1, la define como: *"Prenda de vestir que cae desde la cintura."*

Pero si usted acude a una carnicería y el cliente previo solicita del dependiente "falda", se está refiriendo a la séptima de las acepciones admitidas por la RAE:
*"En la res, carne que cuelga de las agujas sin asirse a hueso ni costilla."*

En los casos como el del ejemplo de la falda, no puede haber confusión.

En el caso de la palabra digitalización sí hay confusión, porque se refiere a dos aspectos estrechamente relacionados, pero distintos: uno es el origen del otro.

"Digitización" *[palabra que no existe en castellano]* es el proceso por el cual se transforma la información de un formato físico a su versión digital. Por otra parte, la "digitalización" es el uso de la tecnología para mejorar los procesos corporativos. En pocas palabras, digitización se refiera a la información, en tanto que digitalización se refiere a los procesos

En inglés ese problema no existe, porque poseen dos palabras, muy parecidas, pero distintas. Son digitization y digitalization.

Digitization is the process of transforming information from a physical format to a digital version. While digitalization is the practice of utilizing technology to enhance corporate processes. In a nutshell, digitization relates to information, whereas digitalization relates to processes.

Hemos preferido incluir el original en inglés, y a continuación ofrecer nuestra traducción:

"Digitización" [palabra que no existe en castellano] es el proceso por el cual se transforma la información de un formato físico a su versión digital. Por otra parte, la "digitalización" es el uso de la tecnología para mejorar los procesos corporativos. En pocas palabras, digitización se refiera a la información, en tanto que digitalización se refiere a los procesos.

Lo que dejamos en el aire para su debate es si vale la pena instar a la Real Academia Española a que defina dos palabras distintas referidas a los dos conceptos que hemos descrito, o por el contrario, digitalización quede únicamente para referirse a la transformación de la información del mundo físico al de la versión digital. La otra acepción (la de usar la digitalización como herramienta para optimizar procesos) será tan obvia en el futuro, que tal vez nadie tendrá interés ya en referirse a ella y encontrar una palabra que lo defina, de la misma manera que hoy nadie se preocupa por el proceso de martillar, o el concepto de Alta Fidelidad, que han pasado a la historia.

# Calendario de formación AEC



| Formación **En Directo** | | Horas | Ene. | Feb. | Mar. |
|---|---|---|---|---|---|
| **CALIDAD** | | | | | |
| CA | Calidad Mental: Taller de Descubrimiento y Entrenamiento | 10 | 24ene-17feb | | |
| CA | Evaluación y Seguimiento Eficaz de la Calidad de los Proveedores | 12 | 30-31 | | |
| CA | Taller: Herramientas de Transformación Organizacional | 8 | | 6-7 | |
| CA | Taller Especializado en Gestión por Procesos | 8 | | 13-14 | |
| CA | Quality Engagement: Clave de la Gestión de la Calidad | 12 | | 13-14 | |
| CA | Implantación de un SC en Laboratorios de Ensayo y Calibración ISO 17025 | 12 | | 14-16 | |
| CA | 8D: Las 8 Disciplinas. Método de Resolución de Problemas | 4 | | 15 | |
| CA | Gestión del Riesgo | 16 | | 20-22 | |
| CA | Programa Intensivo Industria 4.0. | 24 | | 20-22 | |
| CA | Taller: Implantación ISO 9001 | 16 | | | 1-3 |
| CA | Taller: Gestión del Conocimiento | 12 | | | 1-2 |
| CA | Taller: Gestión Avanzada de Indicadores | 16 | | | 6-7 |
| CA | Taller: Herramientas para Potenciar tu Comunicación Interpersonal | 16 | | | 8-10 |
| CA | Finanzas de la Calidad | 12 | | | 21-23 |
| CA | Liderazgo para Sistemas de Gestión | 16 | | | 22-23 |
| CA | Gestión de la Mejora Continua. PDCA/SDCA | 4 | | | 23 |
| **AUDITORÍAS** | | | | | |
| AU | Auditorías Internas de Sistemas de Gestión Integrados | 24 | 23-26 | | |
| AU | Auditorías Internas de ISO 9001:2015 | 12 | | 6-7 | |
| AU | Implantación y Auditoría de Sistemas de Gestión según ISO 45001 | 12 | | | 13-15 |
| AU | Auditorías Avanzadas en Sistemas de Gestión | 18 | | | 15-17 |
| **LEAN - SEIS SIGMA** | | | | | |
| 6S | Introducción a Seis Sigma | 8 | 25-26 | | |
| **EXPERIENCIA DE CLIENTE** | | | | | |
| CX | Digital Customer Experience | 8 | | 2 | |
| CX | Métricas Customer Experience y Voz del Cliente | 12 | | 15-17 | |
| **INNOVACIÓN** | | | | | |
| INN | Design Thinking | 10 | | 9 | |
| INN | Lean Startup | 8 | | | 8 |
| **PECAL** | | | | | |
| PE | APQP para el Sector Industrial | 16 | | | 6-8 |
| PE | Claves para la Realización de Auditorías Internas PECAL/AQAP | 8 | | | 28-29 |
| **AEROESPACIAL** | | | | | |
| AE | Diseño e Implantación de Norma EN 9100:2018 | 12 | | 1-3 | |
| **PREVENCIÓN DE RIESGOS LABORALES** | | | | | |
| PRL | Taller: Legislación de Prevención de Riesgos Laborales | 12 | | 13-15 | |
| **MEDIO AMBIENTE** | | | | | |
| MA | Claves de la nueva Ley de Residuos | 4 | 31 | | 17 |
| MA | Taller: Cálculo de la Huella de Carbono | 12 | | 7-9 | |
| MA | Taller: Autoevaluación del Cumplimiento del Principio DNSH | 4 | | 16 | |
| MA | Taller: Economía Circular y Residuo Cero | 16 | | 22-24 | |
| MA | Principales Claves para la Elaboración de Planes de Descarbonización | 4 | | | 7 |
| MA | Taller: Legislación Ambiental | 12 | | | 8-10 |
| MA | Taller: Cálculo de la Huella Hídrica | 12 | | | 14-16 |
| MA | Taller: Análisis Ciclo de Vida | 12 | | | 21-23 |
| MA | Taller: Implantación de Sistemas de Gestión Energética ISO 50001 | 12 | | | 27-29 |
| **RESPONSABILIDAD SOCIAL** | | | | | |
| RS | ODS en la Estrategia Empresarial | 8 | 30-31 | | |
| RS | Información no Financiera y Memorias de Sostenibilidad GRI | 12 | | 1-3 | |
| RS | Taller: Implantación de Planes de Igualdad | 12 | | 7-9 | |
| RS | Finanzas e Inversiones Sostenibles | 8 | | | 9-10 |

Puede acceder al listado completo de cursos a través de nuestra web:

## Formación **En Directo**

| | | Horas | Ene. | Feb. | Mar. |
|---|---|---|---|---|---|
| **SEGURIDAD ALIMENTARIA** | | | | | |
| SA | El estándar BRC V.9. Principales cambios | 8 | 26-27 | | |
| SA | Taller: Implantación de un Sistema de Inocuidad según ISO 22000 | 8 | | 9-10 | |
| SA | Taller: Implantación de un Sistema Food Defense | 8 | | 23-24 | |
| SA | Taller: Medición de la Cultura de Inocuidad Alimentaria | 8 | | | 21-22 |
| **PROTECCIÓN DE DATOS DPD/DPO** | | | | | |
| PD | Taller: Implantación de ISO 27001 | 12 | 30-31 | | 27-28 |
| PD | Taller: Implantación del Esquema Nacional de Seguridad (ENS) | 12 | | 21-23 | |
| PD | Taller: Análisis de Riesgos y EIPD | 8 | | | 21- 22 |

## Formación **Online**

| | | Horas | Meses |
|---|---|---|---|
| CA | Introducción al Software Estadístico R | 50 | 24ene-17mar |
| CA | Implantación de Sistemas de Gestión de Calidad ISO 9001:2015 | 50 | 27ene-17mar |
| CA | Estadística Práctica Aplicada a la Calidad | 50 | 30ene-14abr |
| CA | Técnico en Gestión de Calidad | 80 | 31ene-19may |
| CA | Experto Europeo en Gestión de la Calidad | 150 | 16feb-26jul |
| CA | Auditorías de Sistemas de Gestión | 50 | 6mar-25abr |
| CA | Gestión por Procesos | 120 | 9mar-30jun |
| CA | Gestión de Riesgos Empresariales | 120 | 16mar-30jun |
| 6S | Lean Seis Sigma Green Belt | 150 | 23feb-30may |
| CX | Experto en Customer Experience Management | 120 | 23feb-28jun |
| RS | Experto Europeo en Sostenibilidad y Responsabilidad Social | 120 | 22feb-14jul |
| MA | Experto Europeo en Gestión Ambiental | 150 | 15feb-26jul |
| MA | Implantación de Sistemas de Gestión Ambiental ISO 14001:2015 | 50 | 27feb-19abr |
| MA | Experto en Gestión y Sostenibilidad Energética | 100 | 28mar-28jul |
| INN | Experto en Gestión de la Innovación | 120 | 22mar-30jun |
| SA | Experto Europeo en Seguridad Alimentaria | 120 | 24feb-14jul |
| PD | Programa Avanzado Delegado de Protección de Datos | 104 | 23ene-11may / 23mar-28jul |
| PD | Procedimiento Sancionador en Protección de Datos | 30 | 31ene-3mar |
| PD | Protección de Datos y Seguridad en IoT, Big Data e IA | 40 | 9feb-24mar |
| PD | Protección de Datos y Relaciones Laborales | 60 | 15feb-21abr |
| PD | ENS e ISO 27001 para Cumplir con el RGPD | 60 | 16feb-28abr |
| PD | Programa Superior Delegado de Protección de Datos | 200 | 22feb-28jul |
| PD | Publicidad Digital y Protección de Datos | 40 | 14mar-21abr |
| PD | Requisitos para Implantar SG ISO/IEC 27701:2019 | 25 | 16mar-28abr |
| PD | Protección de Datos en el Sector Educativo | 60 | 21mar-12may |
| PD | Análisis de Datos para la Toma de Decisiones | 50 | 23mar-28abr |

## Formación **Mixta**

| | | Horas | Meses |
|---|---|---|---|
| CA | Programa Superior Quality Manager | 200 | 16feb-26jul |
| CA | Programa Superior de Auditores Sistemas de Gestión | 90 | 6mar-25abr |
| MA | Programa Superior Manager en Gestión Ambiental | 200 | 15feb-26jul |

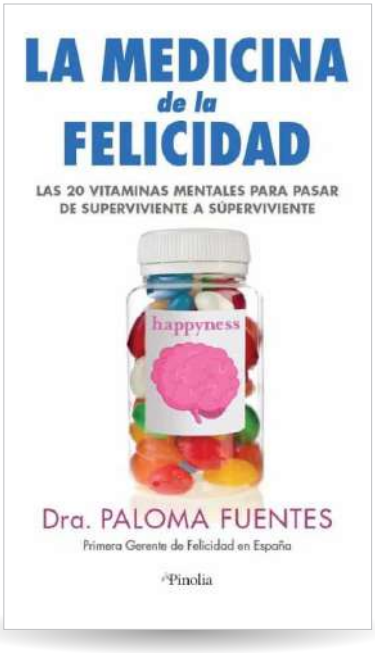


Cursos bonificables a través de la **Fundación Estatal para la Formación en el Empleo**

Desde la AEC gestionamos los trámites necesarios para la bonificación a través de la Fundación Estatal para la Formación en el Empleo sin ningún coste adicional a todas las empresas que lo soliciten y realicen la formación con nosotros.

Contacta con el Centro de Formación AEC
for@aec.es
Tel. 912 108 120

## LA MEDICINA DE LA FELICIDAD




**LA DOCTORA PALOMA FUENTES SE DEFINE COMO «HAPPYTÓLOGA», ES DECIR, ESPECIALISTA EN FELICIDAD.** Ha desarrollado la mayor parte de su trayectoria profesional en la empresa Mahou-San Miguel, como Responsable Médico del área de alta dirección y posteriormente como gerente de felicidad, siendo la primera persona en ocupar este puesto en una gran organización española. Conferenciante internacional, Directora del primer Master Universitario de Felicidad Individual y Organizacional (INDORG). Creadora del Modelo HAPPYNET® y cocreadora del CHEF®, cuestionario de Habilidades Especificas de Felicidad. Sus propuestas y experiencia la han convertido en una experta mundial en Felicidad Organizacional, un concepto que va un paso más allá de la Salud Laboral y la Psicosociología.

Su libro aborda la salud como el pilar sobre el que edificamos nuestras vidas. Sí, sabemos que este pilar se construye día a día con los alimentos, el ejercicio físico y el descanso, pero también con nuestros pensamientos, nuestras emociones, nuestras palabras y la red de afectos que tejemos a nuestro alrededor. Los avances científicos demuestran que el cerebro y la mente son los dos elementos básicos sobre los que construimos nuestra salud. Y solo contando con una energía biológica excepcional podemos fortalecer estos dos elementos, mejorar nuestro vigor y resistencia y aumentar nuestra creatividad para poder alcanzar nuestras metas personales y profesionales. Esa energía biológica es la Felicidad. Este libro te aproxima a una nueva forma de entender la salud y la felicidad. A través del cuidado de nuestro cerebro y nuestra mente, embárcate en un apasionante viaje personal y conoce las 20 vitaminas extraordinarias con las que podrás edificar tu vida con Salud y Felicidad.

**Autoría:** Dra. Paloma Fuentes • **Edita:** PINOLIA • **Idioma:** CASTELLANO

## LA FÁBRICA DE LA EXPERIENCIA.
### Nuevas fórmulas para convertir la experiencia de cliente en algo memorable


**TRAS EL ÉXITO COSECHADO POR "LA FÁBRICA DE LA EXPERIENCIA. MANUAL DE COMBATE EN 100 REFLEXIONES PARA DISEÑAR O MEJORAR LA EXPERIENCIA DEL CLIENTE", SANTIAGO MUÑOZ-CHÁPULI HA VUELTO A PUBLICAR Y ESTA VEZ HA CONTADO CON LA COLABORACIÓN DE LA PRESIDENTA DE LA ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD, BEATRIZ LÓPEZ GIL, ENCARGADA DEL PRÓLOGO DE LA PUBLICACIÓN.**

En este segundo volumen llega la Fábrica de la Experiencia más actualizada y ampliada, donde encontrarás nuevas fórmulas, conceptos y conocimientos ligados a sus 10 dimensiones. ¿Quieres lograr que tu equipo se ponga la camiseta? ¿Quieres mejorar la experiencia de tus clientes y que se sientan VIP? ¿Quieres implantar tecnología en tu centro de contacto? ¿Cómo puedo monitorizar y medir la calidad? ¿Cómo elegir el gráfico adecuado para nuestros datos? Estos títulos y muchos más los encontrarás en esta segunda parte.

Además, nos presentan a nuevos expertos que han colaborado y contribuido en la creación de artículos, manuales, guías basadas en sus experiencias reales y llenas de conocimiento, que nos harán saltar de una dimensión a otra. Todos ellos con entusiasmo. compromiso y rigor, valores compartidos por el equipo, para seguir ayudando a diseñar, construir, diagnosticar o mejorar las operaciones de clientes, mientras se esfuerzan por conseguir experiencias memorables.

Descubre y disfruta de las dimensiones actualizadas de la Fábrica de la Experiencia de la mano de Santiago Muñoz-Chápuli, David Rodríguez Francisco, Ángel Martínez, Alex Esclamado, José Enrique Borrego, Antonio Negrón, Montse Serrano, Julia Lozano, Modest García, José María León, Ivan Borisov, Carina Bencomo, Caterina Di Marco y Yolanda Muñoz.

**Autoría:** Beatriz Felipe Pérez • **Edita:** CIRCULO ROJO • **Idioma:** CASTELLANO

# FORMACIÓN PARA EMPRESAS

AEC incompany

**Pensamos en tu equipo para impulsar el crecimiento de tu empresa**

Analizamos las necesidades de tu empresa para **diseñar programas a medida** que aseguren el cumplimiento de tus objetivos a través del **desarrollo de habilidades** en las personas y **mejoras en los procesos** de tu organización.

**Adaptamos todo nuestro catálogo a tu empresa** y creamos acciones formativas especializadas y exclusivas con especialistas de reconocido prestigio.

## Dinos qué necesitas y nosotros, juntos, diseñamos tu curso

## Lleva a tu empresa al siguiente nivel

Más información: incompany@aec.es | Teléfono: 912 108 122 | www.aec.es

Protección de Datos by AEC

# Delegado de Protección de Datos: la profesión del futuro

## Nuestra diferencia

**Profesorado referente:**
expertos en activo para potenciar el aprendizaje.

**Experiencia online innovadora:**
clases online impartidas por los expertos.

**Foros de alto valor y networking:**
oportunidad de intercambiar experiencias y resolver dudas.

**Contenidos y casos prácticos**
de aplicación inmediata al perfil del DPD.

**Simulador para preparar la certificación:**
+300 preguntas para practicar y consolidar conocimiento.

**Más de 1.000 profesionales DPD han confiado en la AEC**

**¡Elige tu formación e impulsa tu carrera!**