NEWS

JUNIO 2023

# CLICK CIBER

## PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS, EL GRAN DESAFÍO

## DIGITALIZACIÓN DEL SECTOR INDUSTRIAL Y ENERGÉTICO: SUS RIESGOS

## IA EN OT

## ¿LA NUBE PUEDE SER OT?

## ATAQUES A LA CUARTA REVOLUCIÓN INDUSTRIAL

## ¿Credenciales comprometidas?

**50 millones**
de ataques a contraseñas cada **DÍA**

**580 / SEGUNDO**

## ¿Mala experiencia de usuario?

**60%**
DE VIOLACIONES DE DATOS

**x credenciales COMPROMETIDAS**

**Los sistemas de autentificación basados en contraseña y doble factor se han quedado obsoletos. Las tecnologías de inteligencia artificial mejoran la verificación de la identidad, optimizando la experiencia del usuario y multiplicando su seguridad.**

GRUPO TRC
DEPARTAMENTO DE CIBERSEGURIDAD

MONITORIZACIÓN DE AMENAZAS
DETECCIÓN Y RESPUESTA ANTE CIBERAMENAZAS
TECNOLOGÍA TESTADA EN NUESTRO CYBERLAB

www.grupotrc.com

arculix by SECUREAUTH

**Autenticación multifactor invisible e inteligente**

Más información: omikhaylov@secureauth.com
608747971

# EQUIPO


**DIRECTOR**
Carlos Lillo

**SUBDIRECTOR**
Carlos Valerdi

**REDACTOR JEFE**
Javier Lillo

**DIRECTORA DE DISEÑO EDITORIAL**
Blanca Martín

**EDITOR / COORDINACIÓN**
Javier Lillo

**DIRECTORA DE ARTE**
Fernanda Lago

**ILUSTRACIÓN PORTADAS Y LOGO**
Angelo Cataldo


# COLABORADORES

AGUSTÍN VALENCIA
ALFONSO CALVO
CAYETANO DE JUAN
CÉSAR RODRÍGUEZ
CLAUDIO CARACCIOLO
JOAN MASSANET
JOSÉ MIGUEL PAREJO

JUAN BERGA
LORENA GONZÁLEZ
PABLO ALARCÓN
RAFA TORTAJADA
RAÚL GUILLÉN
SANTIAGO INGOLD
XAVI BERTOMEU

# INDÍCE

TREND MICRO™ | Global Leader in Cybersecurity

# Experimente el poder de una plataforma de ciberseguridad unificada

Comprenda, comunique y mitigue mejor los riesgos cibernéticos de su empresa con Trend One.

Contacto

trendmicro.es

News

# ClickCiber

# EDITORIAL

CARLOS Lillo

# Orgullo y Tormenta.

Hoy toca volver a sacar pecho, y por varios motivos. Se cumple estos días un año desde que fuimos galardonados con una Antena de Plata a nuestro programa de radio por parte de la Federación de Profesionales de Radio y TV, tesoro que compartimos con nuestros oyentes de ambos lados del Océano Atlántico, puesto que, desde aquella ceremonia en el Paraninfo de la Universidad de Alcalá, nuestro programa ha dado un estirón, emitiéndose ya a través de 122 medios de Radio y TV repartidos entre 11 países. Desde luego la tecnología importa, y algo debemos hacer bien cuando la audiencia secunda aquella Antena de Plata tan presente.

Entre el anterior número de marzo y este, ha alboreado El Centinela de Red, una publicación que liberamos los domingos a modo de una hoja parroquial en la que recogemos recortes de prensa del sector, documentándolos con los correspondientes enlaces a la noticia original.

En cuanto a este número que ahora tienes, el hilo conductor es el mundo industrial, que no se reduce a la fabricación de bienes, ya que muchas organizaciones privadas y públicas tienen equipos industriales, como son plantas robotizadas de logística que complementan a las factorías propiamente llamadas.

Estos sistemas industriales (OT) son objeto de una casuística muy compleja ya que deben estar funcionando siempre: una parada de 15 minutos en una cadena de producción puede ser catastrófica con consecuencias económicas muy relevantes. Es decir, la disponibilidad es el criterio decisivo.

Sin embargo, la disponibilidad ya no se puede ver aislada del entorno actual en el que los ciberataques son cada vez más persistentes y el mundo OT es objetivo primario; un ciberataque exitoso puede detener una planta y pedir un rescate para liberar sus efectos. En este contexto, los CIO y CISO añaden una preocupación a las habituales de los sistemas IT, con la complejidad añadida de que en muchos casos los mundos OT e IT -y sus responsables- han vivido en mundos paralelos con recelos entre ambos. Es la tormenta perfecta.

Esperamos que la presente edición de la revista sirva para dar algo de luz. Para ello hemos contado con colaboraciones que llenan de orgullo a este director.


CLICKCIBER
JULIO 2020
Nº 1
ESTEGANOGRAFÍA.
EL ARTE DE OCULTAR LA INFORMACIÓN
CIBERSEGUROS
por qué son tan importantes para las empresas
¿Hola SASE!
Fake News
UNA AMENAZA MUY REAL
LA CIBER SEGURIDAD EN LA CLOUD
IDENTIFICACIÓN DE SAAS A TRAVÉS DE MÓVILES
ANÁLISIS DE UN ATAQUE Ransomware


CLICKCIBER
Septiembre 2020
Nº 2
Evitar el fraude en el correo electrónico con DMARC
LA NUEVA ERA DE LA SEGURIDAD EN LA NAVEGACIÓN WEB Y SAAS
JUEGOS DE GUERRA
Analizamos este thriller de ciencia ficción que pone en cuestión si las máquinas deberían tener autonomía para tomar decisiones.
Entrevista A
PEDRO PABLO PÉREZ
CEO BUSINESS SECURITY UNIT EN TELEFÓNICA
ÍNDICE CLICKCIBER NGFW 2020
¿Cuáles son los fabricantes de Next Generation Firewalls (NGFW) mejor valorados?

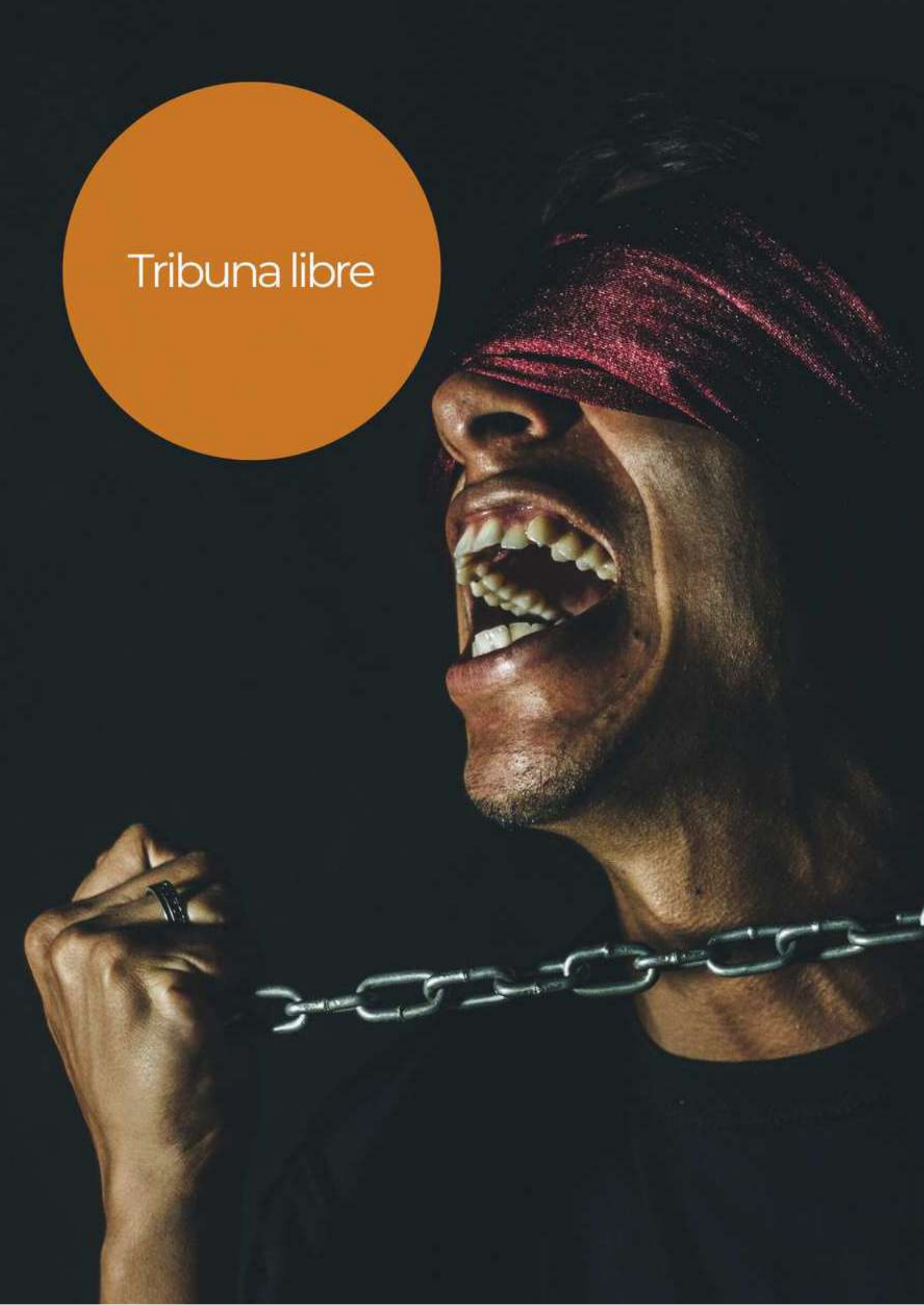

WHAT YOU NEED TO STarT A POdCast

MEDIGATE
by Claroty

# Securing XIoT for Healthcare

*Ingecom*

# Tribuna libre



Creación de contenidos, redacción, cronista. Participante en ClicktertuliaTV desde 2015. Redactor Jefe en Estrella Digital entre 2015 y 2008. Y anteriormente, ha ocupado cargos como asesoría y consultoría en desarrollo de proyectos en comunicación, organización eventos y diseño de contenidos, y asesoría en desarrollo medios de comunicación digitales, entre otros.

# IA: es la verdad, amigos y amigas, es la verdad

JUAN BERGA

IA ia Ai Ia iA ia

# EN REALIDAD, EL RIESGO VA MÁS ALLÁ

La amenaza es que aumenta la posibilidad de crear imágenes falsas

A final del siglo pasado (1995), Jeremy Rifkin escribió: “El fin del trabajo. El declive de la fuerza del trabajo global y el nacimiento de la era posmercado”. Argüía que una Tercera Revolución Industrial acabaría con el trabajo tal y como lo habíamos conocido.

Si hace 28 años, el libro parecía imaginar un futuro inquietante, calculen lo que ocurriría ahora, cuando los riesgos sobre el empleo producido por la Inteligencia Artificial (IA) es ya el presente.

Como ya les he dicho en algún sitio,

sospecho que lo que hoy llamamos "inteligencia artificial" no es ni artificial ni inteligente.

Los primeros sistemas de IA estaban fuertemente dominados por reglas y programas, por lo que al menos estaba justificado hablar de "artificialidad".

Pero los de hoy, extraen su contenido del trabajo de humanos reales: artistas, músicos, programadores y escritores cuya producción creativa y profesional ahora se apropia en nombre de salvar la civilización.

En cuanto a la parte de "inteligencia", la fuerza de la IA moderna radica en la coincidencia de patrones. No es de extrañar dado que uno de los primeros usos militares de las redes neuronales, fue detectar barcos en fotografías aéreas.

Boris Eldagsen, fotógrafo alemán de 52 años, ha hecho público que ganó el premio de fotografía de Sony con una imagen generada por IA.

Si no se puede distinguir la diferencia entre una fotografía y una imagen generada por IA, entonces todo tipo de creación, ese momento en que el ser humano compite con un dios, desaparece.

En realidad, el riesgo va más allá: el verdadero desafío que presenta la IA no es que pueda sacudir nuestro apego a la creatividad humana como algo único e insondable, ni siquiera que pueda destruir puestos de trabajo y, potencialmente, industrias enteras – especialmente en el mundo de la comunicación-.

La amenaza es que aumenta la posibilidad de crear imágenes falsas y falsas verdades. El pánico es, en última instancia, que la realidad va a ser una mezcla de verdad, alucinaciones (así es como lo llaman cuando la máquina hace algo extraño) y deliberadamente no - verdad. Propaganda utilizada para entregar un mensaje singular, con exclusión de otros mensajes.

El propio director ejecutivo de Google ha dicho que “ las preocupaciones sobre la inteligencia artificial lo mantienen despierto por la noche y que la tecnología puede ser "muy dañina" si se implementa incorrectamente”.

Sundar Pichai también pidió un marco regulatorio global para la IA, similar a los tratados utilizados para regular el uso de armas nucleares, ya que, advirtió, “la competencia para producir avances en la tecnología podría dejar de lado las preocupaciones sobre la seguridad”.

La moratoria investigadora propuesta por Elon Musk o Zuckerberg tiene pinta más de batalla comercial que de preocupación por el riesgo sobre la verdad, conociendo a sus autores. Tampoco la prohibición resuelve nada, como puede observarse en tantas materias.

La regulación puede ser un camino, al menos en las realidades democráticas a las que deseamos pertenecer.

Parece haber un desajuste entre el ritmo al que la sociedad piensa y se adapta al cambio en comparación con el ritmo al que evoluciona la IA.

La única ventaja es que, al menos, estamos más alerta que en otras ocasiones sobre sus peligros potenciales. En comparación con las tecnologías a las que se refería, en 1995, Rifkin, hay más gente preocupada por la nueva al principio de su ciclo de vida.

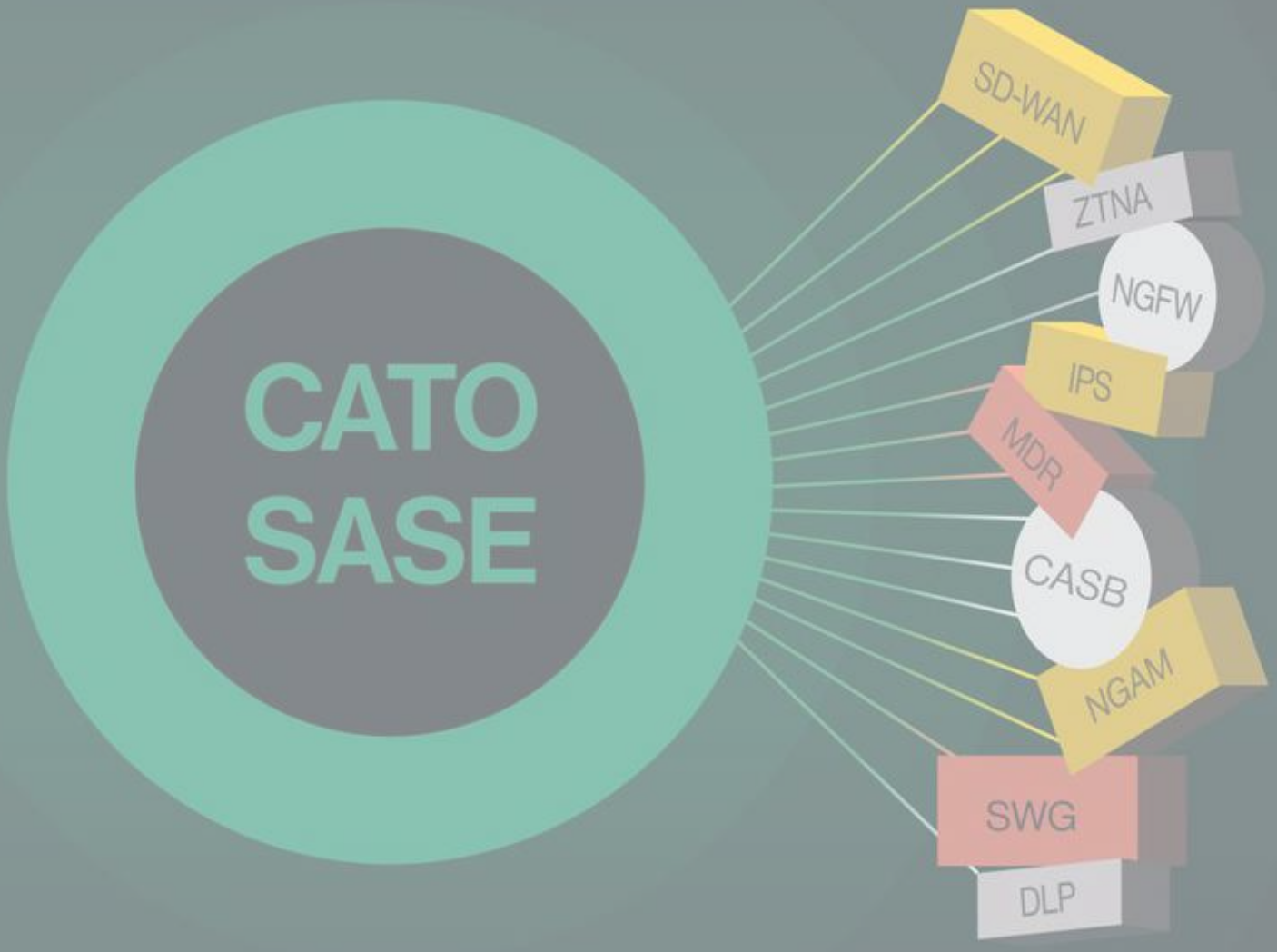
No obstante, esa preocupación no nos hace estar, necesariamente, más protegidos. No solo la velocidad de crecimiento es tan exponencial que no es aprehensible; que sectores productivos enteros se vean condenados no ya a jornadas de cuatro días sino a la ausencia de jornada y rentas mínimas. No solo es la seguridad.

Ahora se trata de la verdad. En el guasap de la revista que generosamente acoge algunas de mis crónicas, Joan Massanet se hacía la pregunta transcendental: era sobre la ética y la inteligencia artificial. Me sumo a su reflexión: es la verdad, amigos y amigas, es la verdad.

CATO
NETWORKS

# Ready for Whatever's Next

## SASE, SSE, ZTNA, SD-WAN:
## Your journey, your way.



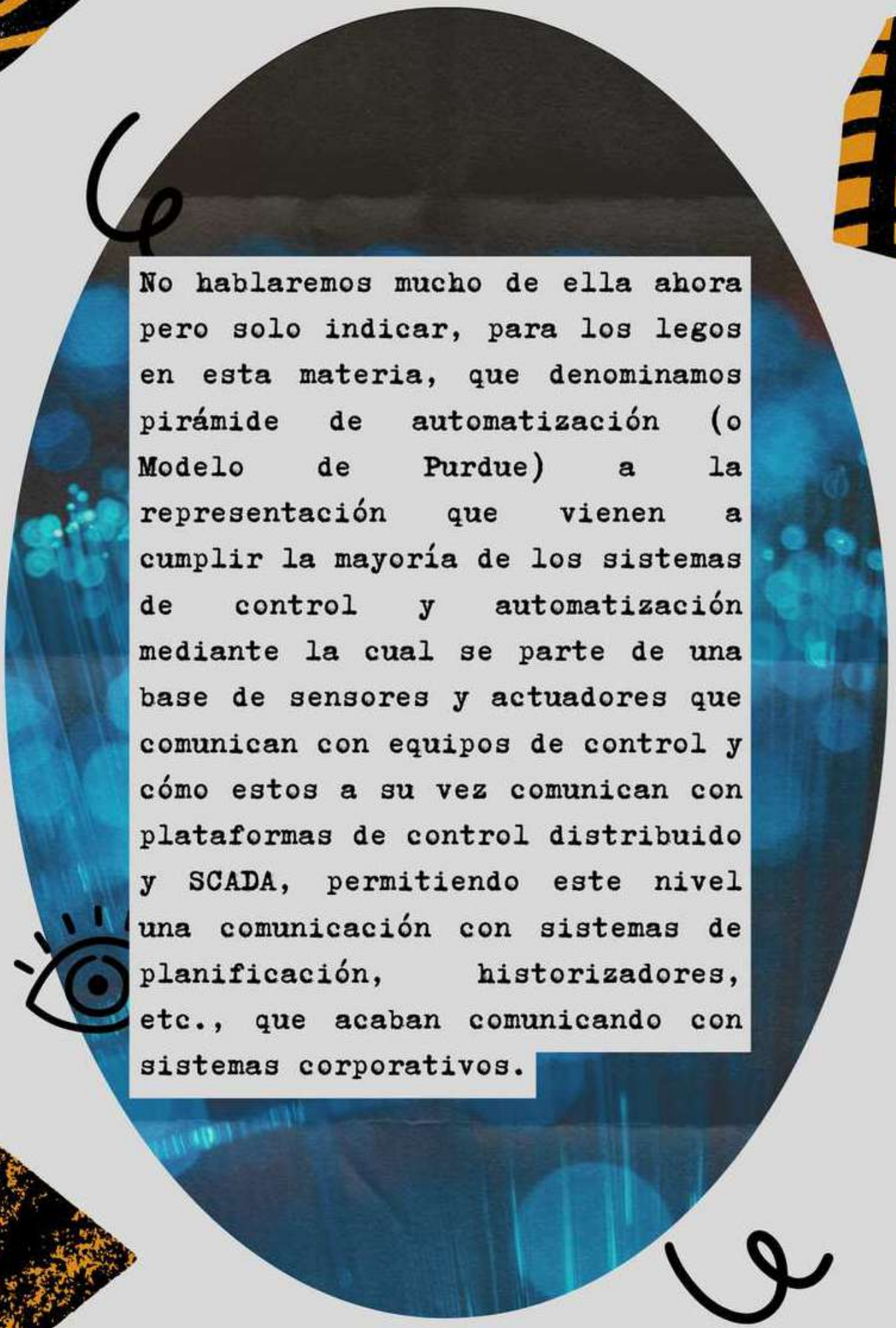

www.catonetworks.com

# En Profundidad

Ingeniero Industrial por ICAI y Máster en Ciberseguridad por UPC-ViU. Lleva 20 años vinculado al mundo de la energía desde todos susámbitos y a la ciberseguridad desde 2012. Es buen conocedor de lasinstalaciones críticas, sus tecnologías, entornos y regulaciones.Dedica su tiempo libre a su mujer y a sus hijos, lo que le tiene muyentretenido, aunque siempre le queda algún hueco para impartiralguna clase, dar alguna charla o ir de acampada

# ¿LA NUBE PUEDE SER OT?

Tradicionalmente se ha escrito mucho sobre la pirámide de automatización y cómo hay una gran frontera entre el mundo IT y el mundo OT.



No hablaremos mucho de ella ahora pero solo indicar, para los legos en esta materia, que denominamos pirámide de automatización (o Modelo de Purdue) a la representación que vienen a cumplir la mayoría de los sistemas de control y automatización mediante la cual se parte de una base de sensores y actuadores que comunican con equipos de control y cómo estos a su vez comunican con plataformas de control distribuido y SCADA, permitiendo este nivel una comunicación con sistemas de planificación, historizadores, etc., que acaban comunicando con sistemas corporativos.

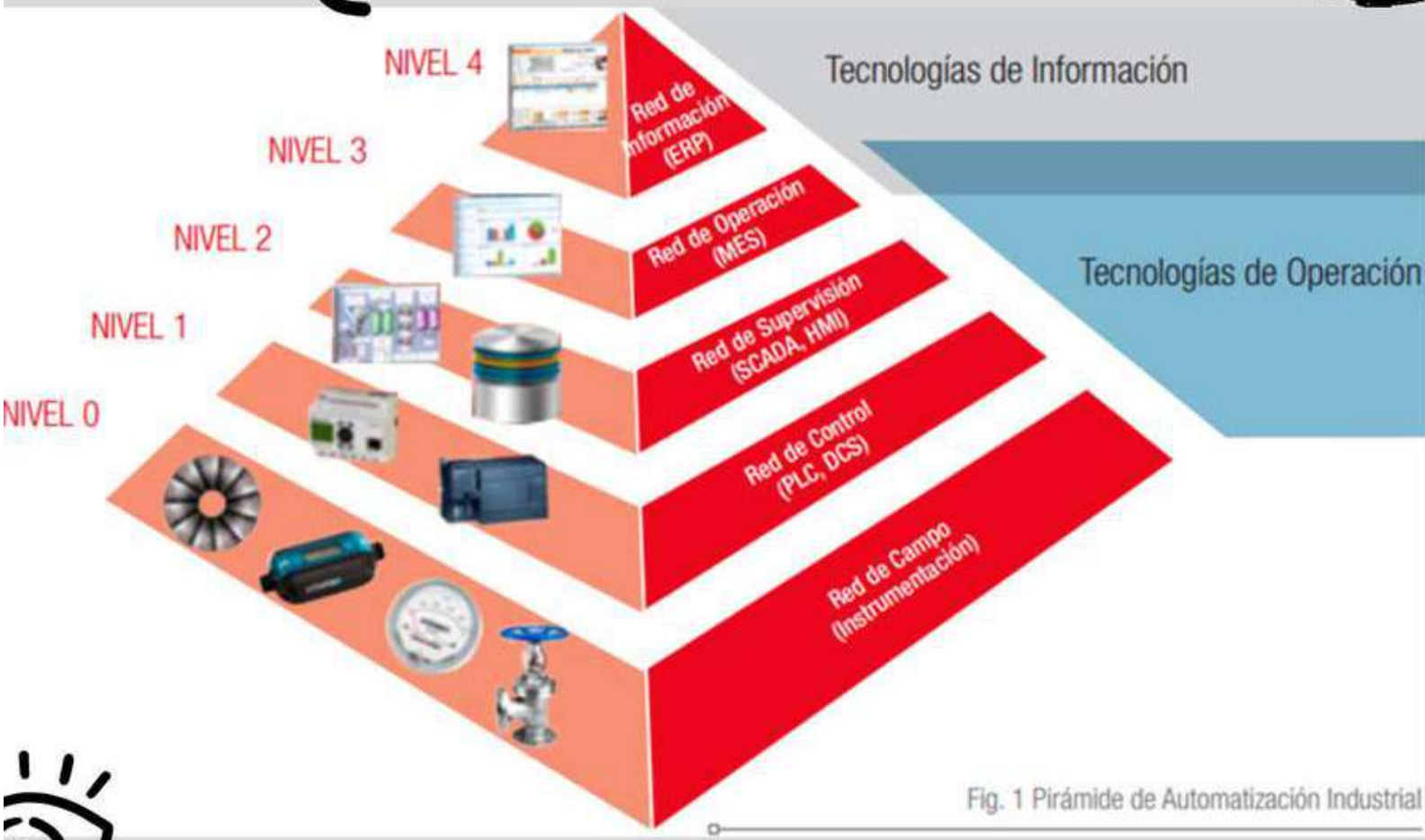



Fig. 1 Pirámide de Automatización Industrial

Hay algunos aspectos como son el enfoque hacia la disponibilidad frente al de la confidencialidad, el tratamiento de los protocolos industriales para comunicación con las máquinas, el análisis del impacto de las comunicaciones en aspectos como la latencia que, junto a algunos requisitos fundamentales de la normativa industrial, trataremos de abordar en este artículo.

Lo cierto es que el mundo industrial se está acelerando, quizás no a la velocidad que a muchos les gustaría, pero también lo está haciendo en un número de dimensiones que permiten pensar en entornos muy distintos a los actuales en no demasiado tiempo.

En mi caso particular, si hace 10 años me hubieran dicho de ver un SCADA en la nube, seguramente no me lo habría creído ni habría dedicado muchos minutos a discutir sobre tema por lo inverosímil que me hubiere parecido.

Pero no vayamos directamente a algo como el control desde la nube sino que, les propongo abordar varios pasos antes que nos ayudarán a entender el camino que ya estamos recorriendo.

Empecemos por el concepto de la virtualización, por el que podemos aprovechar un mismo hardware para alojar distintas máquinas virtuales, y cada una consumiendo una cantidad determinada de recursos. En muchos entornos ha sido esta precisamente la vía que han encontrado muchas instalaciones para alargar la vida de sus sistemas obsoletos de manera compatible con los nuevos equipos. De esta manera, un servidor con varios núcleos, funcionando en 64bits y con un sistema operativo moderno, nos permitía alojar una máquina virtual de un sistema Windows de 32bits y poder montar sobre él un SCADA y un MES.

Las capacidades de comunicación y de procesado de estos equipos y de las redes de planta actuales disiparon rápidamente cualquier duda sobre compatibilidad, añadiendo además capacidades extra de redundancia y alta disponibilidad.

Pero podemos ir a casos más modernos y a más bajo nivel de la pirámide; recientemente ha sido Siemens quien acaba de anunciar la virtualización de sus PLCs, pero otros competidores como Honeywell ya ofrecen su plataforma Hive, de manera que se puede elegir, entre un conjunto de controladores, qué procesos y cargar en qué controladores como principal y en cuáles como secundario, de modo que el programa ya no es algo que resida en un único controlador y la computación se independiza de la capa de señales de campo.

Y de los controladores al concepto del IoT; equipos muy sencillos, generalmente para toma de datos, que albergaban varios sensores, una placa base muy barata (generalmente derivado de Arduino o Raspberry) con una conectividad a internet. Hay que decir que cada vez es más normal poner prefijos al IoT para diferenciarlos de equipos ya masivos como los smartwatch o los altavoces inteligentes como Google Nest o Amazon echo. Esto nos ha devenido, además, en construcciones adaptadas a entornos específicos. Hablamos de IIoT (Industrial IoT), de MIoT (Medical IoT) y, para generalizar pero sin mezclar, xIoT. Por cierto, muchos de estos ya nos los encontramos con multitud de aplicaciones para proyectos de Smart Cities o de Edificios Inteligentes.

Forcepoint

# Welcome to the power of ONE

Forcepoint ONE

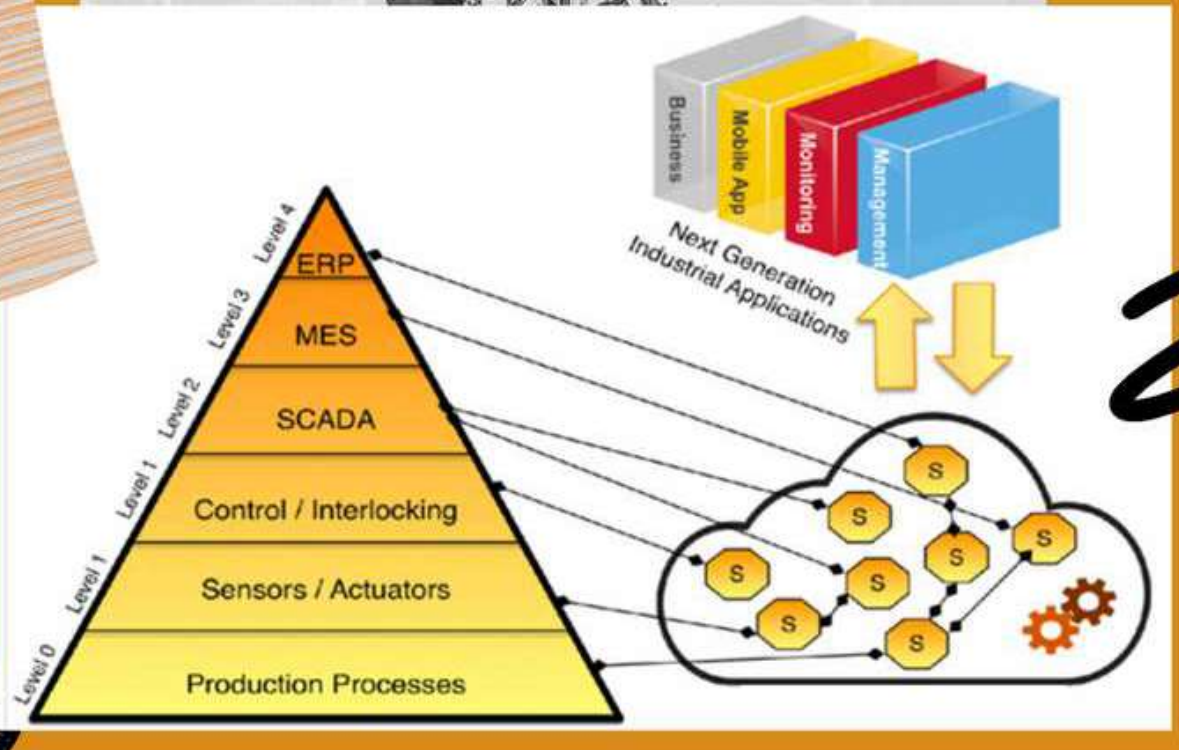
ONE Platform
ONE Console
ONE Agent

www.forcepoint.com

Con este tipo de dispositivos se ha acelerado la adopción de entornos Cloud en los que poder llevar datos de manera masiva y aprovechar sus capacidades de computación y escalado. Tenemos muchísimas aplicaciones de Google Cloud, Amazon (AWS) o Microsoft (Azure) en las que actualmente podemos disfrutar “en tiempo real” de información que muchos usuarios comparten con una experiencia de usuario fabulosa.
Dicho todo esto, ¿es suficiente para convencernos? Quizás en parte, porque ya hay una cantidad de proyectos para entornos industriales y de smartbuildings con casos de uso basados en xIoT.
En industria vemos muchos casos de sensórica de vibraciones que permite hacer diagnósticos avanzados de los equipos sujetos de desgaste dinámico y, por tanto, predecir y evitar paradas forzadas por averías, pero también en otros casos, alargar intervalos de mantenimiento hasta que se tengan un diagnóstico que lo requiera.

En Smartbuildings es muy común buscar optimizar el consumo energético, tanto a nivel de aire acondicionado, calefacción y ventilación (HVAC) como de iluminación analizando el uso de las plantas y las salas de los edificios gracias a sensores de temperatura, luz o movimiento.
Lo cierto es que podríamos hablar de otros ejemplos en logística, movilidad o medicina y todos nos llevan a un mismo punto, sensores que se conectan a internet y que condicionan el funcionamiento de nuestros sistemas de control y automatización.

De hecho, esta cuestión es la que emplean algunos para decir que la pirámide de automatización está obsoleta, precisamente por las infinitas capacidades de conectividad que permiten las nuevas tecnologías, tanto a nivel de equipos como de los propios entornos de comunicaciones.



Sin querer parecer un purista, valga la opinión de un humilde escribiente para asegurar lo contrario, pero estableciendo una matización importante: el modelo de Purdue puede que, en el pasado, tuviera una base material por cuanto los tipos de comunicación y conectividad condicionaban qué podía hablarse con qué, sin embargo, también establece una jerarquía que permite entender cómo los equipos y los sistemas funcionan. Por cierto, en dicha jerarquía, la nube no se debe pintar en la cúspide de la pirámide sino como un nivel al lado de cada uno de estos niveles y que, internamente, deberá respetar similares principios, como veremos después.

Es decir, la pirámide de automatización establece una relación jerárquica sin la cual, será imposible hacer diagnósticos de averías en sistemas complejos. Y es por esto que las nuevas normas ya consideran propuestas de despliegues de sistemas IIoT coherentes con el resto de sistemas en planta para asegurar que los nuevos sistemas mantienen esta jerarquía, como ya adelantaba NIST en su draft de la 800-82 rev.3

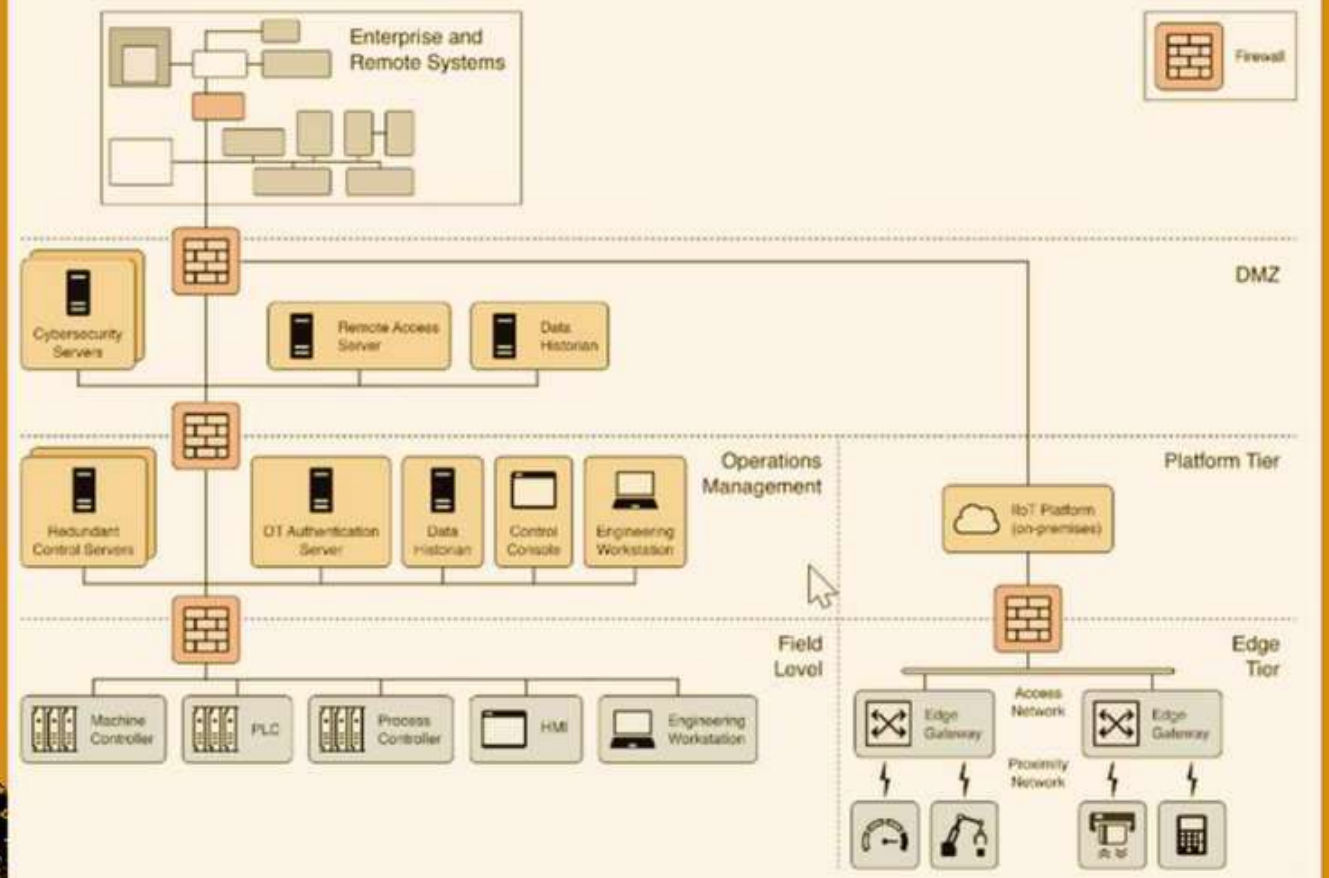



**Figure 19: Security architecture example for DCS system with IIoT devices**

Ya tenemos aplicaciones que están yendo a la nube, que nos están ofreciendo modelos predictivos o cálculos de eficiencia que nos mandan consignas al campo para operar de acuerdo a los escenarios resultado de sus cálculos. También encontramos sistemas de ejecución de fabricación (MES), cuyos modelos analíticos también empiezan a migrar... así que, ¡vayamos ya a la nube!

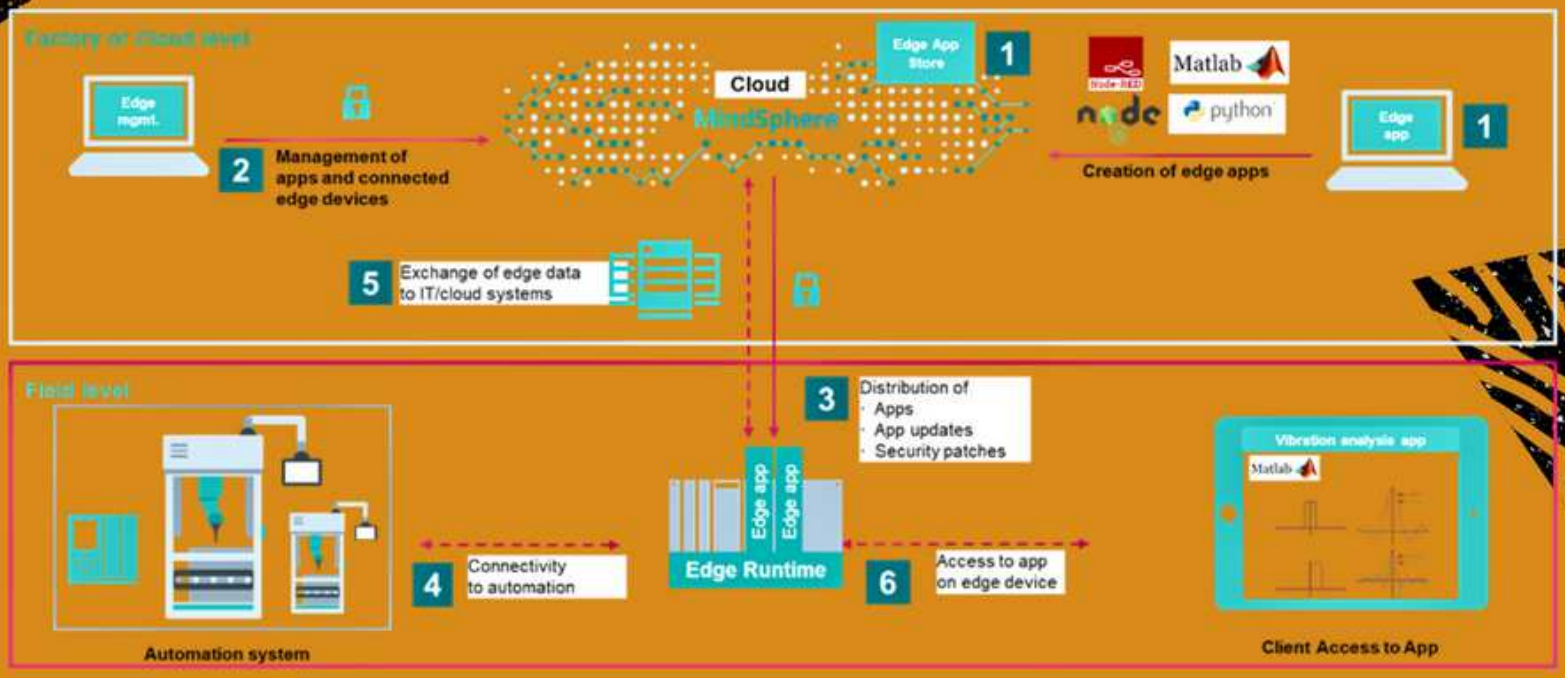
Uno de los temores clásicos con la nube es el de perder el control, de que otro opere en la plataforma y no quede clara la división de responsabilidades.

Recuerdo que hace mucho tiempo, un ingeniero de quien aprendí mucho me decía: "si la nube se cae, ¿de quién es la responsabilidad?"

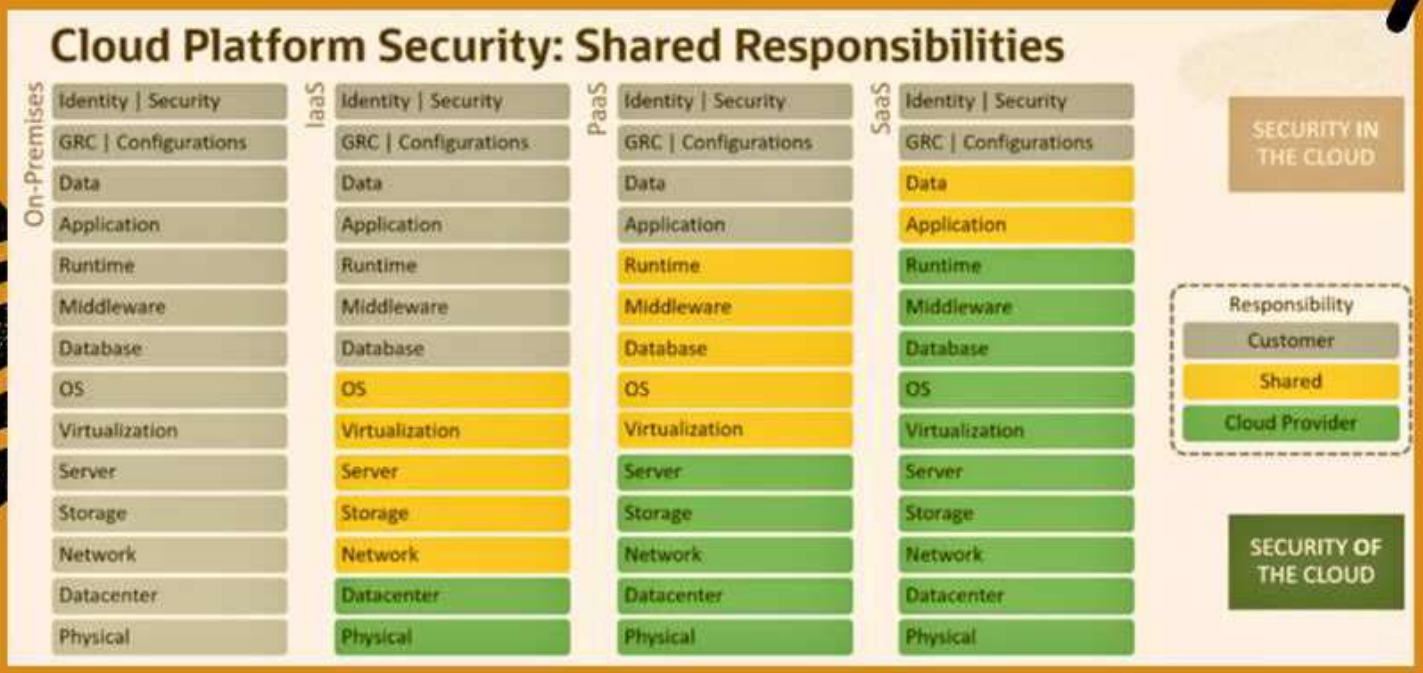
Antes de responder a ello, es bueno ir a los básicos de la nube, empecemos por el modelo de servicio, IaaS, PaaS o SaaS.

YEn IaaS (Infrastructure as a Service), el hiperescalar (Azure, AWS o Google Cloud) nos da el servicio de conectividad y arquitectura, siendo nosotros quienes nos hacemos responsables de todo lo que se instale y cómo se comunique -por conexiones definidas por software-, así como las capas de seguridad que queremos aplicar a todo el entorno, desde una segmentación fuerte. Prácticamente cualquier servidor que funciona virtualizado se puede llevar a la nube a lo que se llama VPC (Virtual Private Cloud).

En el modelo PaaS (Platform As A Service), normalmente una empresa ha desplegado un entorno orientado a unos procesos sobre la plataforma del hiperescalar. Hay ejemplos de varios tecnólogos industriales que ofrecen sus plataformas Cloud para que podamos cargar, no solo nuestros datos, sino nuestros modelos de plantas o sistemas, algoritmos y rodar sobre todos estos modelos de simulación, optimización, hasta incluso plantear configuraciones alternativas con los que valorar desempeños futuros. El primer caso así lo hizo GE con su plataforma Predix, y quizás algunos de los más relevantes hoy día los tengamos con Siemens Mindsphere.



En el modelo SaaS (Software as a Service) nosotros utilizamos todo el software como un servicio y lo que subimos son nuestros datos. El modelo más claro, aunque no conocido por todos, es Microsoft 365, de modo que usamos todo el Office pero somos responsables de los archivos que creamos, dónde los guardamos o con quién los compartimos. Pero si nos vamos al mundo industrial tenemos algún player muy relevante como es el caso de AVEVA Connect
Aquí uno debe pararse y traer el típico esquema de compartición de responsabilidades.



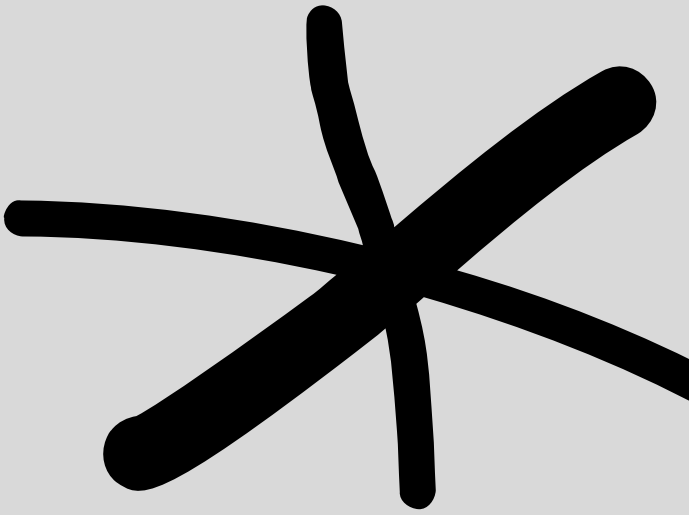

¿Puedo subirlo todo a la nube y olvidarme? Por supuesto que no, al menos si lo que me preocupa es mantener la misión crítica que aquí nos ocupa y la clave es mantener ese sentido de responsabilidad que nos permita identificar que aspectos, internos o externos nos pueden afectar.

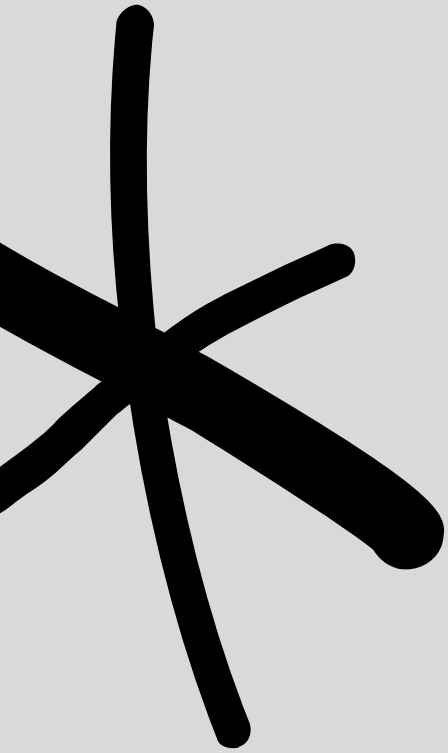
El concepto de responsabilidad de los sistemas que, según la documentación en inglés que se consulte, nos habla de distintos niveles, “responsibility, accountability, ownership” y que el personal de las infraestructuras críticas lo tiene muy claro, va desde hacer lo que me compete hasta asegurarme de que las cosas que necesito que funcionen, aunque no dependan de mí, lo hagan para que mi sistema funcione.

Con estos postulados el listón está realmente alto, ¿lo podríamos conseguir? Lo cierto es que no hay ningún sistema o ecosistema operado y mantenido al 100% por una única entidad.

El concepto de las líneas de comunicaciones dedicadas ya ha sido abandonado por modelos más eficientes en los que sí se hacen distintos usos de una misma infraestructura, asegurando eso sí, los criterios de disponibilidad o calidad de servicio que se requieren. Aún más: el concepto de SD-WAN, con redes definidas por software, es ya una realidad en entornos críticos.

Muchos entornos críticos operan ya sus entornos con centros de proceso de datos (CPD) redundados y totalmente virtualizados. A partir de aquí, ¿podríamos hablar de entornos en los que la nube fuera privada? Es decir, que hablemos de la nube como una tecnología que simplifica el acceso, la computación y la escalabilidad, pero desde nuestra propia infraestructura. Pues es un modelo que ya se está dando.





En otros casos se ha ido evolucionando de manera que se permiten conexiones entre las infraestructuras privadas y los hiperescalares para obtener óptimos de accesibilidad, tiempo de respuesta y privacidad. Incluso en este modo híbrido hay quien tiene acuerdos con estos hiperescalares para que sean ellos directamente quienes operen, mantengan y actualicen sus CPDs.

Por tanto, podemos distinguir una gama de modos de operación de la tecnología cloud desde la infraestructura privada hasta la nube pública, con distintos modelos híbridos, y en todos ellos también definir si iremos a emplear la nube como IaaS, PaaS o SaaS.

Lo primero, ¿nube 100%? La respuesta es NO. Puede haber un sistema de control en nube, ya los hay para entornos de energía solar fotovoltaica, pero no podemos ni debemos renunciar a tener el control local. Pensemos en los escenarios, especialmente en ventanas de mantenimiento, en que las actuaciones nos hagan perder conexión con el exterior, debemos saber localmente lo que pasa y poder custodiar localmente esos datos. Además, no olvidemos que hay muchas acciones de protección de los sistemas que requieren controles y protecciones locales, ¿dejaríamos dichas protecciones sin una mínima capacidad de visualización y control local que nos indique qué ha pasado?

Pensando en entornos de manufactura podría verse al revés, ¿cuánto de mi SCADA o MES llevar a la nube? Hay fabricantes como Ignition o el mencionado Aveva que nos ofrecen todo el abanico de posibilidades de despliegue.

Bien entendido, estaremos hablando de resiliencia, se podría operar desde una infraestructura en nube sabiendo que se tiene el respaldo en planta.

¿Y qué hay de las latencias?

Lo cierto es que, si atendemos a los reportes de los 3 principales ya citadas, todas tienen Región en España y permiten tests con resultados más que satisfactorios.

¿Qué importancia puede tener la cuestión de las regiones de las nubes?

Para muchas multinacionales es un dato prioritario conocer la ubicación de las regiones de centros de datos, no solo para cuestiones de latencias sino también para las cuestiones relativas a soberanía de datos y de legislación aplicable.

¿Y a nivel regulatorio?

Si miramos el entorno de la energía en España, veremos que el operador nacional REE ya permite su uso, eso sí, siempre que sea en modelo IaaS. Si miramos más allá de nuestras fronteras, veremos que reguladores en USA como NERC-CIP aceptan en uso de la nube como complemento a las funciones necesarias para el entorno energético y podremos encontrar guías de cumplimiento de los principales proveedores de nube.

¿Y a nivel de ciberseguridad?

Es una cuestión fundamental que enlaza con la anterior, que necesita abarcar todos los aspectos, desde los técnicos a los organizativos.

¿Aspectos organizativos de seguridad de la nube?

Por supuesto, pensemos en la aplicación de separación de funciones y de mínimos privilegios, esto ahondaría más en la separación IT-OT. Pero también es verdad que no hay dos empresas iguales y, tal como hemos visto en el diagrama de responsabilidades de la nube, necesitará haber separación entre aplicaciones y datos, pero quizás se plantee una gobernanza coordinada de las comunicaciones y hasta de las identidades para uno y otro entorno.

¿Y a nivel de arquitectura segura? No está demás plantearse una parte solo de OT frente a otra de IT, aunque ambas residan en el mismo proveedor.

# Planteemos las mismas cuestiones de diseño que aplicaríamos a un entorno industrial:

- Prohibición por defecto salvo las necesidades documentadas.

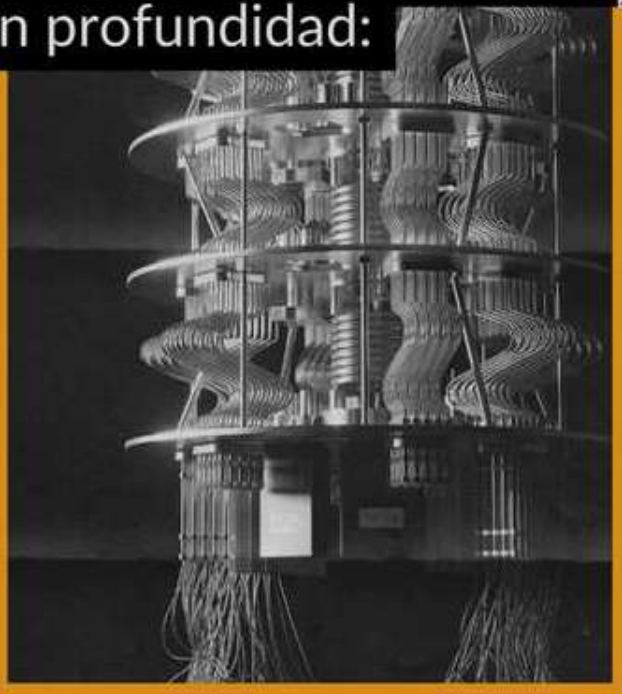
- Entornos de repositorio de datos separados de los entornos de control.

- Diseño estricto de las comunicaciones entre VPCs, tanto a nivel de origen y destino, como de protocolos, comandos, APIs y aplicaciones permitidas o qué partes deben estar expuestas y cuáles no.

- Definir qué otros requisitos de datos existen para envío al exterior -especialmente de organismos regulatorios- para asegurar entornos intermedios para extracciones seguras de los datos sin comprometer el repositorio maestro.

- Niveles necesarios de redundancias y de configuraciones en alta disponibilidad, tanto para repositorios como para switches y firewalls en el entorno nube.

## ¿Y qué otros controles debemos plantearnos? Pensemos en la aplicación de la filosofía zero-trust y en el modelo de defensa en profundidad:



- Chequeo continuo de conexiones y equipos de origen
- Vigilancia de la actividad de las cargas de trabajo así como posibles conexiones nuevas, especialmente de las que no debieran estar expuestas
- Pensemos en la importancia clave de la gestión de identidades, roles y niveles de privilegio
- Sistemas de autorización y trazabilidad de peticiones, ya no solo a nivel de SCADA o Historian, sino del conjunto completo de la nube, tanto para dar acceso como para revocarlo
- El empleo de los propios firewalls en nube, especialmente de sus capacidades de inspección de tráfico industrial, lo que permitirá reducir la superficie de ataque y establecer controles realmente granulares sobre qué se puede hacer y con qué aplicaciones y usuarios, tanto Norte-Sur (perímetro) como Este-Oeste (segmentación interna)
- Aspectos como los de monitorización y detección pueden ser mucho más ventajosos en cuanto a la disponibilidad de recursos para correlación y aplicación de reglas, conforme ya se hace con muchos entornos de seguridad como de EDR/XDR.

En resumen, la nube OT existe y se puede ir a ella, la adopción de fabricantes industriales y de usuarios lo muestra. Ahora bien, el trabajo de arquitectura de seguridad es algo que requiere un diseño previo al despliegue y que permitirá una asunción de responsabilidades acorde con la política del negocio.


allot
See. Control. Secure.
¿Conoces realmente tu red?
Compréndela, contrólala y securízala
Allot optimiza el tráfico de red, entrega servicios más rápidamente y protege tu infraestructura y tus datos más preciados.
¡Tu conocimiento será tan bueno como sea el entendimiento de tus datos!
www.allot.com


Para
Empresas

Técnico Superior En Informática De Gestión. Auditor sénior en ciberseguridad, colegiado como perito Judicial en informática forense. Diferentes certificaciones, como Cybersecurity Essentials por CISCO, CPHE (Certificado profesional de hacking ético). Cursos finalizados pendientes de certificación, PCAP (Programming Essentials In Python) por CISCO, CyberOps Associate por CISCO. EC Council Hacking Y Ciberoperaciones por CISCO, formador ocupacional por la Junta De Andalucía. Formador de formadores especialidad Tele Formación. Programación VB.NET, Python, lenguaje Ensamblador. Actualmente cursando el CEH.

Ha trabajado como consultor en The Security Sentinel, auditando empresas de nivel internacional como Farmacéuticas y partidos políticos de gran relevancia, organismos oficiales como la Junta De Andalucía, Entidad Nacional De Acreditación. Ha trabajado como formador, impartiendo módulos al servicio Andaluz De Salud, Fundación O.N.C.E…. Su última formación fue por medio de la Fundació IL3- De La Universidad De Barcelona al PDI de Chile, edición 2022 (Estándares corporativos en protección de datos y detección y análisis de datos vulnerables). En estos momentos trabajando con ARELANCE, impartiendo cursos de ciberseguridad. Terminando nuevo libro de bastionado en sistemas y redes informática por editorial Ra-Ma.

# Ataques a la cuarta revolución industrial.

Es raro el día que no sale en los medios de información, alguna noticia relacionada con un hackeo por parte de un ciberdelincuente a organismos o empresas como:

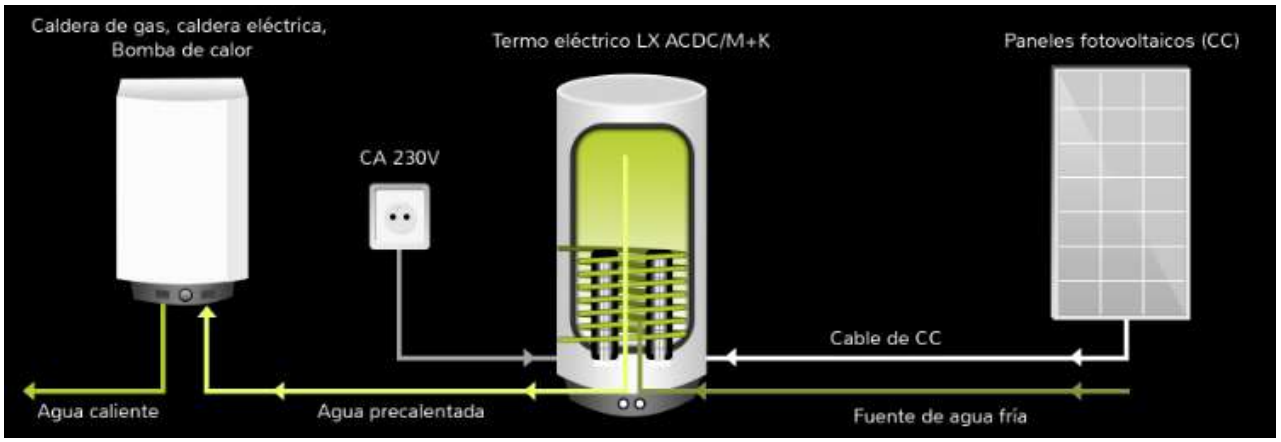
Hospitales.
Hoteles.
Industria alimentaria.
Compañías eléctricas.
Compañías farmacéuticas.
Gestión de aguas.
Gestión de trenes.
Centrales nucleares.
.....

No es nada nuevo saber que las empresas industriales llevan digitalizando sus instalaciones hace ya algun tiempo. Estas empresas, usan internet para conectarse y poder ser controladas en un momento determinado a distancia, para tener acceso a datos, estados..... El caso es hacer de la industria una producción inteligente y eficiente.

He tenido la gran suerte de conocer algunas de estas industrias, bien desde un punto vista como programador o bien desde el punto de vista de auditor de ciberseguridad.

Este tipo de industria se apoya en lo que se denomina IOT (internet de las cosas). Uno de los principios de diseño de este tipo de industria sería el de “Decisiones descentralizadas”, en pocas palabras un sistema industrial, en un momento determinado, puede tomar decisiones por sí misma.

Por ejemplo, supongamos el control de una caldera de agua (simulación):




Supongamos que este sistema se controla mediante un termostato:

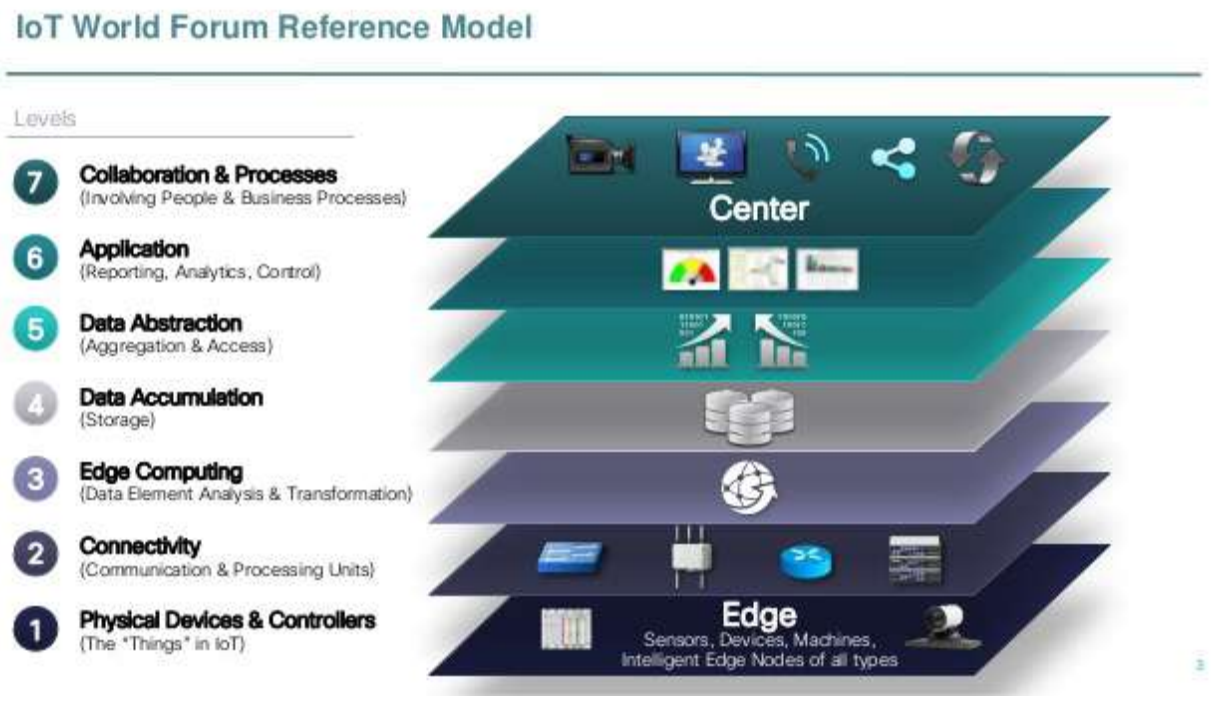
Este termostato está conectado con algún software y según la temperatura registrada, el software industrial puede tomar decisiones sobre el correcto funcionamiento de la caldera.

Bueno hasta aquí, ya nos podemos hacer una pequeña idea, y extrapolar la revolución industrial a sectores como un invernadero dedicado a la plantación de tomates. Este invernadero puede estar controlado por un sistema de calefacción (calderas) y ese mismo termostato del que hablaba anteriormente; si el termostato detecta una caída en la temperatura ambiente, se activa la cadera y regula la temperatura dentro del invernadero, con objeto de no perder la producción, en este caso de tomates.

Este sistema al mismo tiempo puede estar controlado por el propio agricultor que, dentro de los principios de diseño, se correspondería con “Asistencia Técnica”. De forma remota, el agricultor puede estar al tanto de estos cambios de temperatura y del funcionamiento correcto de todo su sistema.

Esta comunicación entre los dispositivos que están en el invernadero y el agricultor que podría estar en su casa, estaría dentro de los principios de diseño, “Interoperabilidad”. La “Interoperabilidad” es la conexión de maquinas y personas por medio de internet de las cosas o (IOT).

Una vez visto algunos de los puntos del principio de diseño, y ya teniendo una idea un poco más clara de lo que es IOT, se pueden definir 7 capas para IOT:




**7.- Colaboración y Procesos.- En donde se involucra directamente a personas y los ciclos del negocio.**
**6.- Aplicaciones.- Todo lo relativo a reportes, análisis y control.**
**5.- Abstracción de los Datos.- Adición y acceso a datos generados por capas inferiores.**
**4.- Acumulación de los Datos.- Almacenamiento de datos generados por capas inferiores.**
**3.- Edge Computing.- Análisis y transformación de los datos generados por la capa 1.**
**2.- Conectividad.- Unidades para comunicación y pre-procesamiento de los datos.**
**1.- Dispositivos y Controladores Físicos.- Las "Cosas" (sensores y actuadores).**
**Ataques a la cuarta revolución industrial.**


# SECURING THE EXTENDED INTERNET OF THINGS (XIOT)

Unmatched Visibility and Protection for Industrial, Healthcare, and Commercial Cyber-physical Systems.

CLAROTY

claroty.com

Ataques a la cuarta revolución industrial.

El motivo de los ataques a la industria pueden ser muchos. Las motivaciones de los ciberdelincuentes, podrían ser:

Espionaje industrial.
Dejar no operativa la industria, con fines de degradar un gobierno o militares.
Acceso a sus datos, con fines lucrativos.
.....

## ¿Pero como lo hacen?, ¿Cómo entran en industrias o en nuestros dispositivos IOT?

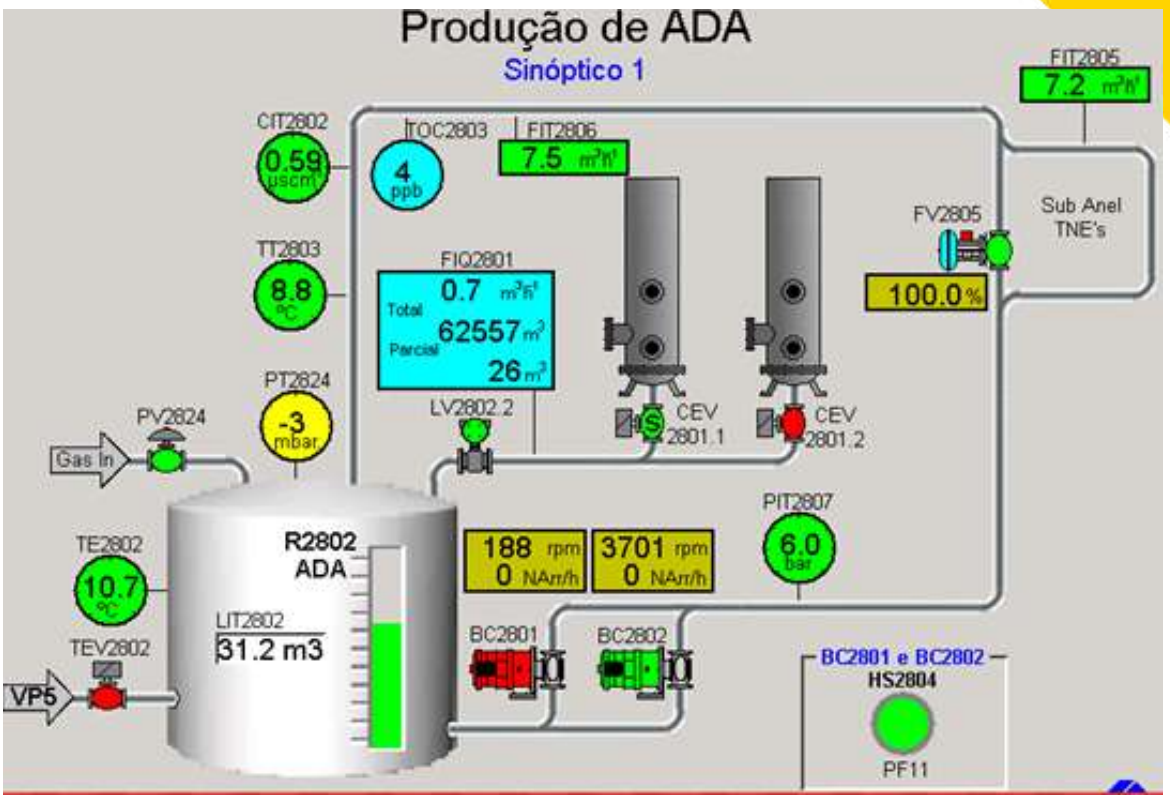
Bueno, todo dependerá un poco del fin del ciberdelincuente, pongámonos en el fin más destructivo que hay, el de quitar la vida humana o tener monitorizado los patrones diarios de una persona. Ya en 2017-2018, los Estados Unidos prohibieron a sus soldados tener activo el GPS de sus teléfonos o dispositivos de entrenamiento, como rastreadores de fitness. Estos soldados en territorio hostil, hacían ejercicio y sus datos, de tiempo, ruta y posición se subían a Strava, una red social basada en internet y GPS, enfocada al deportista. De esta forma un ciberdelincuente, no solo identifica un patrón de movimiento de una persona y hábitos, sino que, en el caso de estos soldados, podían estar hasta destapando la posición de su base.

En este ejemplo podíamos estar hablando de un uso “inocente”, por parte de un usuario de su dispositivo IOT para hacer fitness, pero sus datos aprovechados con fines nada buenos… Este dispositivo IOT, estaría situado en la grafica superior en la Capa 1.

Dentro de la industria, los dispositivos IOT, pueden ser desde:

Sensores con los que controlar temperaturas, medias….

Supongamos una industria, farmacéutica, donde tienen una serie de termos que controlan el agua para la creación de algún fármaco.




Estos termos incorporan una serie de sensores, donde pueden entre otras cosas medir la temperatura. Estos sensores, se pueden comunicar con la capa superior, por medio de PLC (Controladores Lógicos Programables), RTU (Unidades Terminales Remotas)…
Algunos de estos dispositivos con S.O. embebido, otros dependen de estaciones con S.O. comunes como Windows, Linux, Unix….

Si un ciberdelincuente pudiera interceptar de alguna forma esta comunicación o alterar el sensor, la producción podría verse gravemente afectada.

Dentro de la revolución industrial, básicamente un ciberdelincuente puede explotar cada una de las capas, en las que pueda detectar una brecha de seguridad y si no encuentra una brecha, por medio de otro tipo de ataques, abrir una nueva.

Según mis propias investigaciones y basándome en auditorias en sectores tan fuertes como el farmacéutico, transporte o construcción, voy dar algunas claves de por donde entran estos ciberataques.

Los ataques pueden ser dividíos en dos categorías:

Ataques dirigidos.
Ataques casuales.

## Ataques dirigidos.

En este tipo de ataques, el ciberdelincuente, fija un objetivo, y averigua todo lo posible, como dominios conectados en la red, traceo de puertos..., estudia físicamente si le es accesible la empresa, para ver si puede introducir algún dispositivo como BadUSB.... En definitiva, serían muchas las técnicas que podría utilizar.

## Ataques casuales.

En este tipo de ataque, el ciberdelincuente, solo mira por internet, buscando una serie de puertos, usando IP's al azar.

Sobre este punto he realizado un pequeño estudio, y me he encontrado con medianas y grandes empresas, totalmente abiertas, y algunas de estas empresas estarían dentro del sector de la revolución industrial.

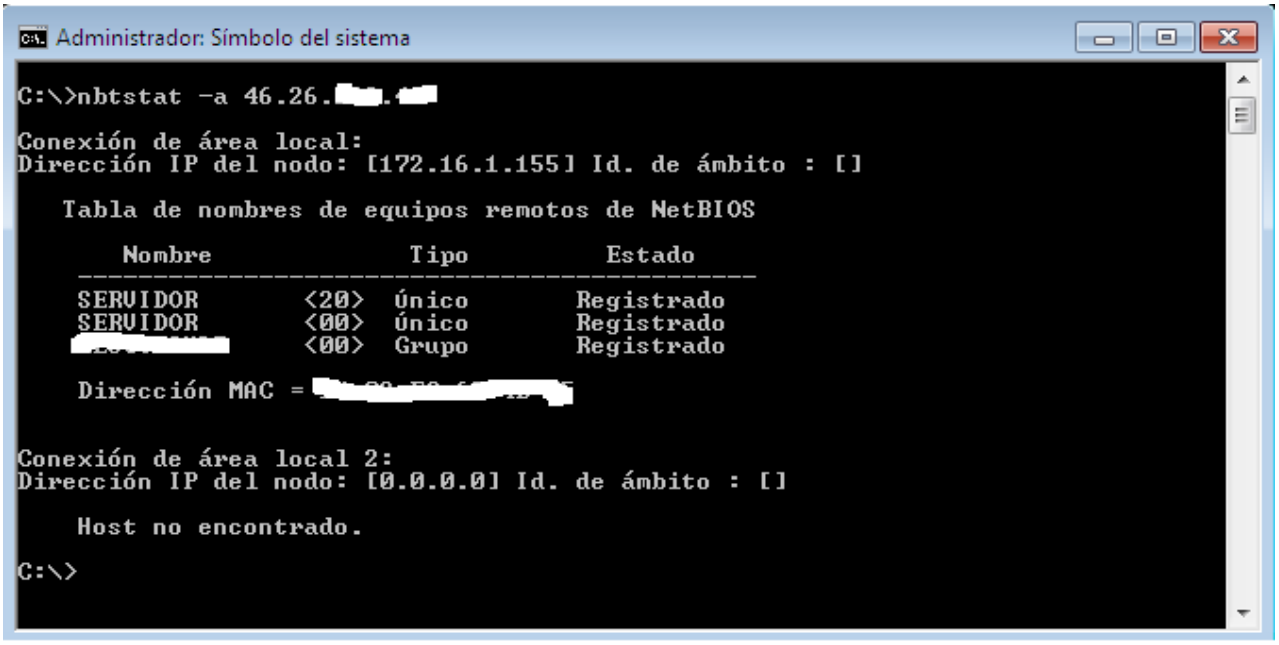
¿Tienes un Windows 7?, si lo tienes ya puedes probar esta técnica con muy pocos conocimientos. Solo vas a necesitar básicamente tres comandos:

Nbtstat
Net view
Dir

Un ciberdelincuente, usara un pequeño programa, que le haga este trabajo manual que voy a explicar ahora.

Veamos en qué consiste:

Desde un XP o Windows 7, virtualizado, puede abrir una CMD o Shell de Windows. Seguidamente se coge una IP publica, al azar, por ejemplo 46.26.229.40.

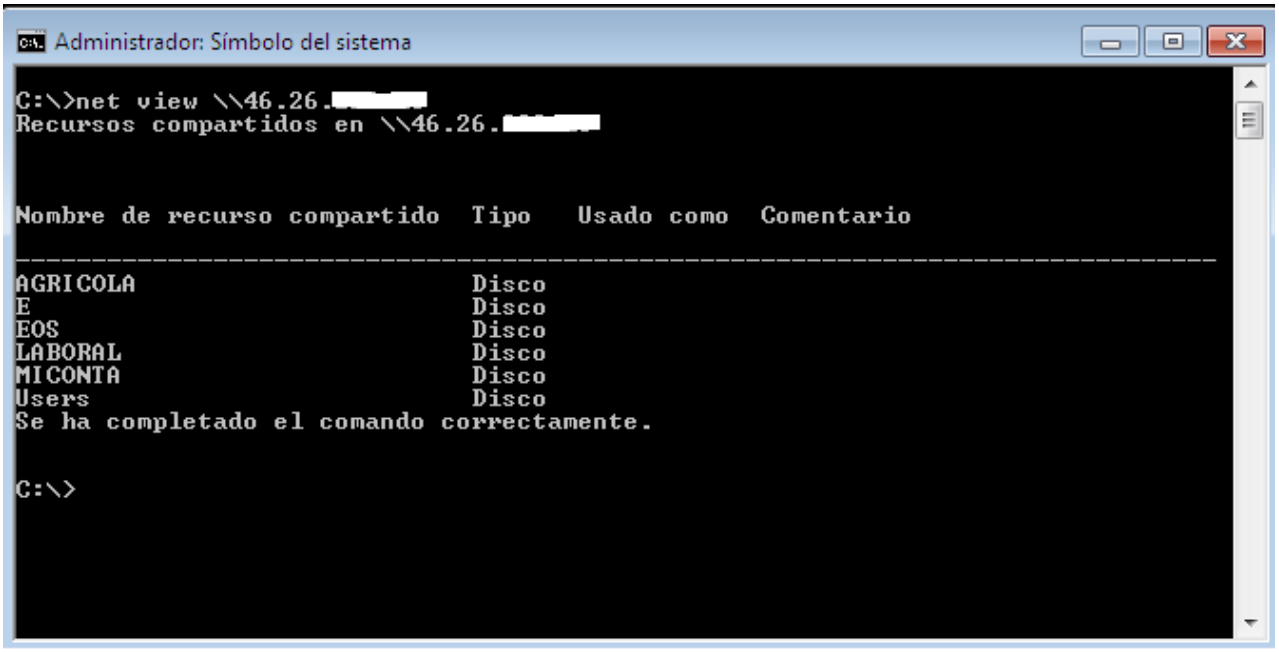



El comando “nbtstat” se usa para poder ver tablas de nombre de equipos, tanto en equipos locales como en remotos. El usar este comando con Windows 7 o Windows XP, es porque Windows 10, lo tiene limitado a ver equipos locales y no remotos y hay que realizar una serie cambios en la configuración para poder usarlo.

Si nos fijamos en la imagen superior, estoy “traceando” de forma manual, con IP externas, y he conseguido dar con un ordenador el cual podría tener los recursos abiertos. Dentro de esta información, este comando da el nombre del grupo de trabajo, en este caso es el nombre de la empresa, borrado por protección de datos.

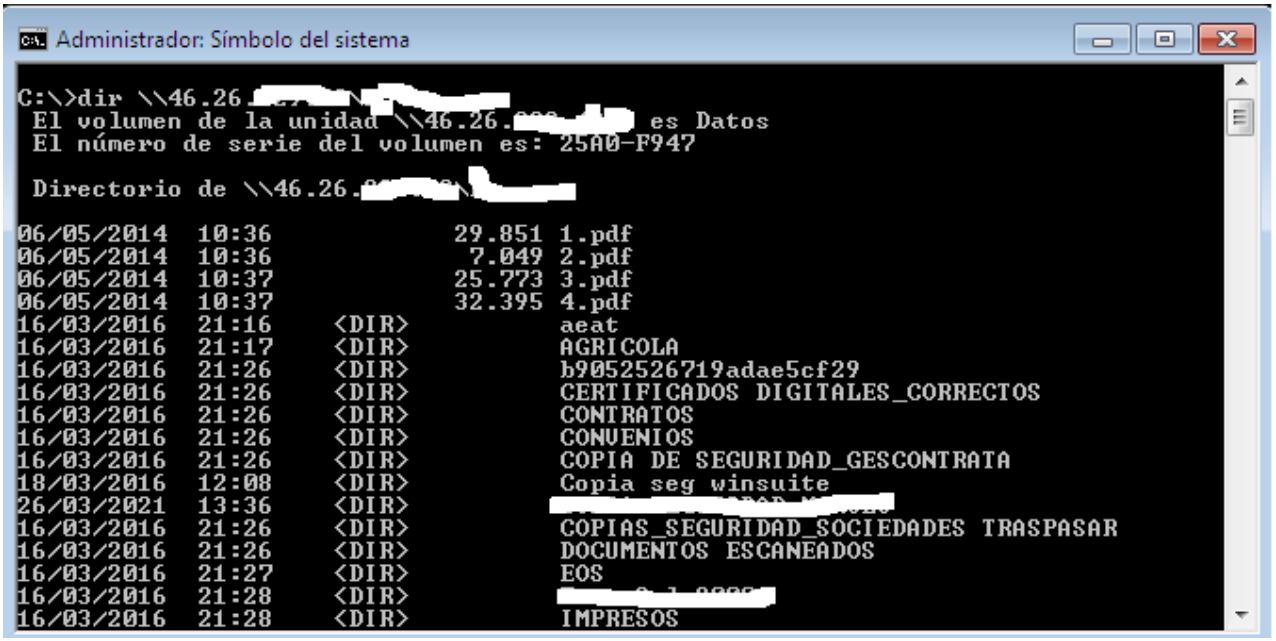
Ya solo con esto, sabría el nombre de la empresa que tiene una brecha de seguridad, y podría indagar por internet para ver a qué se dedica, donde esta geolocalizada, que más puertos tiene abiertos…

El caso es que si ahora en la consola pongo:




Este comando permite ver los posibles recursos compartidos del "objetivo".

El siguiente comando que podría probar es:



Un ciberdelincuente o equipo de Ransom, puede tener el programa buscando IP al azar; con este tipo de problema y de una forma automática, entrar en los recursos compartidos y cifrar todo. Realmente un equipo de Ransom más “fino”, una vez detectado esta brecha, intentaría sacar más información sobre la empresa y escalar privilegios para cifrar lo máximo posible.

Estos ataques “casuales” han afectado a:

-Empresas internacionales de paquetería.

-Empresas de transportes, a nivel nacional o internacional.

-Empresas industriales de compontes para vehículos, nivel nacional/europeo.

-Pequeña y mediana empresa.

# Fallos comunes por donde se puede entrar en una industria.

Recuerdo que en una auditoría a una farmacéutica internacional, en una de sus delegaciones de producción, había que auditar unos 200 activos, y para poder entrar en esta red, tenía que hacerse por medio de una VPN.

Bueno, hasta aquí todo bien. Nos dan el acceso a la red, por medio de VPN y en ese momento empieza la auditoria.

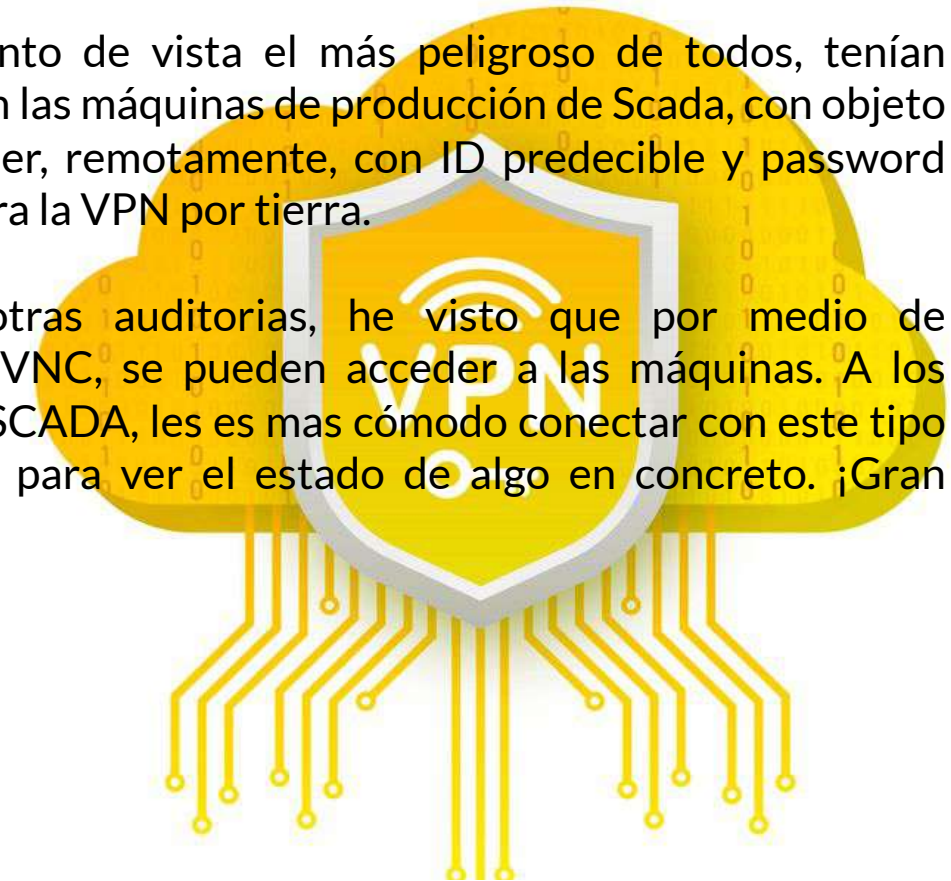
Comprobamos que se podía hacer brecha por medio de:

Sistemas operativos desfasados: una de las máquinas de producción, que controlaba una serie de calderas de agua, tenía instalado un Scada, por motivos de presupuesto, pero la versión del Scada era antigua y solo parecía ir bien en un Windows 2000 server. Con un usuario "Administrado" como clave "1234".

Acceso a servidores por medio de Microsoft SQL Server, puertos abiertos de SQL server, con usuario sa y sin clave.

Y desde mi punto de vista el más peligroso de todos, tenían instalado Vnc en las máquinas de producción de Scada, con objeto de poder acceder, remotamente, con ID predecible y password "12345". Esto tira la VPN por tierra.

En muchas otras auditorias, he visto que por medio de TeamViewer o VNC, se pueden acceder a las máquinas. A los operadores de SCADA, les es mas cómodo conectar con este tipo de aplicaciones para ver el estado de algo en concreto. ¡Gran fallo!



En otra ocasión participé en el desarrollo de una aplicación que conectaba con un programa de automatización de plantas de hormigón; en este caso tenían un SCADA de una empresa nacional. Las delegaciones de la planta de hormigón, que están repartidas, conectaban con el servidor de la empresa por medio de ODBC hacia una base de datos, y esta conexión sincronizaba los datos de todas las delegaciones con el servidor principal. En este caso, como en la película, “Cometieron dos errores” muy graves.

El puerto de la base de datos estaba expuesto, sin protección de una VPN.
El usuario sa tenía su clave muy, muy predecible. Con un poco de ingeniería social, salía. Una vez dentro del sistema de base de datos, que era un Microsoft SQL Server, se podía acceder al servidor.

# La mala administración de un sistema puede evolucionar en un Ransom.

Para resumir un poco:

La comodidad a la hora de administrar un sistema: es un error si un empleado o gerente quiere desde su casa ver sus carpetas; es un error, por parte del administrador del sistema, compartir recursos, abrir puerto 445 en el router y trabajar de esta manera.

Es un grave error dejar expuesto el puerto del gestor de base de datos, con programa de ataque de fuerza bruta, y si la clave no es muy robusta, se pueden conseguir entradas a nuestros datos y saltar al servidor.

Es un gran error tener una VPN y dentro de algún activo de esta, tener Teamviewer, VNC..., para conectar desde fuera; tira por tierra la protección que nos brida nuestro túnel privado virtual.

Es un grandísimo error trabajar con versiones de sistemas operativos desfasados o no actualizados correctamente.

Wifis de invitados que no están correctamente separadas en VLAN diferentes.

Un gran error, tener la página web corporativa en un servidor instalado en el mismo CPD o infraestructura de la empresa y, para colmo, tenerlo dentro del mismo segmento de red.

sealpath™
Smart Protection for Sensitive Data

# PROTECCIÓN Y CLASIFICACIÓN DE DATOS IMPULSADA POR IA/ML

Tecnología avanzada para la visibilidad y el control dinámico de sus datos en tiempo real.

EVITA EXFILTRACIONES POR RANSOMWARE

FACILITA COLABORACIÓN SEGURA

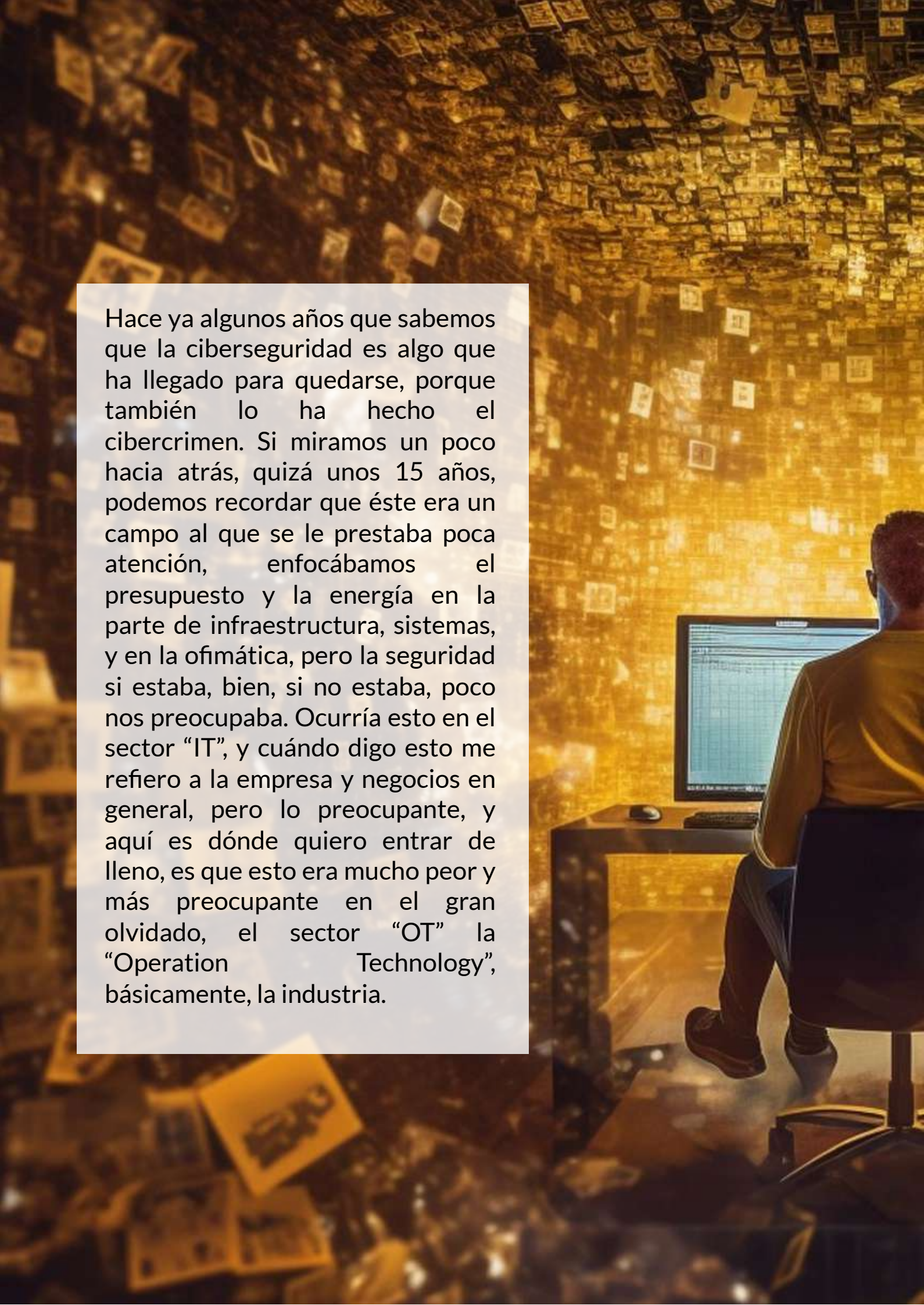
CUMPLIMIENTO REGULACIONES GDPR, PCI...

MINIMIZA EL RIESGO DE FUGAS DE DATOS


sealpath.com | 944 425 922
sales@sealpath.com

Argentino como Fangio. Licenciado en Sistemas, MBA en Tecnología Informática y Transformación Digital y Máster en Desarrollo Directivo. La tecnología está en mis células. Eterno aprendiz. Me desvela la Ciberseguridad y el desafío de futuro, tanto que dejé mucho pelo pensando en él. Más de 15 años trabajando y liderando el área de IT en el sector de investigación, energía y construcción como CIO y CISO. Actualmente Ingeniero de Ciberseguridad.
Además, soy Trader e Inversor.
¿Una frase arraigada? “No te des por vencido, ni aún vencido.” Almafuerte

# Protección de infraestructuras críticas, el gran desafío

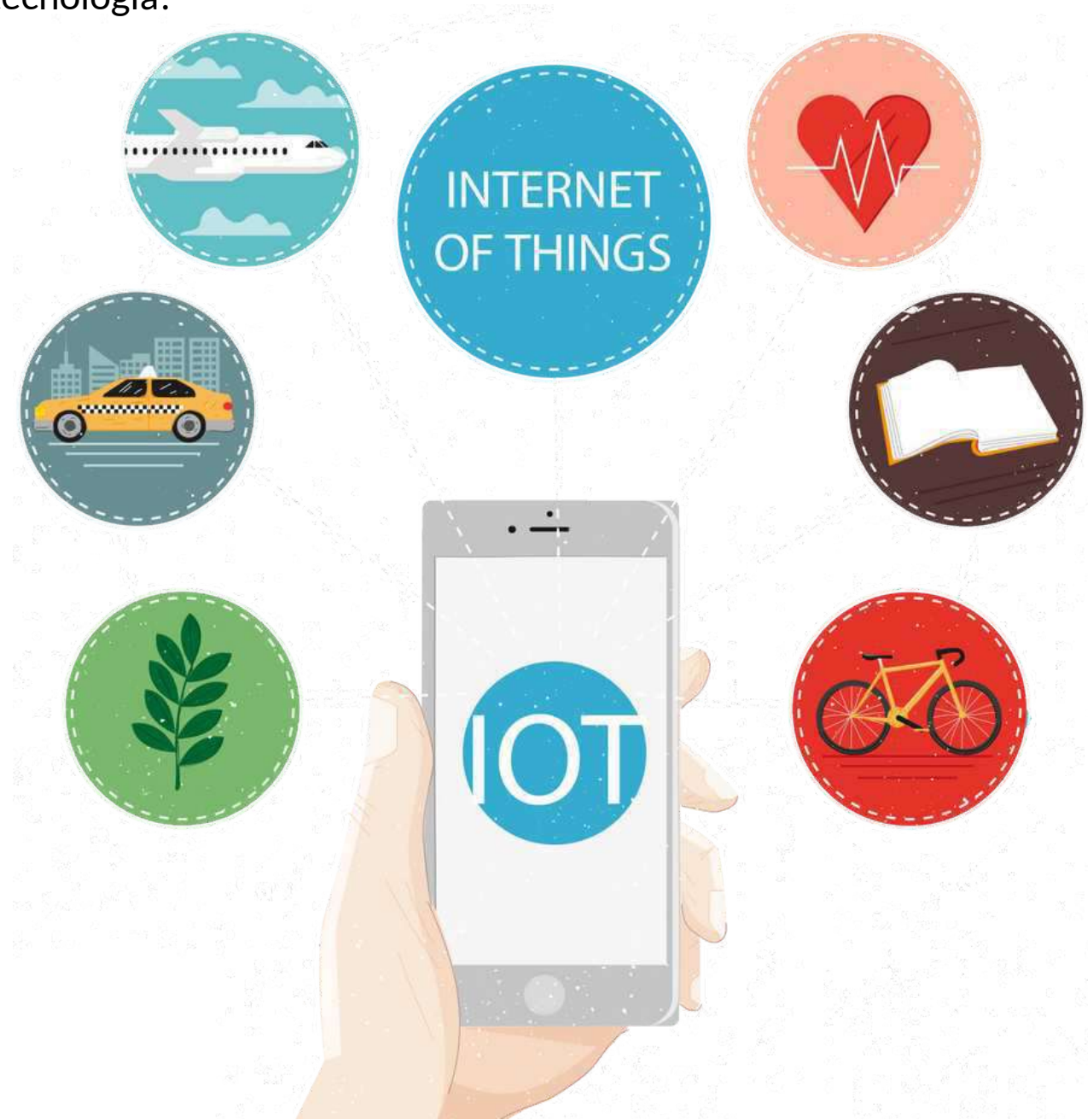


Hace ya algunos años que sabemos que la ciberseguridad es algo que ha llegado para quedarse, porque también lo ha hecho el cibercrimen. Si miramos un poco hacia atrás, quizá unos 15 años, podemos recordar que éste era un campo al que se le prestaba poca atención, enfocábamos el presupuesto y la energía en la parte de infraestructura, sistemas, y en la ofimática, pero la seguridad si estaba, bien, si no estaba, poco nos preocupaba. Ocurría esto en el sector “IT”, y cuándo digo esto me refiero a la empresa y negocios en general, pero lo preocupante, y aquí es dónde quiero entrar de lleno, es que esto era mucho peor y más preocupante en el gran olvidado, el sector “OT” la “Operation Technology”, básicamente, la industria.

Pensemos por ejemplo una planta de energía que comenzó a construirse a principios de los años 2000, con tecnología de la época y que se tarda 5 años en terminar su construcción, luego llega la fase de pruebas, puesta en marcha y salida a producción; supongamos 7 años. Al ritmo al que la tecnología evoluciona, lo más seguro es que en ese período de tiempo, la tecnología utilizada para las comunicaciones, controles, operaciones y demás en esa planta, haya evolucionado al menos 2 veces. Además, pensemos que seguramente la tecnología se compró al comenzar la planta, porque se especifica esto en la fase de diseño que podría haber ocurrido 2 años antes al menos, con lo cual, al comenzar la construcción ya la tecnología si no es obsoleta está próxima a serlo. Si proyectamos esto, desde principio a fin, nos termina dando un total de… ¿10 años? Estoy hablando de una planta de energía termoeléctrica, y a modo de ejemplo, si pensamos en una nuclear estos tiempos son mayores y todo mucho más complejo.

En ese período de tiempo, creo que no es necesario decirlo, la tecnología no solo evoluciona, sino que seguramente cambia. Imaginemos entonces, que de la mano de eso comenzamos a hablar de la industria 3.0 a partir de la aparición de internet, las comunicaciones y la globalización. Este tercer período podemos considerarlo como tal a partir del año 2006 que fue avalado por el Parlamento Europeo a partir del desarrollo del concepto por parte de Jeremy Rifkin. Apenas unos años después comenzaron a circular conceptos como el IoT (Internet of Things), los coches eléctricos, la convergencia entre IT y OT, la Nube, las redes inteligentes, la robotización de los procesos y, si nos acercamos un poco más, ya hablamos de Machine Learning e Inteligencia Artificial.

Ahora bien, tras este pequeño repaso por los últimos 30 años de historia…¿Realmente el sector evolucionó de la mano de la tecnología?

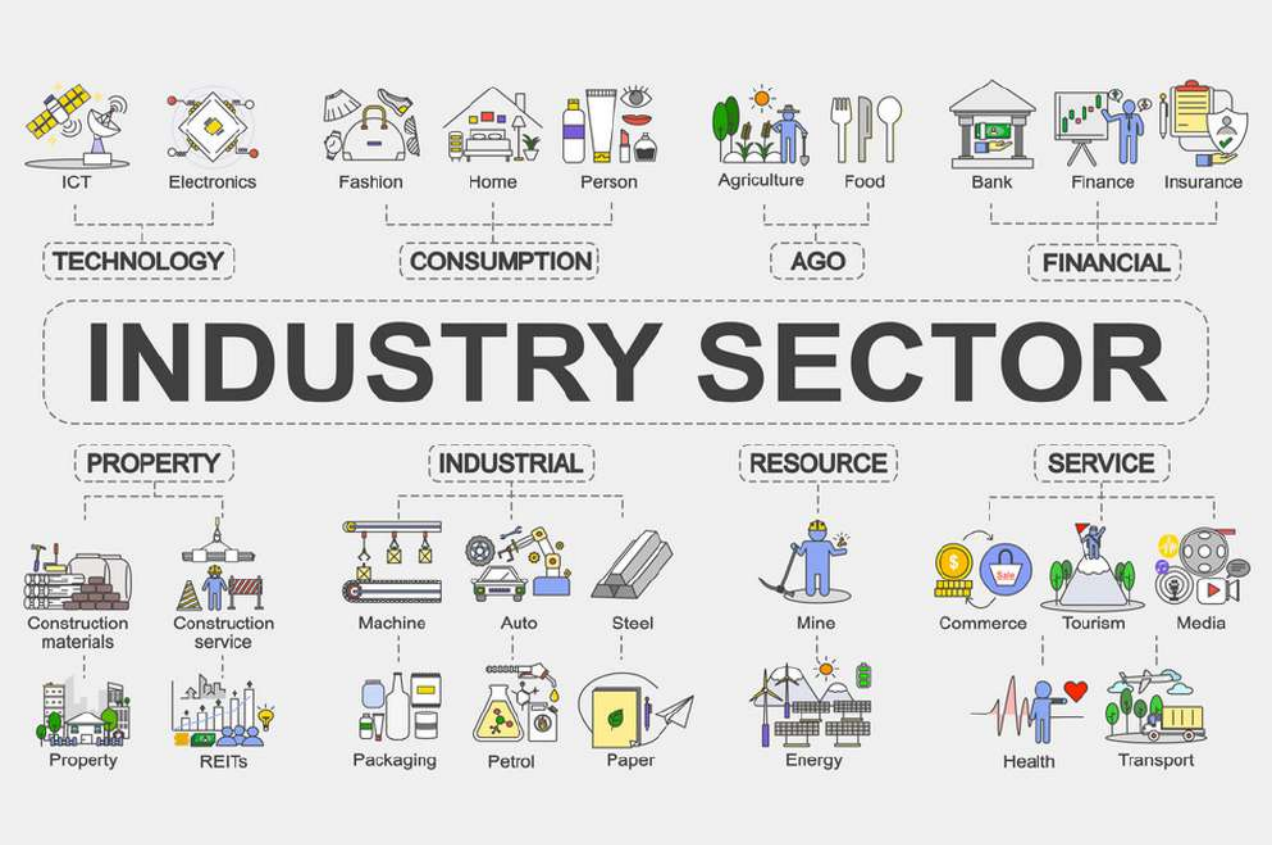


Claro que no. Pero no hay que caer en la trampa de creer que esto ha sido por desidia, por falta de interés o por algún motivo específico. No, esto se debe a múltiples factores y muchos de ellos son inherentes al sector en sí. Una planta de energía, de fabricación o una infraestructura de transporte, no son sectores dónde se pueda acompañar la evolución tecnológica de una forma sencilla. El solo hecho de plantear un salto tecnológico podría significar un "revamping" completo de esta, y no hablemos si este cambio debe producirse en la parte de ciberseguridad, comunicaciones y operaciones, pues entonces podría ser más complejo de lo que suponemos.

Hasta ahora, poca importancia se le ha dado a la seguridad informática del sector. La comunicación entre los múltiples elementos, la obsolescencia de los sistemas operativos y del software utilizados en estas infraestructuras puede, fácilmente, datar de 10 años o más siendo optimistas, y el gran problema es que los fabricantes tampoco han evolucionado, el software fabricado para la automatización y control de cualquier sistema, sigue siendo el mismo que para un Windows XP y ya ha dejado de ser compatible hace una pila de años con los nuevos sistemas.

Esto sin mencionar que hace 10 ó 15 años hablábamos de antivirus para proteger los equipos, los cuáles se basaban en firmas y podían estar bien para la época, pero así como evolucionan los sistemas y la tecnología, también evoluciona el crimen organizado y hoy no basta con un antivirus, debemos hablar de tecnologías que no solo se basen en firmas sino en comportamiento, sean capaces de detectar anomalías y aplicar las medidas de seguridad adecuadas para proteger los activos de las infraestructuras, causando el menor impacto posible porque, recordemos que, son sectores en producción en los cuáles un milisegundo puede cambiar todo o un ramsonware podría ser letal para el negocio. Pensemos solamente en que podría ocurrir si un ataque cambiara los datos de presión o temperatura de un fichero que viaja de forma plana en una red industrial. Quizás en una planta de biomasa sería un problema, pero, ¿en una nuclear?

Hasta ahora solo he mencionado el sector OT o industrial, pero lo que no he dicho es que gran parte de las empresas que están bajo esta denominación son lo que llamamos comúnmente infraestructuras críticas, es decir, compañías de generación y distribución de energía, gas, agua, comunicaciones, puertos, hospitales, aeropuertos, etc. Para poner en contexto de qué hablamos cuándo hablamos de industria:




Fuente: https://seguridad.prestigia.es/principal 1

Solo en 2022 los ciberataques a estos sectores aumentaron en Europa un 11% y el sector industrial ha sido el más afectado quedándose con el 32% del total de estos ataques en este mismo año. Dicho así puede parecer una simple estadística, pero vamos a ver en números cuánto le cuesta a las empresas un ciberataque. “Las empresas podrían incurrir en más de cinco billones de dólares en costes adicionales y pérdidas de ingresos en los próximos cinco años como consecuencia de los ciberataques, casi el tamaño de las economías de Francia, Italia y España combinadas, según el estudio Securing the Digital Economy: Reinventing the Internet for Trust.

El informe, con una base de 1.700 encuestas a consejeros delegados y altos ejecutivos de compañías de todo el mundo, apunta a la industria tecnológica, la farmacéutica y la del automóvil como las más expuestas a los riesgos cibernéticos. Sólo la primera se juega más de 750.000 millones de dólares, según el estudio, por los 642.000 millones del sector farmacéutico o los 505.000 del automovilístico."


Fuente: https://www.expansion.com/economia-digital/companias/2019/01/25/5c4a342ee5fdeabc508b4677.html

Hasta aquí vemos la gravedad del caso, en sectores de mucha importancia, pero también podemos ver que, si bien los ataques a infraestructuras críticas ya eran una constante antes, durante y después de la pandemia, la invasión de Rusia a Ucrania ha intensificado estos, haciendo foco en el sector energético y de transporte sobre todo.

El primer hito en referencia a esto, sucedió en 2010 cuándo de la mano de Stuxnet, un malware que explotaba un Zero-Day alojado en un USB, se encargó de comprometer una central nuclear de Irán.

En 2012 aparece BlackEnergy que se utilizó para diversos ataques de DDOS a organizaciones de todo tipo pero, en diciembre de 2015, más de la mitad de los hogares de la región Ucraniana de Ivano-Frankivsk se quedaron sin electricidad durante horas. Un año antes, se detectó el malware Havex, un troyano del tipo (RAT) capaz de recolectar datos de sistemas de control industrial. La intención era hacer inteligencia para luego diseñar ataques dirigidos a infraestructuras utilizando el hardware de los fabricantes. En 2016 la red eléctrica de Ucrania se vio afectada por otro ataque, en esta ocasión el Industroyer, una amenaza capaz de controlar los interruptores de las subestaciones eléctricas utilizando protocolos de comunicación industrial.

En los años siguientes esto evolucionó y en 2017 llegó NotPetya, que apuntaba al sector energético y financiero. Era ni más ni menos que un falso ramsonware, que no pretendía generar ganancias sino caos. Logró paralizar a toda Ucrania y luego comenzó a propagarse a nivel global gracias al exploit EternalBlue (el mismo utilizado por WannaCry).

Situándonos en el 2022, cuándo da comienzo una nueva invasión de Rusia a Ucrania, los ataques a este tipo de infraestructuras se han intensificado aún más, traspasando las fronteras de Ucrania de forma tal que, se han visto afectadas compañías de todo el mundo, sobre todo en Europa, EEUU y Latinoamérica. Así es como en este año se detectó un malware llamado HermeticWiper: su función es borrar datos de las organizaciones, principalmente de Ucrania. Unas semanas después se identificó a CaddyWiper que apuntaba al sector financiero. Luego en abril del mismo año, el CERT-UA dio respuesta a un incidente que atacó principalmente a un proveedor de energía de Ucrania. Se trataba de la evolución de Industroyer, el Industroyer2, que comparte similitudes con el primero.

## Podría seguir este relato y no tendría fin.


Mi intención no es aburrir, sino concientizar. Entender que en este sector en el que se abarca tanto, no es lo mismo hablar de una Central Nuclear que hablar de una planta embotelladora, aunque en su amplio espectro tienen titulares de tecnología punta y también de gran olvidado. Bueno, lo dejo abierto a debate. Claro está que, sin dudas, es el que más impacto causa cuándo la víctima de un ataque es la que nos mantiene la electricidad, calefacción, agua, sistemas de pago, transporte, viajes, etc. Y hoy contamos con herramientas para que, con el menor impacto posible y haciendo un plan de recuperación adecuado ante los desastres, podamos protegernos a la espera del próximo salto tecnológico que obligatoriamente se tendrá que dar.

Lo principal es entender que hoy, si bien no se aplica a todos los sectores pero sí a la mayoría, la convergencia entre OT e IT es inevitable, la industria 4.0 está aquí, las Smartcities ya son una realidad, pero debemos hacer especial foco, no solo en la transformación digital sino también, en la ciberseguridad que es y será la gran protagonista del mundo hiperconectado que viene.

yubico

# No todas las soluciones de MFA son iguales

## YubiKey es tu llave de seguridad multiprotocolo resistente al phishing

smart management

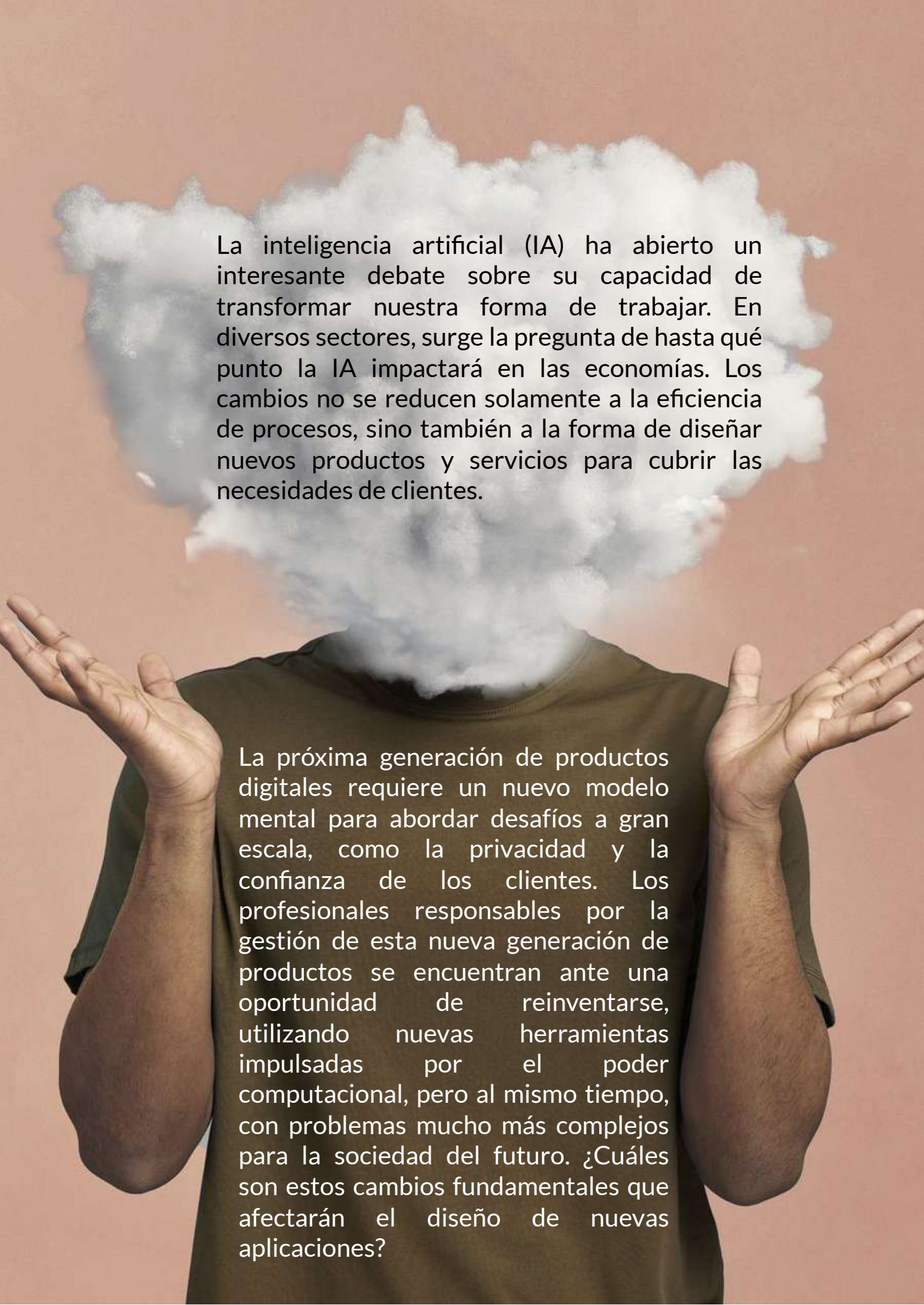
Official E-Commerce Reseller yubico

Compra tus YubiKeys en
smartmanagement.es

Ingeniero en Sistemas, MBA en Gestión Estratégica de Proyectos y especialización de Diseño de Servicios. Mas de 16 años trabajado con empresas de diferentes segmentos en el diseño e implementación de productos digitales, incluyendo innovaciones para SAP y Amazon. Cree en el poder del diseño y tecnología para generar grandes cambios en la vida de las personas.

# IA

## Y GESTIÓN DE LA NUEVA GENERACIÓN DE PRODUCTOS DIGITALES



La inteligencia artificial (IA) ha abierto un interesante debate sobre su capacidad de transformar nuestra forma de trabajar. En diversos sectores, surge la pregunta de hasta qué punto la IA impactará en las economías. Los cambios no se reducen solamente a la eficiencia de procesos, sino también a la forma de diseñar nuevos productos y servicios para cubrir las necesidades de clientes.

La próxima generación de productos digitales requiere un nuevo modelo mental para abordar desafíos a gran escala, como la privacidad y la confianza de los clientes. Los profesionales responsables por la gestión de esta nueva generación de productos se encuentran ante una oportunidad de reinventarse, utilizando nuevas herramientas impulsadas por el poder computacional, pero al mismo tiempo, con problemas mucho más complejos para la sociedad del futuro. ¿Cuáles son estos cambios fundamentales que afectarán el diseño de nuevas aplicaciones?

# Diseño Computacional

El diseño, como práctica, está en constante evolución. En su esencia, cada vez que diseñamos una solución estamos en búsqueda del mismo objetivo: identificar una necesidad específica y encontrar la mejor solución posible. Pero a lo largo de nuestra historia su influencia se ha ido expandiendo en diferentes áreas, desde su tradicional aplicación al mundo físico (arquitectura, industria, moda) hasta su más reciente versión en el mundo empresarial con el famoso 'Pensamiento de Diseño' o Design Thinking, buscando equilibrar la viabilidad empresarial, la tecnología y las necesidades de los clientes. La adopción de tecnología en nuestra vida diaria y el crecimiento exponencial del poder de procesamiento de datos ha dado lugar a una nueva era del diseño: el Diseño Computacional. En esta nueva vía, el diseño gana una nueva perspectiva, pasando de la experiencia empírica y conocimientos de los profesionales, a hacer uso de aplicaciones y algoritmos para resolver problemas. Parámetros, modelos y contenido generado automáticamente, se han transformado en la nueva caja de herramientas para la creación y mejora de nuevos productos digitales.

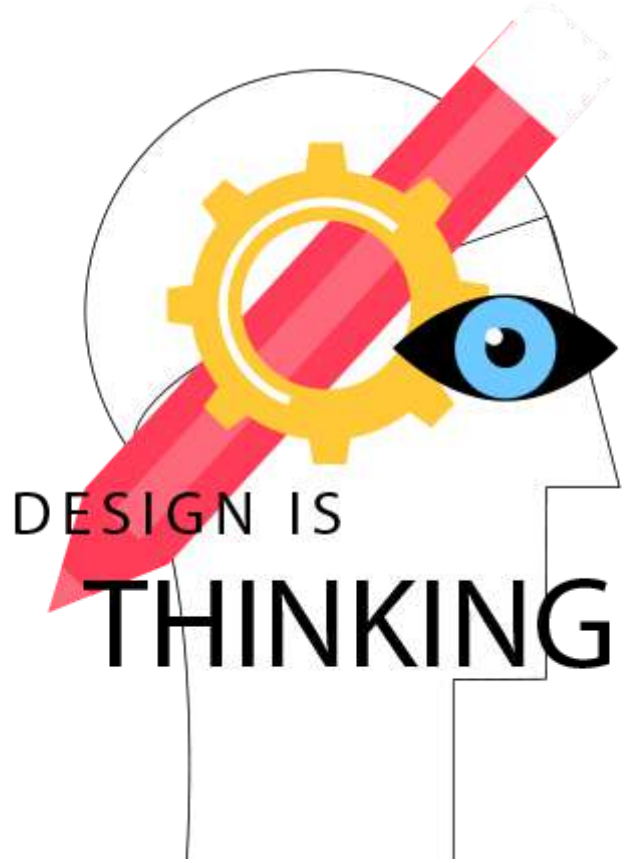
Tecnologías como IA se están transformando en un diferencial competitivo para empresas que diseñan nuevos productos, aumentando la eficiencia y generando soluciones más robustas. De cierta forma, la IA ha eliminado la barrera de entrada para muchos profesionales interesados en el diseño de nuevas aplicaciones: con el uso del conocimiento colectivo es posible identificar necesidades de clientes, idear posibles soluciones, realizar pruebas de concepto e incluso desarrollar aplicaciones de prueba sin necesidad de programar código. Podríamos usar una analogía: de la misma forma que los lenguajes de programación abstrajeron algoritmos y procesos computacionales complejos, la IA está creando este tipo de abstracción para diseño. En el campo del diseño, la IA viene a ser una herramienta poderosa tornando los datos, a gran escala, el activo más importante durante el proceso.

Sin embargo, a medida que nuevas herramientas han transformado la forma de diseñar soluciones, la complejidad de los problemas ha cambiado de forma significativa. La productividad y personalización de aplicaciones que hacen uso de tecnologías como IA viene acompañada de desafíos como la privacidad, ética e inclusión. Empresas y startups dispuestas a innovar no pueden ignorar estos factores si quieren ser competitivos y mantener la confianza de sus clientes. Estos elementos que hace algunos años parecían opcionales o, cuanto menos, recomendados, pasan a ser la base fundamental durante el proceso de diseño. La nueva generación de aplicaciones deberá continuar enfocada en el usuario, pero también deberá inspirar confianza, hacer uso correcto e intencional de datos y contar con mecanismos de transparencia para la toma de decisiones.

# Gestión de la nueva generación de Productos Digitales

El diseño computacional ha cambiado la forma de crear nuevas soluciones. Dirigir el ciclo de vida de nuevos productos digitales, desde su introducción hasta su madurez, requiere de nuevas herramientas y técnicas. Algunos cambios importantes en esta gestión incluyen:

# El uso de IA como acelerador




La dinámica tradicional de divergencia y convergencia del Design Thinking ganan una nueva perspectiva con el uso de IA. El entendimiento de un problema u oportunidad de los usuarios puede ser complementado con el uso de herramientas generativas, aprovechando grandes volúmenes de datos para encontrar tendencias y nuevas perspectivas. Las empresas están comenzando a hacer uso de herramientas como ChatGPT para auxiliar investigaciones de mercado o análisis de sentimiento de clientes. Las sesiones de ideación (brainstorming) pasan a ser más interactivas, descubriendo conexiones con soluciones de problemas similares. Finalmente, la creación de prototipos y pruebas de concepto se pueden optimizar mediante simulaciones y visualización basadas en IA.

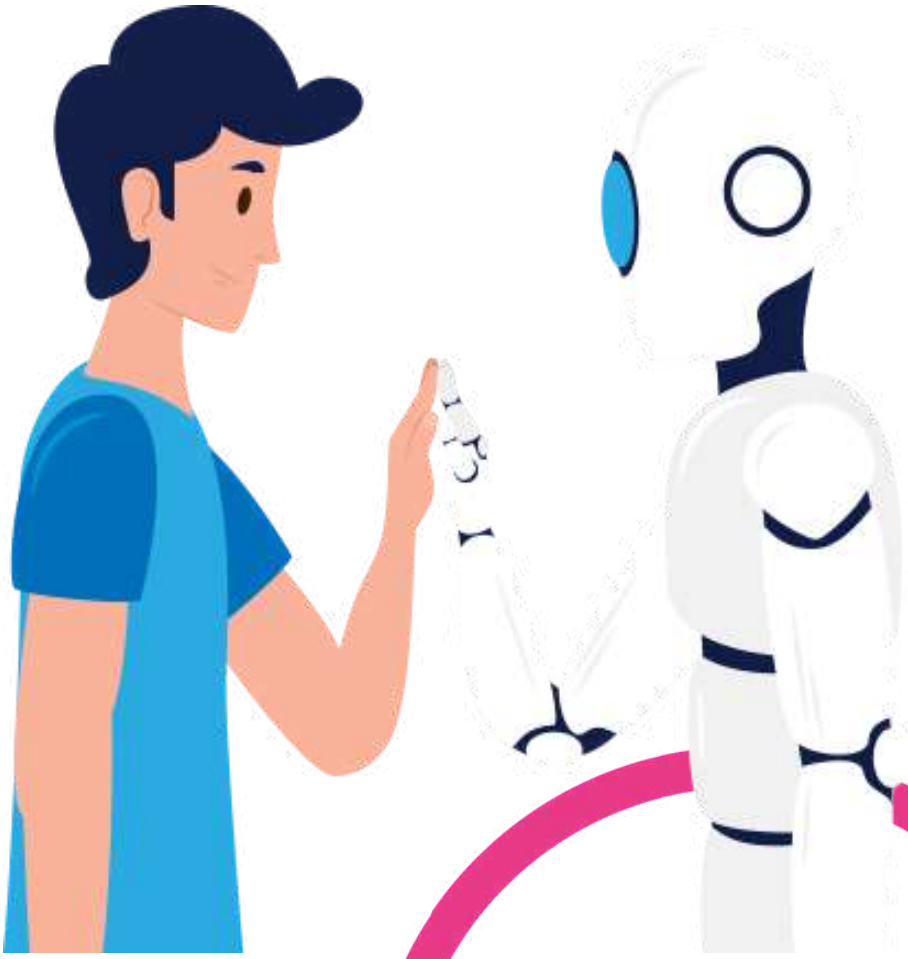
# Privacidad by-design.

La nueva generación de productos opera sobre una nueva 'economía de confianza'. Clientes que no confían en un producto, lo dejarán de usar rápidamente. La privacidad debe ser parte integral del proceso de diseño desde el inicio. Esto quiere decir que como responsables por el diseño de una nueva aplicación nos debe preocupar de igual forma elementos de usabilidad (UX) como los derechos de acceso a los datos, políticas de retención, la seguridad & almacenaje y hacer uso de la información con el propósito intencional. La confianza de los clientes en una empresa estará directamente relacionada con el cuidado que esta tenga con sus informaciones.

# Ética

IA ya forma parte de nuestras vidas y la tendencia es tornarse un elemento integral de cualquier producto y servicio del futuro. Cuando hablamos de ética, abrimos un espacio amplio y complejo por la búsqueda de equilibrio entre conceptos como justicia, prejuicios y responsabilidades de sistemas, especialmente cuando estos son usados para la toma de decisiones. Las nuevas tecnologías, en especial la IA, son abstractas y en algunos casos difíciles de interpretar. Por tanto, el diseño de experiencias debe tener en cuenta la transparencia de cómo dichos sistemas toman soluciones, y una identificación continua donde prejuicios den paso a resultados que puedan excluir, ofender o impactar, en otras formas, la vida de los usuarios. El diseño debe llevar en consideración los impactos de segundo-tercer orden para anticipar cualquier efecto no deseado.

# Un futuro virtuoso



Son muchos los desafíos pero, en igual o mayor número, son las oportunidades y beneficios de los productos digitales del futuro. Nos encontramos ante un cambio fundamental en la forma en que diseñamos, operamos y mejoramos soluciones que pueden agregar valor, no solo a problemas de negocios, sino también a retos sociales como la salud, la educación y el crecimiento económico. Se trata de una oportunidad para reinventarse.

OPTIMUS

# EDR

Endpoint Detection & Response

# TODO INCLUIDO

## SIN COSTE ADICIONAL

**FUNCIONES *INCLUIDAS***

CTI
(ANÁLISIS AUTOMÁTICO Y EN TIEMPO REAL)
+
SANDBOX
+
INTELIGENCIA ARTIFICIAL
+
PLATAFORMA DE INTELIGENCIA DE AMENAZAS
(THREAT HUNTING Y ANÁLISIS FORENSE)


## PROTEJA SUS ENDPOINTS
DE FORMA HIPERAUTOMATIZADA

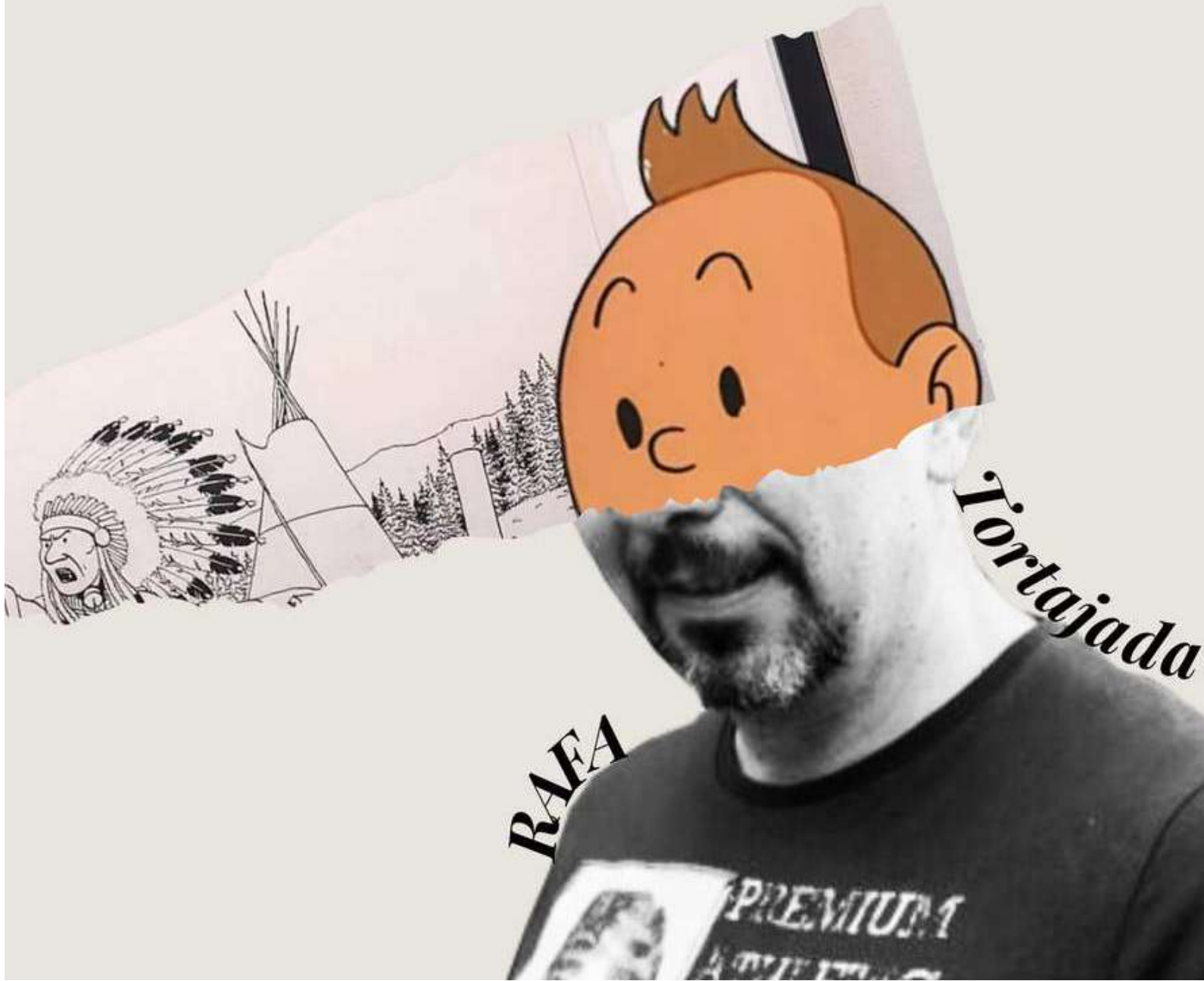
CONTACTE
CON NOSOTROS
spain@tehtris.eu
tehtris.com

TEHTRIS
FACE THE UNPREDICTABLE

Ingeniero de Telecomunicaciones, master en gestión de empresas de Telecomunicaciones Politécnica Madrid, Master en Gestión de la seguridad Telefónica/Univ Alcalá

Apasionado de la tecnología y de los deportes cuando puedo. También me encanta dar clases y charlas sobre tecnología y seguridad

Actividad profesional: Telefónica e Ingecom S.L



# VEHÍCULOS AUTÓNOMOS

**Los sistemas informáticos han ido revolucionando nuestro entorno desde hace relativamente poco; ¿qué son 40 años desde que se empezó a comercializar masivamente esta tecnología?**

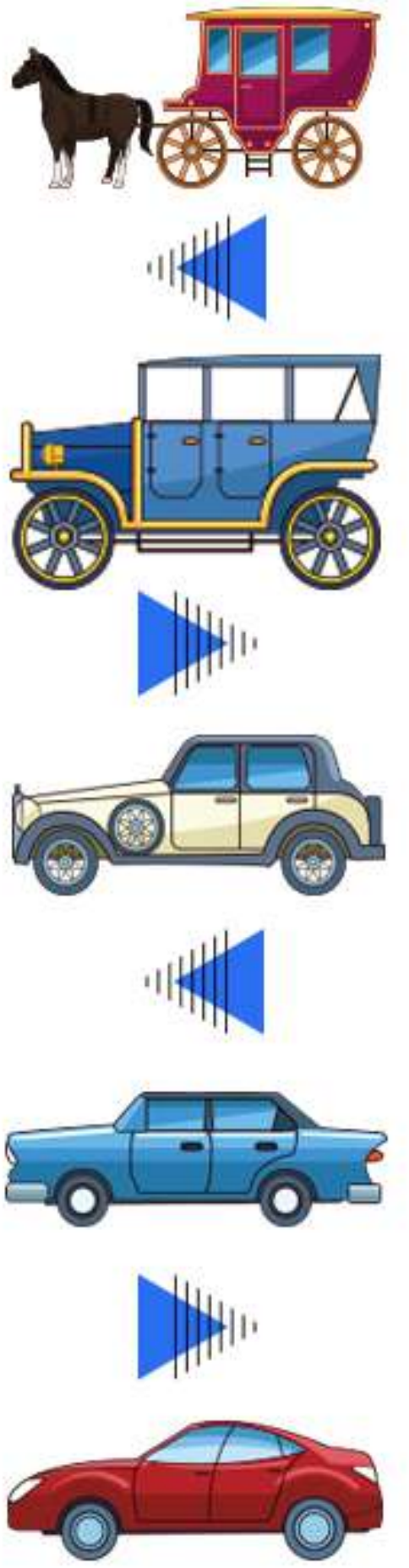
Esta revolución empezó en otro sector como el automovilístico hace algo más de 100 años, pasando de “conducir” animales como caballos y sus carretas, a empezar a conducir vehículos de motor que cambiaron tanto el panorama como las reglas, ya sea en ciudades como en carreteras. Ahora estamos viviendo una nueva revolución y es el vehículo autónomo.

Cada vez tenemos más automatismos en los vehículos que nos ayudan en la conducción, está normalizado desde hace décadas el coche automático, tenemos control de crucero, control de carril, control de distancias con radar, sensores de presencia de viandantes, cámaras traseras y delanteras, sensores para ayuda e incluso hay coches que pueden aparcar solos y un largo etc. de soluciones cada vez más automatizadas. Entre ellas tenemos una SIM conectada en nuestro vehículo. Así que gradualmente hemos ido aumentando la cantidad de contenido autónomo dentro de un vehículo.

Todas estas ayudas son bien recibidas y, ahora, estamos por dar el siguiente paso que son los coches autónomos, pero para recorrer este camino, debemos realizar otra revolución y avances importantes, como ya ocurrió hace 100 años. El objetivo final es que estos vehículos no necesiten ni volante, ni aceleradores, ni frenos, y solo les tengamos que decir dónde queremos ir para que nos lleven.

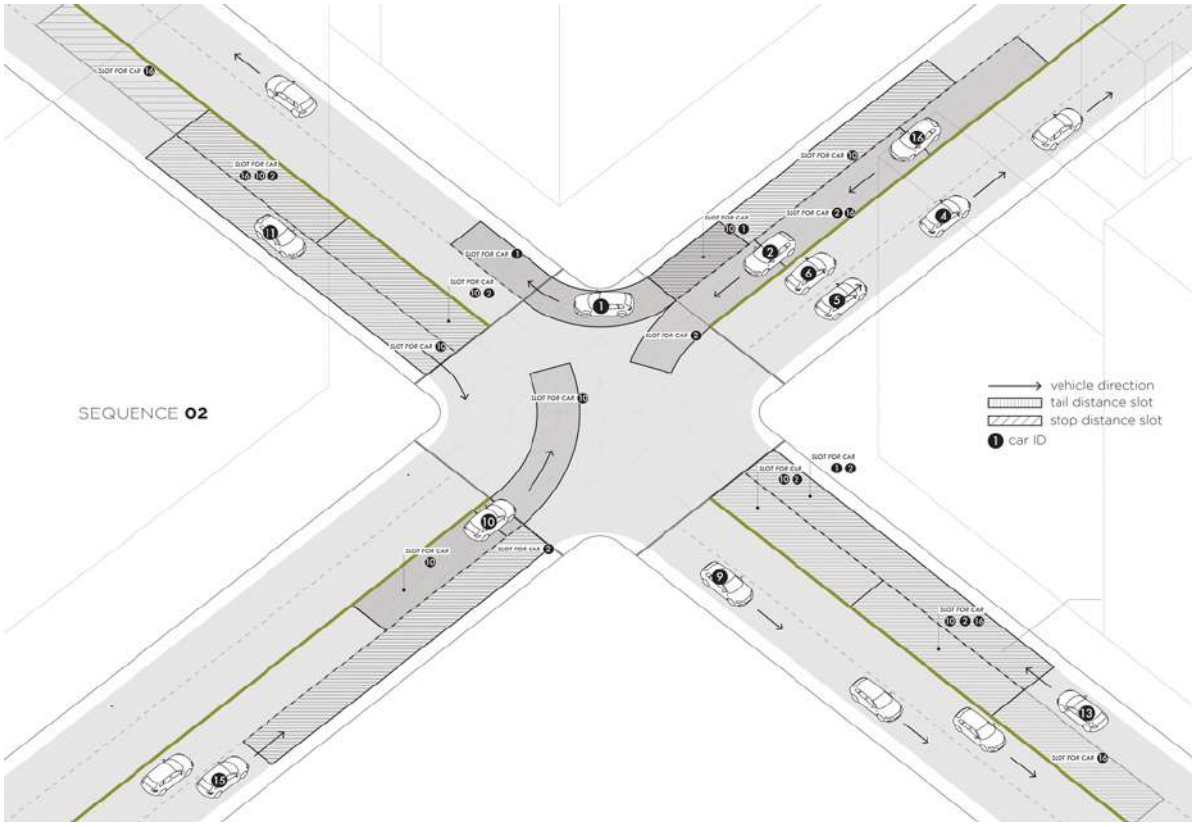
Para llegar al punto final de tener un vehículo totalmente autónomo nos encontramos con múltiples retos y no solo el rechazo o desconfianza de parte de la población (a esto se contesta sabiendo que los aviones se pilotan de forma autónoma y pueden aterrizar de igual manera), sino también retos tecnológicos.

# Desafío vehículos autónomos vs conducción humana



Uno de los principales desafíos para los vehículos autónomos en la vía pública es la cooperación y colaboración seguras entre múltiples vehículos utilizando la percepción basada en sensores y las comunicaciones entre vehículos. El problema surge cuando varios vehículos autónomos intentan ocupar el mismo espacio simultáneamente [1], esto hace que pueden chocar entre sí, quedar bloqueados o frenar bruscamente, lo que hace que sea incómodo o inseguro para los pasajeros de un vehículo autónomo. Hay multitud de escenarios en una conducción real en la que debemos adelantar, cambiar de carril etc., por ejemplo, pensemos en una intersección: con un coche autónomo tendremos que prever hacia dónde va a girar un vehículo o si va a seguir recto, si debemos cambiar de carril y además cálculos sobre velocidad y aceleración. Para minimizar el impacto sobre los tiempos de espera y el consumo, las tomas de decisión de cada vehículo, deben ser instantáneas y comunicadas al resto de vehículos en tiempo real. Aquí hay otro problema que surge: la adopción del vehículo autónomo, como la evolución de vehículos tirados por caballos al vehículo de combustión que no fue inmediata y convivieron durante años, no se va a producir directamente, sino que habrán muchos años de convivencia, por lo que los algoritmos que deben llevar los vehículos autónomos han de tener en cuenta que tendrán que interactuar con vehículos conducidos por humanos.

En un futuro con la adopción total del vehículo inteligente, veremos la muerte de los semáforos, según un estudio del MIT [2] junto con el Instituto Suizo de Tecnología y el Consejo Nacional de Investigación de Italia, tuvieron la idea de un nuevo tipo de intersección llamada Light Traffic. Su sistema usaría sensores para mantener a los automóviles sin conductor a una distancia segura entre sí y asignaría a cada automóvil una ranura de cruce cuando llegue a un cruce. Las velocidades se ajustarían automáticamente al acercarse para garantizar que los vehículos se turnen para cruzar sin tener que detenerse.

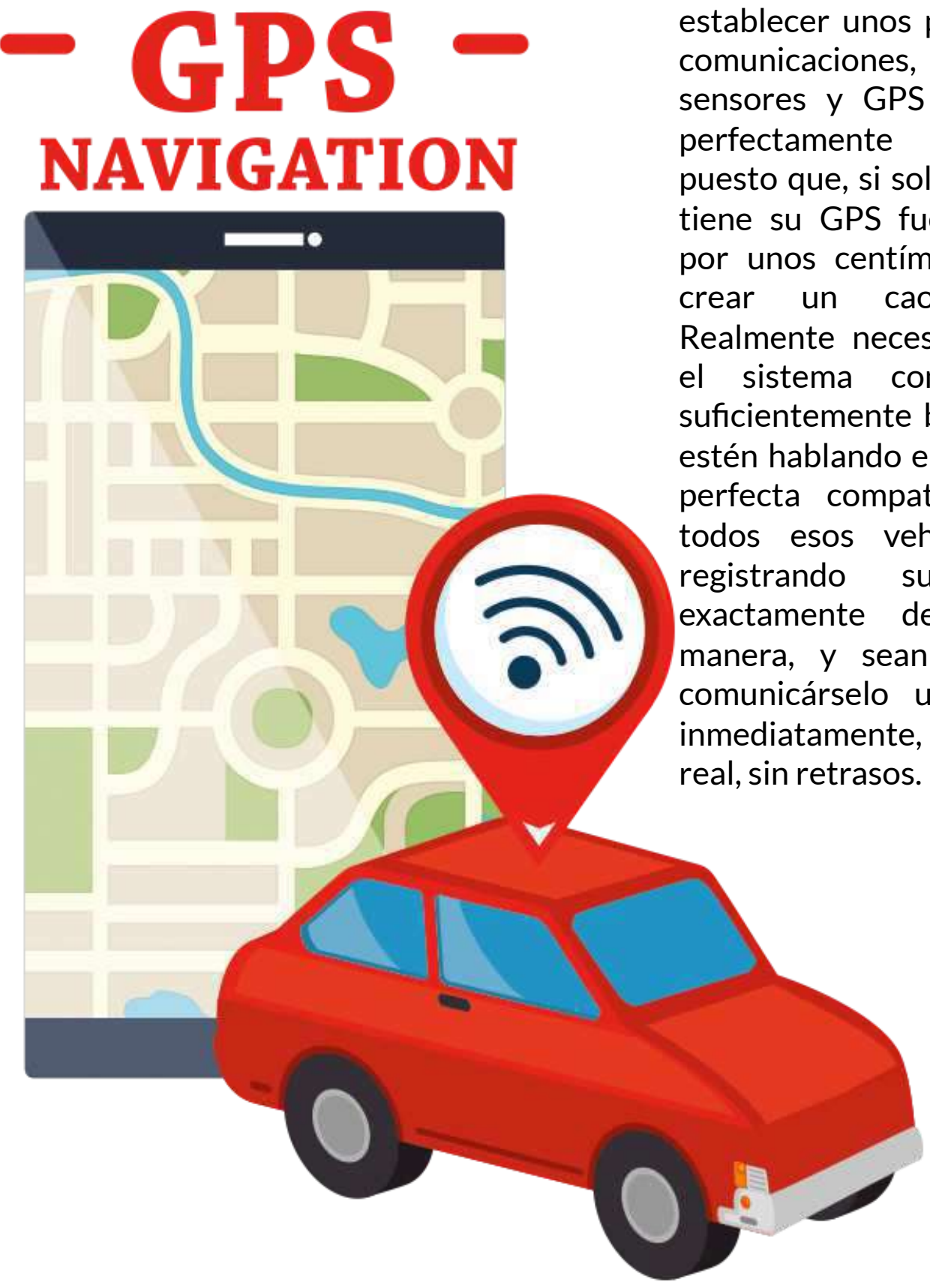



Como ventajas de este sistema tendríamos:

***Reducir drásticamente la cantidad de contaminación emitida por los vehículos que esperan, que estarían quemando combustible innecesariamente.**
***Podrían pasar el doble de automóviles por los cruces en la misma cantidad de tiempo que en las intersecciones controladas por semáforos.**
***Reducir el tiempo del viaje**

Con algoritmos como los anteriormente mencionados, haría la conducción más segura y acercarían la movilidad a personas que por sus condiciones particulares sean dependientes de otros para ir a un lugar, al permitir el vehículo la completa autonomía de estos colectivos.

# Protocolos de vehículos inteligentes




Todo el intercambio de información necesario entre los vehículos inteligentes y su entorno, se ve ligado a establecer unos protocolos de comunicaciones, así como los sensores y GPS deben estar perfectamente calibrados puesto que, si solo un vehículo tiene su GPS fuera de rango por unos centímetros, podría crear un caos absoluto. Realmente necesitamos tener el sistema configurado lo suficientemente bien para que estén hablando entre ellos con perfecta compatibilidad, que todos esos vehículos estén registrando su ubicación exactamente de la misma manera, y sean capaces de comunicárselo unos a otros inmediatamente, en tiempo real, sin retrasos.

Una serie de objetivos convergen en torno a la necesidad de que los sistemas del vehículo se comuniquen con su entorno y entre sí [3]:

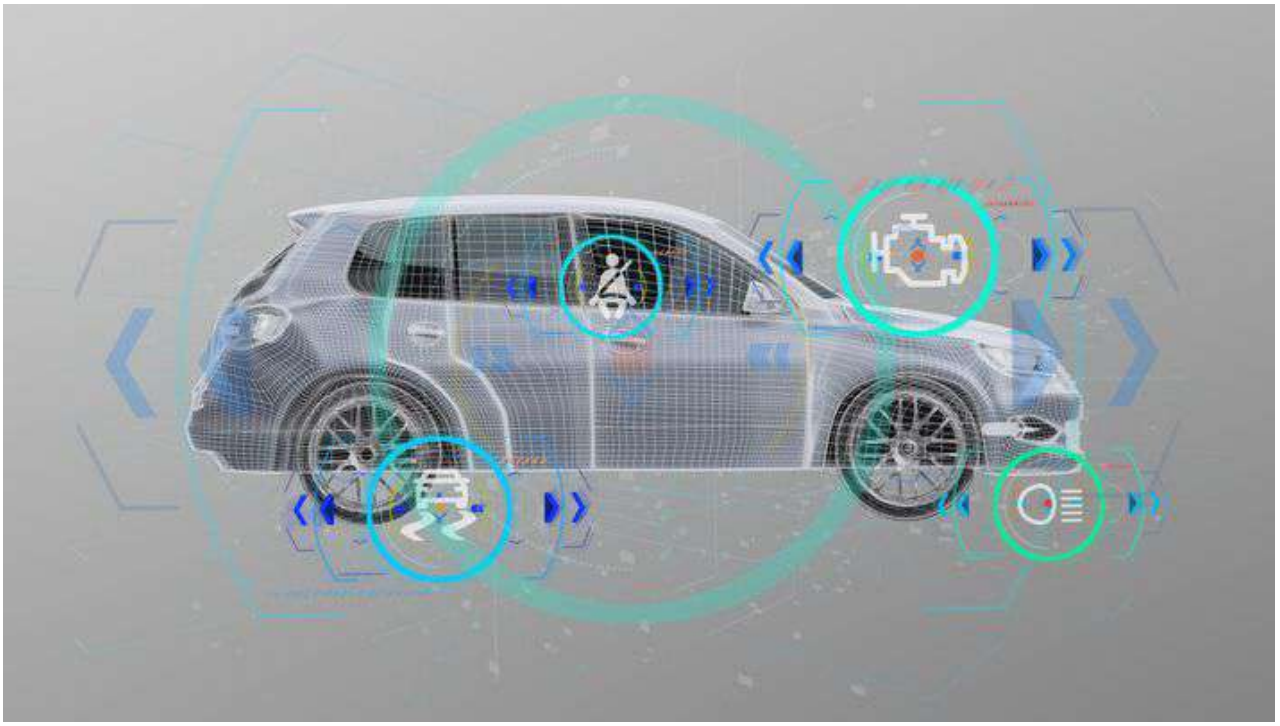
*Los ADAS (Sistemas Avanzados de Asistencia al Conductor) son sistemas de seguridad activos y pasivos diseñados para eliminar el componente de error humano, al operar vehículos de muchos tipos. El papel de ADAS es prevenir muertes y lesiones al reducir el número de accidentes automovilísticos y el impacto grave de aquellos que no se pueden evitar.

*Conectividad a Internet para información y entretenimiento de los pasajeros.

*Gestión remota en tiempo real en respuesta a las condiciones de tráfico en vivo, para mejorar el rendimiento de la flota de vehículos y reducir el gasto de combustible.

*Interacción con semáforos y otras infraestructuras viales para optimizar la eficiencia del tráfico.

*Disponibilidad de estacionamiento automático y otras funciones de conveniencia para el conductor.



QUENTA
SOLUTIONS

# OBSERVABILITY

APPLICATION PERFORMANCE MANAGEMENT

Las soluciones de observabilidad o APM (Application Performance Management) permiten a las organizaciones vigilar las métricas de rendimiento de sus aplicaciones corporativas críticas, al mismo tiempo que se adquiere información para, de forma proactiva, mejorar las prestaciones de dichas aplicaciones y la experiencia de los usuarios.

- Conocer el tiempo de respuesta del 100% de las transacciones de negocio.
- Diagnosticar problemas de rendimiento en producción y desarrollo (disminución del MTTR).
- Monitorizar las aplicaciones, llegando hasta el nivel de código en cada transacción.
- Detectar la causa raíz de los problemas en las aplicaciones.
- Monitorizar cada interacción del usuario final con las aplicaciones (métricas en tiempo real).
- Monitorizar la infraestructura que soportan todas las aplicaciones y servicios.
- Trazabilidad end to end a través de todas las capas y tecnologías.

910 516 779

info@quenta.es

C/ Cidro 2
Planta 2, Oficinas 2 y 3, 28044 Madrid

Para todos estos requisitos nace el protocolo V2X (Vehicle-to-everything). Este protocolo se dedica a la comunicación entre un vehículo y cualquier otra entidad con la que se relaciona o puede verse afectada. En este sistema de comunicación la información de los sensores y otras fuentes viaja a través de enlaces de alta confiabilidad, baja latencia y gran ancho de banda, allanando el camino hacia la conducción totalmente autónoma.

V2X está formado a su vez por diferentes protocolos:

***Vehículo a vehículo V2V: permite que los autos autónomos habilitados para V2X se comuniquen entre sí.**

***Vehículo a infraestructura V2I: permite que los automóviles autónomos obtengan información de edificios, puentes, carreteras, semáforos, etc.**

***Vehículo a peatón V2P: utiliza sistemas de detección de peatones que pueden funcionar con el ADAS de un automóvil.**

***V2H Vehicle-to-Home : los hogares inteligentes pueden enviar y recibir información directamente desde el automóvil.**

***V2N Vehicle-to-Network : esta es una conexión móvil desde el automóvil a la red celular de un proveedor.**

***V2C Vehicle-to-Cloud : brinda acceso directo a redes en la nube mediante conexiones TCP/IP seguras.**

Pero para que todo esto ocurra, se debe sustentar con un entorno de red que permita la comunicación entre las distintas entidades. Esta tecnología de red, utiliza señales inalámbricas de corto alcance para comunicarse mediante una red que cumple con sus estándares. Actualmente hay varios estándares que luchan por tener el control como son:

***802.11P DSRC- Ha sido desarrollado como una enmienda a las especificaciones del estándar IEEE 802.11 para soportar la comunicación ad-hoc entre vehículos y entre el vehículo y la red de infraestructura. IEEE 802.11p también se conoce con nombres como WAVE (Wireless Access for Vehicular Environments o Acceso inalámbrico para entornos vehiculares) y DSRC (Dedicated Short Range Communication o Comunicación dedicada de corto alcance). La red formada por dispositivos compatibles con 802.11p se conoce como VANET (Vehicular Adhoc Network .**

***C-V2X.- El Cellular V2X (C-V2X) es un estándar del 3GPP que describe una tecnología para lograr los requisitos de V2X . C-V2X es una alternativa a 802.11p , el estándar especificado por IEEE para V2V y otras formas de comunicaciones V2X. Cellular V2X utiliza conectividad celular móvil 4G LTE o 5G estandarizada por el 3GPP para enviar y recibir señales de un vehículo a otros vehículos, peatones u objetos fijos como semáforos en sus alrededores. Por lo general, utiliza la banda de frecuencia de 5,9 GHz para comunicarse, siendo esta la frecuencia designada oficialmente como sistema de transporte inteligente (ITS) en la mayoría de los países. C-V2X se desarrolló dentro del Proyecto de Asociación de Tercera Generación (3GPP), para reemplazar las Comunicaciones Dedicadas de corto alcance (DSRC) promovidas por los EE. UU**

Como se puede apreciar ya hay discrepancias e intereses entre diferentes partes para establecer un patrón común. En los vehículos autónomos y conectados no vale que una marca, país o región usen unos protocolos y otros no; la interoperabilidad ha de ser única.

Y si todo esto no fuese un gran problema, hay una serie de barreras existentes para la comunicación V2X como son:

*Integración con sistemas heterogéneos

- Múltiples sistemas de posicionamiento por satélite.
-Proliferación de sensores, giroscopios, radares etc.
-Tecnologías de información abordo, tanto internas como externas.
-Telecomunicaciones externas.
-Un panorama cambiante de comunicación V2X tecnologías, que actualmente incluyen ITS-G5 (en Europa), WAVE-DSRC (en EE. UU.) y CCSA (en China) basadas en el protocolo WiFi IEEE 802.11p, pero que podrían extenderse a una capa física celular, como LTE-V o 5G.

*Alta complejidad técnica: Cada sistema V2X deberá interactuar en muchos frentes, incluidos varios que son inalámbricos o se basan en tecnologías que son nuevas y, hasta el momento, no completamente probadas. Esto, y la gran cantidad de tecnologías que deben combinarse y priorizarse dentro de una sola estructura, hacen que desarrollar un vehículo conectado sea una tarea compleja y multidisciplinaria.

*Satisfacer requisitos estrictos: Antes de que un sistema V2X se considere aceptable para el mercado, deberá ofrecer altos estándares de manera constante en una variedad de requisitos

-Funcionalidad: el sistema debe comportarse consistentemente como el usuario espera.
-Interoperabilidad: Los vehículos deberán comunicarse con otros de diferentes marcas.
-Seguridad: el sistema no debe poner en peligro al conductor.
-Calidad de servicio: a medida que los vehículos se conectan cada vez más, es esencial verificar que las redes del vehículo funcionen como deben.
-Homologación.

*Susceptibilidad a la interferencia del canal: Cualquier canal de comunicación inalámbrica que utilice un sistema V2X podría verse afectado por la interferencia de la señal y otras deficiencias. Esto puede incluir la falta de cobertura, la carga de la red, la interferencia atmosférica, las obstrucciones físicas y la interferencia deliberada o accidental de fuentes de RF de alta potencia.

*Mejorar la seguridad frente a los ciberataques: Todo sistema tan conectado ha de estar blindado ante un ciberataque que podría parar la circulación y poner vidas en peligro.

*Cumplir con la legislación regulatoria y la estandarización: Como hemos visto, hay diferentes normas y estándares, y el reto será tener estándares propios para la tecnología de Vehículos Autónomos independientemente del país, marca etc.

Como resumen, la creciente integración de V2X, ADAS y sistemas automatizados presenta a los ingenieros una serie de desafíos, en particular, la interoperabilidad y la seguridad cibernética. Estos serán los puntos claves para el avance de los vehículos conectados.

# Ejemplo de vehículo autónomo

La universidad de Curtin [4] es la primera universidad australiana en probar un autobús comercial sin conductor. Este piloto contribuirá al creciente campo de investigación en tecnología de conducción automatizada.
El autobús autónomo de Curtin es 100 % eléctrico y utiliza programación digital de entrada, sensores remotos y GPS para determinar su ruta y sortear obstáculos.
El autobús puede transportar hasta 11 pasajeros y conducir con seguridad hasta 45 km por hora. Un técnico viaja en el autobús para monitorear su desempeño y puede operar manualmente los controles si es necesario.
Los vehículos autónomos transformarán no sólo la forma en que viajamos, sino también la forma en que nos relacionamos con nuestra comunidad y el medio ambiente. Algunos de estos posibles cambios positivos incluyen:

***Transporte más seguro y sostenible.**
***Más opciones de movilidad para personas que no pueden conducir (como personas mayores o personas con problemas de visión).**
***Reducción de la congestión del tráfico y la contaminación acústica.**
***Transformación del trazado urbano (se requieren menos viales y aparcamientos).**
***Costes de transporte más asequibles.**
***Aumentos en la conectividad cultural y el compromiso.**

La tecnología de vehículo autónomo va progresando rápidamente, pero como hemos podido ver en este artículo, aún tenemos muchas cosas y escollos que salvar. Pero como todo cambio tecnológico que afecta a las personas debe ser probado, homologado y después ir poco a poco entrando en nuestras vidas, algo que, en un futuro cercano, se acometerá.

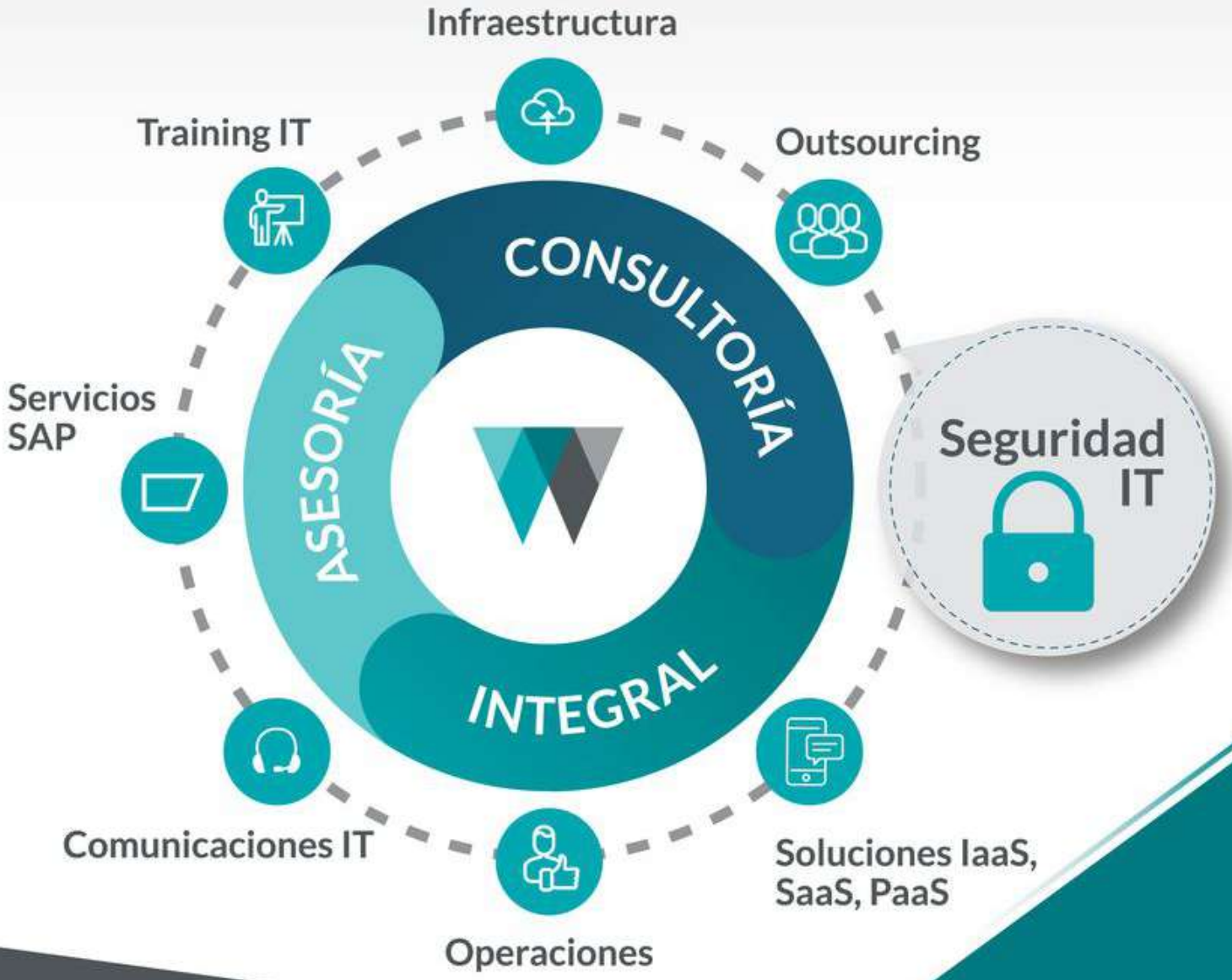
Referencias

[1]https://www.researchgate.net/publication/315914521_A_merging_protocol_for_self-driving_vehicles
[2]https://www.dezeen.com/2016/03/21/light-traffic-junctions-mit-research-smart-intersections-design-driverless-vehicles/#:~:text=A%20group%20of%20researchers%20has,need%20for%20signals%20(%2B%20movie).
[3] https://www.spirent.com/campaign/testing-v2x-systems?utm_medium=digital+ppc&utm_source=google&utm_campaign=automotive&utm_term=v2x%20standards&gad=1&gclid=Cj0KCQjwsIejBhDOARIsANYqkD1FtGSOpLxYajzDTppbtOs5rsT8J6-lvRCPIB0-boC8XaZ-AqROHegaAlj-EALw_wcB
[4] https://research.curtin.edu.au/facilities/driverless-bus/

WEZEN

# Gestión Integral de IT

***Ayudamos a nuestros clientes a mejorar y crecer a través de servicios tecnológicos punta a punta.***




*Together IT is better.*

WEZENGROUP.COM

Conocido como @holesec en las redes sociales, con más de 20 años trabajando en el mundo de la ciberseguridad, actualmente es el Responsable de Plataformas, Innovación y Talento en el CCI. Expositor en grandes conferencias y docente Universitario, autor de un libro y ha desarrollado su carrera en elm undo de la ciberseguridad desde diferentes perspectivas, en pymes, en startups, en corporaciones internacionales, en empresas de oil and gas, como researchers, como consultor… Persona técnica pero muy enfocado a humanizar los conceptos para que todos se suban al mundo de la ciberseguridad.

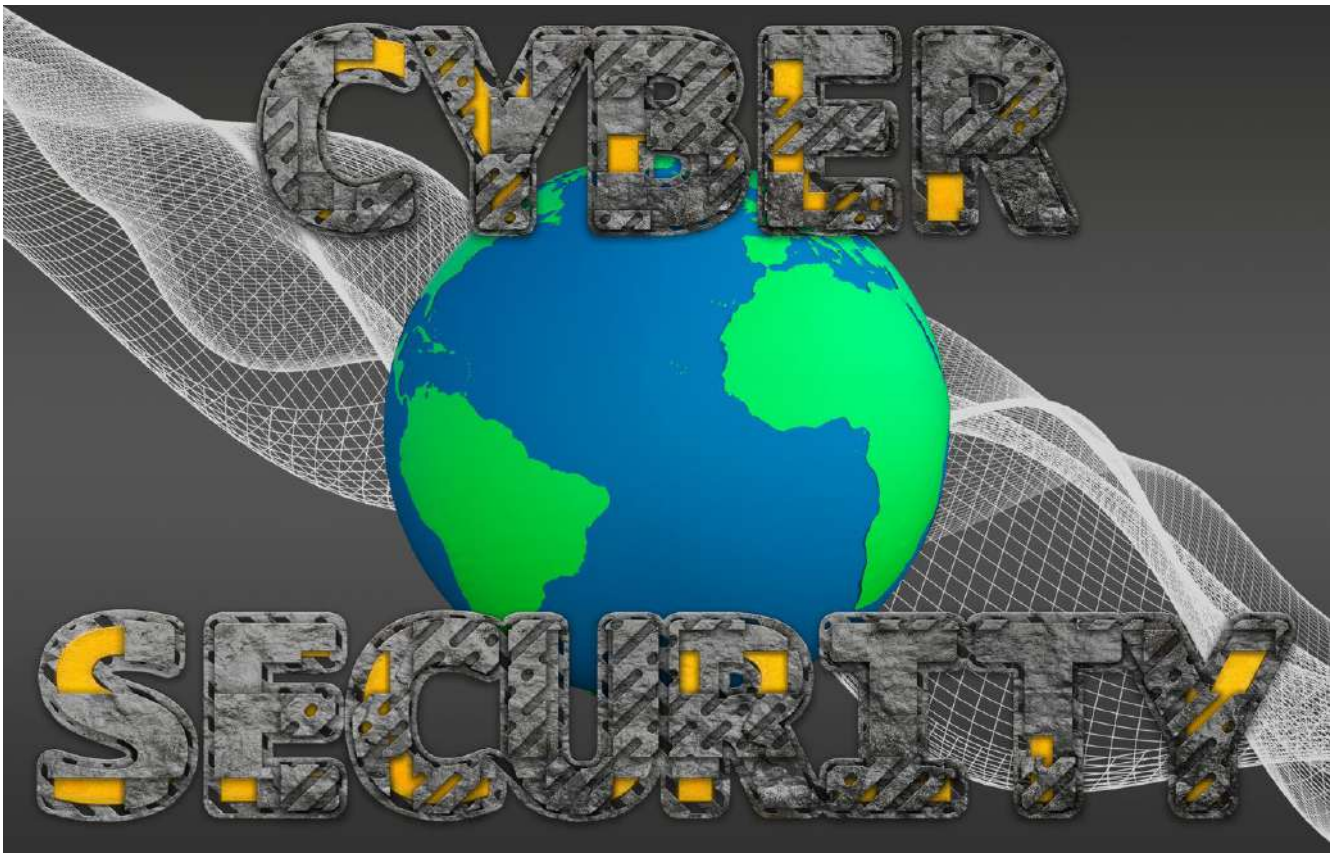

# Hacia una cultura de ciberseguridad industrial, más allá de los requisitos.

Hace tan solo unos 10 años, cuando el CCI estaba naciendo, las charlas sobre Ciberseguridad en las redes industriales eran muy sencillas de dictar. En casi todos los escenarios de protección la respuesta era: “no hay tecnología suficientemente probada para esto aún…” Hoy en día, y con gran admiración por el rápido desarrollo del mercado en esta línea, el discurso es totalmente distinto: hemos visto desarrollarse nuevas soluciones y servicios para el mercado, formarse cientos de profesionales en el ámbito, y hasta incluso hemos visto nacer tanto conferencias como compañías exitosas dedicadas exclusivamente al epígrafe de la ciberseguridad industrial.

Es cierto que todo el ecosistema ha crecido, incluso a nivel político muchos países han adaptado o incorporado a su legislación temas relacionados a la ciberseguridad en entornos industriales (más especialmente enfocados a infraestructuras críticas), y también hemos visto una gran evolución en la generación de material, normas y estándares, herramientas de auditoría y de gap análisis para ayudar a las empresas a desarrollar estrategias de protección. Pero no todo es un camino bonito y lleno de flores, porque a medida que la cuarta revolución avanza, las organizaciones industriales deben adquirir una agilidad para adaptarse al cambio que no es normal en el área pero que el mundo interconectado y digitalizado sí exige.

Mas allá de los esfuerzos de muchas organizaciones por mejorar, no es representativo el número de ellas tratando de ser más seguras si dejamos de lado las infraestructuras críticas que están obligadas en muchos lugares. Aún hoy día nos toca ver que, la mayoría de las solicitudes de nuevos proyectos en el ámbito industrial, no pasan por las áreas de Ciberseguridad (claro que incluso hay organizaciones que ni tienen un área de Ciberseguridad) y, por ende, siguen sin incluir los famosos 7 (siete) requisitos fundamentales (FR) que tan clara y criteriosamente fueron definidos por la, a esta altura ya famosa, ISA/IEC 62443. En términos generales, esto es algo que debe preocuparnos como profesionales y a lo que nos debemos dedicar en dar a conocer.

Quienes trabajaron en el desarrollo de la ISA/IEC 62443 y quienes trabajan en la actualización de todos sus documentos, tienen muy presentes que cada requisito de ciberseguridad independientemente de a que requisito fundamental (FR) pertenezca, está asociado a los niveles de seguridad (SL) que cada organización requiera según legislación o normativa vigente, visión de negocio o necesidad de mercado. Este tipo de documentos no se mete o entromete en la madurez que debe tener una organización, sino que parte desde sus necesidades para definir los requisitos obligatorios.



Actualmente, muchas de las herramientas en el ámbito de la Ciberseguridad Industrial fueron pensadas para implementar controles, para monitorear o bien para auditar o realizar algún tipo de análisis de seguridad, sin embargo muy pocas fueron diseñadas para ayudar a definir los requisitos de seguridad que cada Zona o Conducto, con sus componentes correspondientes, deben cumplir en un proyecto industrial. Estos son los momentos en donde una organización sin fines de lucro como la nuestra, el Centro de Ciberseguridad Industrial, ve la oportunidad de ayudar y colaborar con sus miembros poniendo a disposición herramientas, en este caso como RECIN (la cual fue pensada para educar y ayudar a los profesionales a definir qué requisitos fundamentales (FR) deben cumplir y además sobre cómo encontrar soluciones y servicios de distintos proveedores para poder cumplirlos.

El cambio en el sector, no sólo se genera desde la posición de las grandes empresas y de las consultoras, sino que se genera desde el pequeño accionar que cada profesional en este ámbito puede realizar, porque no se trata de solamente de cumplimiento, sino que de ir más allá, de hacer las cosas bien porque vale la pena hacerlas bien, porque vale la pena tener industrias más seguras para nuestra sociedad. En el CCI lo hacemos a partir de generar espacios de encuentro virtuales o físicos, de publicar documentos, de participar en foros y revistas, de sentarnos a tomar un café con responsables de plantas, fabricantes, consultores, académicos, organizaciones estatales y demás actores, tratando siempre de inculcar una cultura de ciberseguridad industrial, pero sobre todo una cultura basada en el compartir experiencias para hacernos más fuertes y seguros.

Desde el ámbito de la Dirección en una organización industrial hasta el técnico de planta que define los requisitos, o desde quien define una normativa a nivel gubernamental hasta quien hace una consultoría de cumplimiento, todos tenemos responsabilidad para lograr una industria más segura y para que los atacantes tengan menos oportunidades de generar daños a la sociedad o a una industria en particular.

En el CCI ponemos a disposición muchas cosas de nuestros miembros, desde herramientas como RECIN hasta documentos realizados por expertos. Y sabemos que el camino hacia la cultura de la ciberseguridad industrial no es fácil… no lo era hace 10 años, no lo es ahora tampoco, pero en 10 años vimos muchos cambios, y nos enorgullece ser parte de ello. La ciberseguridad no es parte de nuestro trabajo, es una parte de quienes somos y de cómo nos enfrentamos al mundo de los cambios constantes.

# Evolved intelligence against evolved threats

ravenloop

## Sin ciberinteligencia no hay ciberseguridad

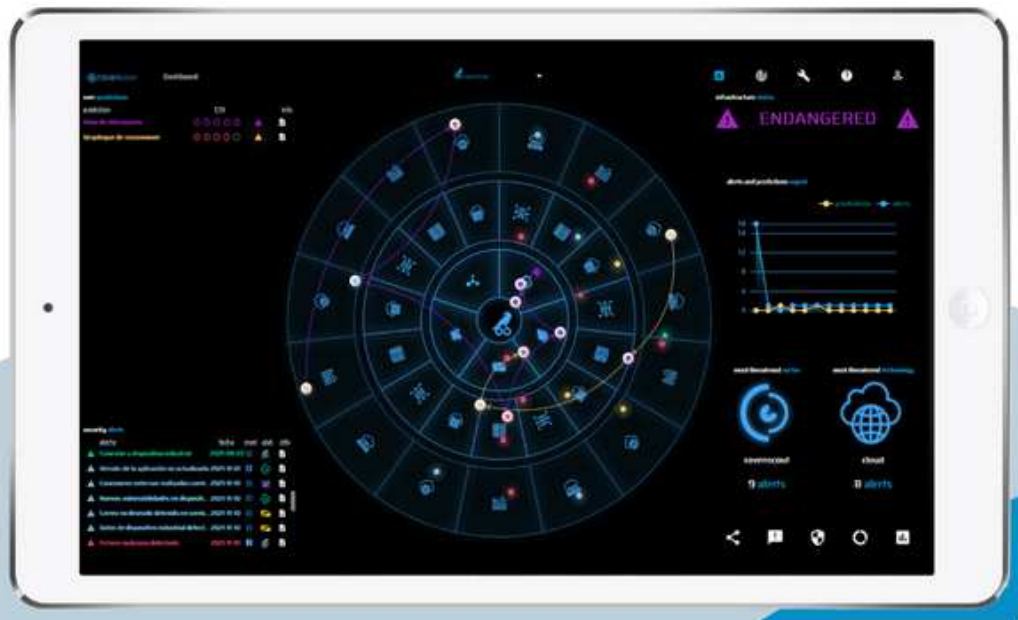
Brechas de seguridad, ataques de ransomware, APTs... cada vez más sofisticados, más personalizados, los nuevos ciberataques se basan en el conocimiento profundo de sus víctimas y en el uso de amenazas desconocidas para burlar los sistemas convencionales de protección.
Los datos para identificar estas nuevas amenazas están ahí, al alcance de la mano pero los analistas de seguridad tienen serios problemas por el volumen de información y por la complejidad del proceso.

## Ravenseer plataforma de ciberinteligencia predictiva

Ravenseer es la última y más compleja pieza del arsenal de ciberdefensa de Ravenloop. Mientras que las otras plataformas se enfocan en la defensa de cada uno de sus vectores, Ravenseer centraliza todos los eventos, alertas, amenazas y anomalías una vez que salen de los motores de Machine Learning. Este es solo el primer paso para predecir con precisión los ataques cibernéticos, completamente interactiva y personalizada. Su modelo de Inteligencia Artificial en constante evolución se alimenta de toda esta variedad de elementos seleccionados para que pueda comenzar el proceso de correlación y predicción

## Bienvenido a la evolución de la ciberinteligencia.

ravenseer




### Acerca de RavenLoop

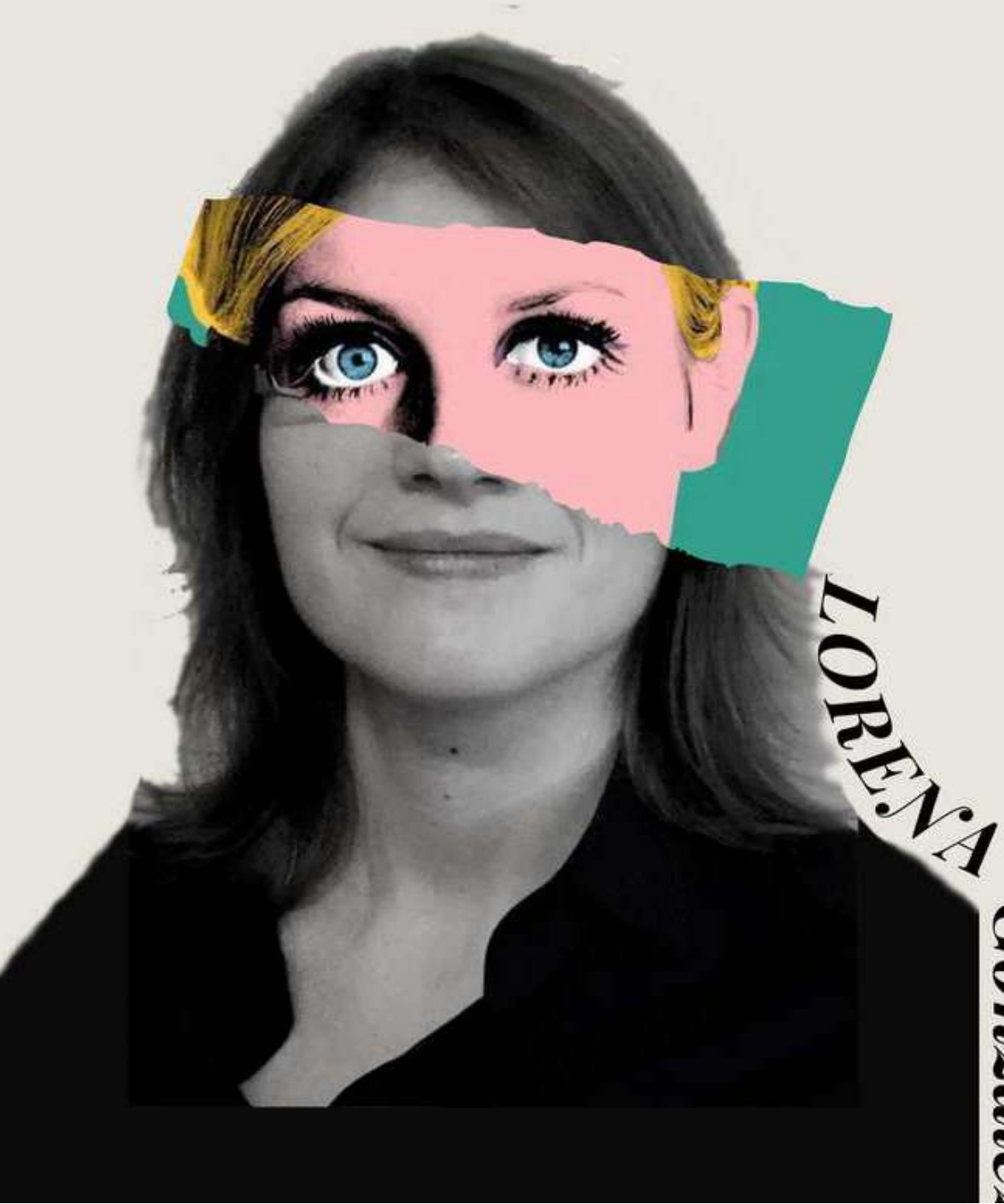
En un mundo digital e interconectado, con ataques cada vez más sofisticados, personalizados y numerosos, aportamos información crítica y conocimiento profundo sobre amenazas, fundamental para extraer todo el potencial de sus soluciones de ciberseguridad y garantizar la resiliencia de su organización.

Ravenloop
Avda Fuente Nueva 12A
28703 San Sebastian de los Reyes - Madrid
Telf: +34 912532315
contacto@ravenloop.io

ravenloop.io

# RINCÓN DEL CISO

Profesora Titular de la Universidad Carlos III de Madrid, en el Computer Security Lab (COSEC). Trabaja en el campo de la ciberseguridad y actualmente se enfoca en la seguridad en el internet de las cosas y las amenazas persistentes avanzadas. Además, es docente en múltiples Grados y Másteres, y también participa en tareas de divulgación.



LORENA González

# Caracterizando ciberamenazas avanzadas aprovechando recursos públicos

Lorena González Manzano


Las empresas de ciberseguridad trabajan constantemente para identificar y eliminar malware, pero los ataques están en aumento, infectando a más dispositivos que nunca. De hecho, según Kaspersky, se detectaron más de 164 millones de malware en el primer trimestre de 2020. Más allá del malware de uso general (en este caso troyanos y ransomware), una amenaza persistente avanzada (APT) es un sofisticado ataque a largo plazo, comúnmente realizado por motivos de ciberespionaje, lanzado contra una entidad objetivo y que hace uso de un conjunto de malware.

Así, se presenta un reto en establecer una diferenciación desde el punto de vista técnico entre programas malignos de uso general y aquellos que se emplean como parte de ataques dirigidos, llamados malware y APT respectivamente de aquí en adelante.

Para realizar la distinción de malware y APT, lo cual es un campo poco explorado, se ha trabajado, por ejemplo, en técnicas de análisis de código y trazas de tráfico [1]. Sin embargo, aquí se plantea el uso de técnicas y tácticas (T&T) en base a MITRE ATT&CK [2] (repositorio y marco de trabajo para proporcionar información y clasificación de ataques reales), donde táctica se define como, ¿qué es lo que el atacante desea conseguir? y técnica se define como las distintas formas para alcanzar el objetivo deseado. Así, se ha trabajado con 12 tácticas y cada una de ellas con un conjunto de técnicas, dando lugar a un total 266 técnicas.

Se comienza seleccionando troyanos y ransomware, por ser malware con características semejantes a una APT, de fuentes relevantes tales como VirusTotal o Malpedia, llegando a obtener 126.376 muestras. Igualmente, se recopilaron muestras de APT, un total de 13.704. Posteriormente se selecciona Hybrid Analysis como herramienta de libre acceso para obtener ATT&CK T&T, por ser una de las que más cantidad de T&T proporcionaba. De ahí se obtiene el conjunto final de datos, formado por 4.686 muestras de APT y 11.651 muestras de malware con sus respectivas T&T.

El primer análisis realizado es un estudio estadístico con el test de Fisher, haciendo uso de la cantidad de T&T por muestra recogidas, para saber si es posible una diferenciación de malware y APT. Una vez planteada la hipótesis de que ambos conjuntos son distintos, el resultado del test avala la aceptación de la hipótesis y, por tanto, es posible continuar con el estudio.

# ANÁLISIS

La segunda parte se basa en realizar un análisis de prevalencia considerando la diferencia en cantidad de técnicas por táctica que hay en cada tipo de malware y en el conjunto de APT. Con esto se persigue estudiar las técnicas más prevalentes en ambos conjuntos. Es posible concluir que hay técnicas como T1179 (Credential API Hooking) y T1215 (Kernel Modules and Extensions) que son más prevalentes en APT, lo cual ocurre porque son técnicas que ayudan tanto a la prevalencia de un malware en un sistema, como a la escalada de privilegios, así como la modificación del kernel para facilitar la carga de información en los sistemas bajo demanda del atacante. En cambio, también se aprecian técnicas como T1053 (Scheduled Task/Job), que ayudan a la ejecución de malware de forma programada y que son más prevalentes en malware.

La caracterización de los atacantes se complementa haciendo uso del modelo TEACH [3], basado en, por cada técnica, establecer si son técnicas que por sí mismas no permiten la explotación (T), técnicas que cualquiera las puede explotar (E), técnicas que requieren pasos adicionales para ejecutarse (A), técnica que requieren de una infraestructura adicional para aplicarse y por tanto, es costoso (C), y técnicas que requieren gran conocimiento de sistemas operativos y hardware (H). El análisis permite determinar que las APT, en línea con lo esperado, utilizan más técnicas “H” y, por ello, requieren no solo experiencia técnica sino también amplios recursos. Un ejemplo de ello son las técnicas incluidas dentro de la táctica TA0005 (Defense evasion), lo cual se considera crítico ya que se espera que las víctimas de APT sean de alto perfil presumiblemente con un fuerte nivel de defensa.

Finalmente, se aplican algoritmos de inteligencia artificial, en concreto, el vecino más cercano (KNN), Random Forest (RF) y perceptrón multicapa (MLP) considerando el balanceo de clases en su ejecución. Se estudia la posibilidad de clasificar APT y malware a nivel de T&T aplicando estos algoritmos. Los resultados demuestran que KNN produce ligeramente mejores resultados considerando los tipos de malware estudiados. KNN es igualmente preferible sólo considerando troyanos y, en cambio, RF es mejor alternativa al evaluar sólo ransomware.

En resumen, este trabajo, del que se puede leer la publicación completa en [4], lleva a cabo un análisis de más de 15,000 muestras de malware de troyanos y ransomware y de APT para construir una sólida diferenciación técnica entre ambos conjuntos y también contribuir al análisis de la competencia de los atacantes. Se ha hecho uso del modelo TEACH para determinar la profundidad técnica de cada T&T de MITRE ATT&CK, y se ha evaluado la efectividad haciendo uso de algoritmos de inteligencia artificial para clasificar las muestras con las que se ha trabajado.

[1] L. F. Martín Liras, A. R. de Soto, and M. A. Prada, "Feature analysis for data-driven apt-related malware discrimination," Comput. Secur., vol. 104, no. C, may 2021.
[2] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "Mitre att&ck: Design and philosophy," in Technical report. The MITRE Corporation, 2018.
[3] The MITRE Corporation. (Last accessed May 2022) MITRE ATT&CKcon 2018.ATT&CK as a Teacher (Travis Smith, Tripwire). [Online]. Available: https://attack.mitre.org/resources/attackcon/
[4] L. González-Manzano, J. M de Fuentes, F. Lombardi, C. Ramos " A technical characterization of APTs by leveraging public resources".

# Estratec360

Tu reto nos inspira

*Expertos en cumplir las expectativas del cliente, asumir retos y mitigar riesgos*

## Continuidad de negocio

## Ciberseguridad

## Automatización

*Un servicio exclusivo en el que el cliente es el centro de nuestro trabajo, mediante transparencia y responsabilidad*


@estratec360

933803334

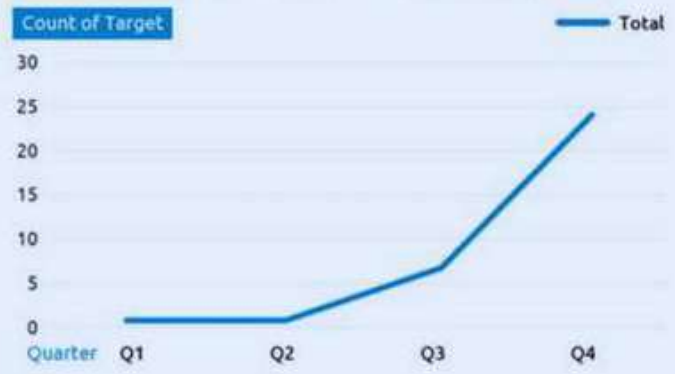
info@estratec360.com

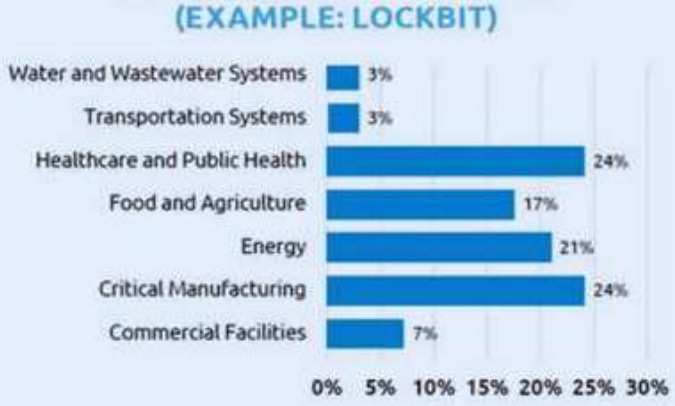
Cuenta con una experiencia de más de 20 años en el mundo de las TIC y la ciberseguridad. Pasando por todas las áreas de negocio: cliente final (OHL, Fertiberia y Grupo Villar Mir),integrador de soluciones y fabricante. Hasta 2023, desempeñó el rol de director de Alianzas Estratégicas en Trend Micro. Actualmente es director de estrategia de ciberseguridad en Trend Micro Iberia. Su reto actual es hacer entendible la ciberseguridad, sus riesgos, mejores prácticas y soluciones, intentando que el mundo conectado sea un lugar mejor para vivir.

# RESUMEN DE INCIDENTES EN EL MUNDO OT EN 2020 EL RANSOMWARE SE CEBA CON LOS ENTORNOS OT.

El panorama de ciberamenazas evoluciona al mismo ritmo que la tecnología, o incluso más rápido. Como resultado, una ciberseguridad insuficiente se ha convertido en una cuestión de seguridad nacional. La Industria 4.0 es un arma de doble filo, y los beneficios de la automatización y la conectividad conllevan riesgos significativos. A medida que más industrias adoptan la automación, la amenaza de ataques a la cadena de suministro se está convirtiendo en un peligro real y presente. Las organizaciones deben dar prioridad a la protección de la red OT como piedra angular de su estrategia de ciberseguridad. Sin embargo, una estrategia no puede formularse sin una comprensión clara de la amenaza que está contrarrestando.

Recientemente el equipo TXOne, una división de Trend Micro, ha publicado un informe que consolida y analiza los delitos cibernéticos y la actividad maliciosa en el ciberespacio, cuantificando además la cantidad de ataques e incidentes que vieron en 2022.
Sin duda alguna, la principal conclusión es que el ransomware ataca de forma especialmente agresiva al entorno OT.




# ATTACKS

SIN DUDA ALGUNA, LA PRINCIPAL CONCLUSIÓN ES QUE EL RANSOMWARE ATACA DE FORMA ESPECIALMENTE AGRESIVA AL ENTORNO OT.

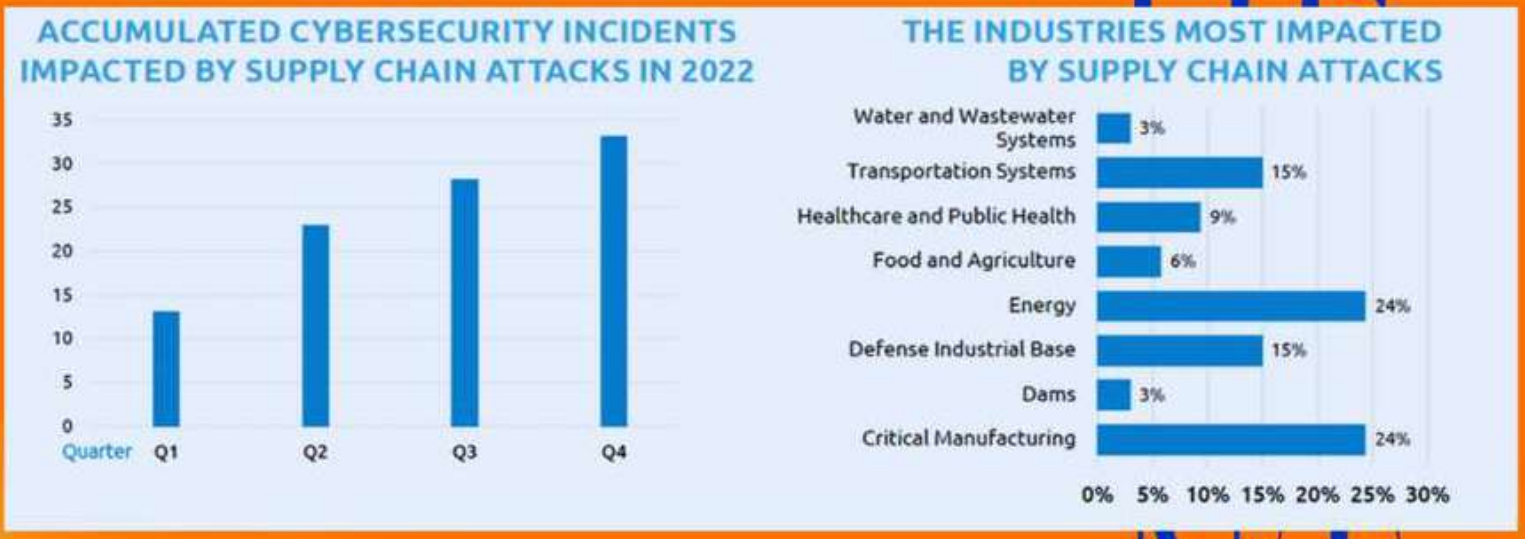
La modalidad ransomware-as-a-Service (RaaS) continúa adoptando el modelo de múltiple extorsión. En la segunda mitad de 2022, empezamos a ver un aumento de grupos criminales de RaaS como Black Basta y Pandora. Pero eso fue sólo el principio. El grupo LockBit 3.0 llevó las cosas a otro nivel con sus cibertácticas maliciosas, desde la destrucción de datos hasta la petición de rescates, incluso ofreciendo información robada a la venta en la Dark-Web.

Por desgracia, ninguna industria estaba a salvo: la fabricación inteligente, la energía y la alimentación y la agricultura se vieron afectadas con violencia, así como la atención médica y la salud pública, que experimentaron una mayor tasa de ataques a través de este modelo “as-a-service”.

Además, el ransomware está en constante evolución y utiliza técnicas sofisticadas para evadir el análisis. Por ejemplo, programas como Egregor y LockBit 3.0 requieren un parámetro secreto para que los investigadores comiencen a estudiar el código malicioso y utilizan tácticas de cifrado avanzadas como la codificación intermitente en pequeños fragmentos para reducir la intensidad de las operaciones de I/O de archivos y evitar el análisis y la detección estadísticos.

# LA CADENA DE SUMINISTRO SIGUE SIENDO UN DOLOR DE CABEZA Y ES UNO DE LOS PRINCIPALES VECTORES DE ENTRADA

INCIDENTS



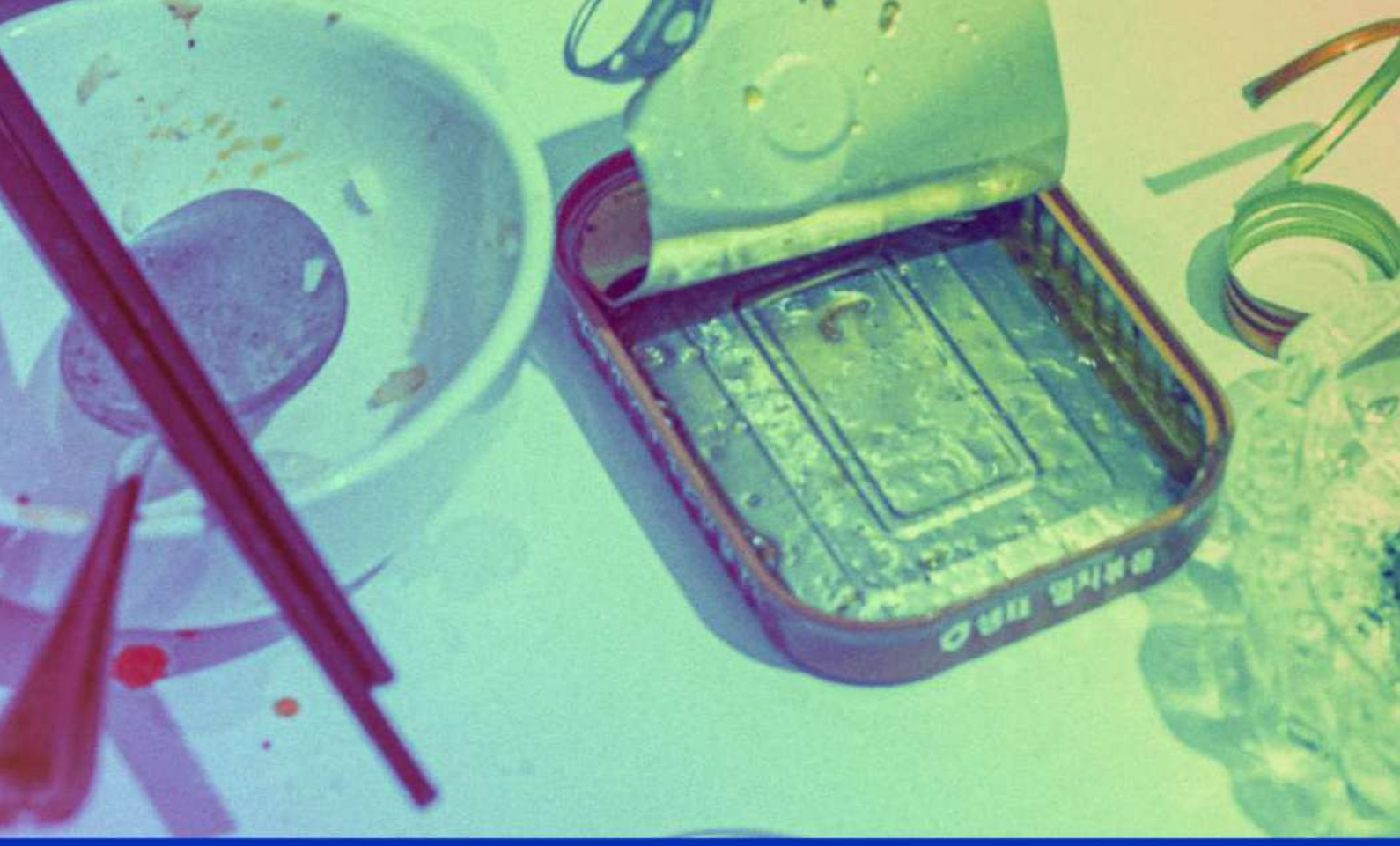
Desgraciadamente en 2022, los ataques a la cadena de suministro en los principales sectores se dispararon. Las industrias de energía y de fabricación crítica se enfrentaron (y se enfrentan) a un riesgo excepcionalmente alto de ataque a la cadena de suministro. De los ataques a la cadena de suministro en 2022, el 24% se produjeron en el sector energético y el 24% en la fabricación crítica.

Las fábricas de automóviles constituían la mayoría de ellos debido al crecimiento de la automatización en esta área, no olvidemos que lideran históricamente la transformación de los procesos productivos. El sector energético también sufrió un incremento significativo del nivel de riesgo debido, en gran parte, a las amenazas de los conflictos geopolíticos y la vulnerabilidad de las interdependencias con otros sectores.

# Fuerzas impulsoras del mercado de seguridad OT

En paralelo, TXOne llevó a cabo un estudio para entrevistar a propietarios de activos y partes interesadas relacionadas en Estados Unidos, Alemania y Japón para averiguar cómo están progresando en cada sector los entornos OT, y así comprender de una forma holística los problemas y causas actuales en un entorno altamente cambiante.

Por lo general, una transformación digital exitosa en la industria comienza identificando casos de aplicación clave y luego implementándolos a pequeña escala en las fábricas. El informe sugería algunos ejemplos.

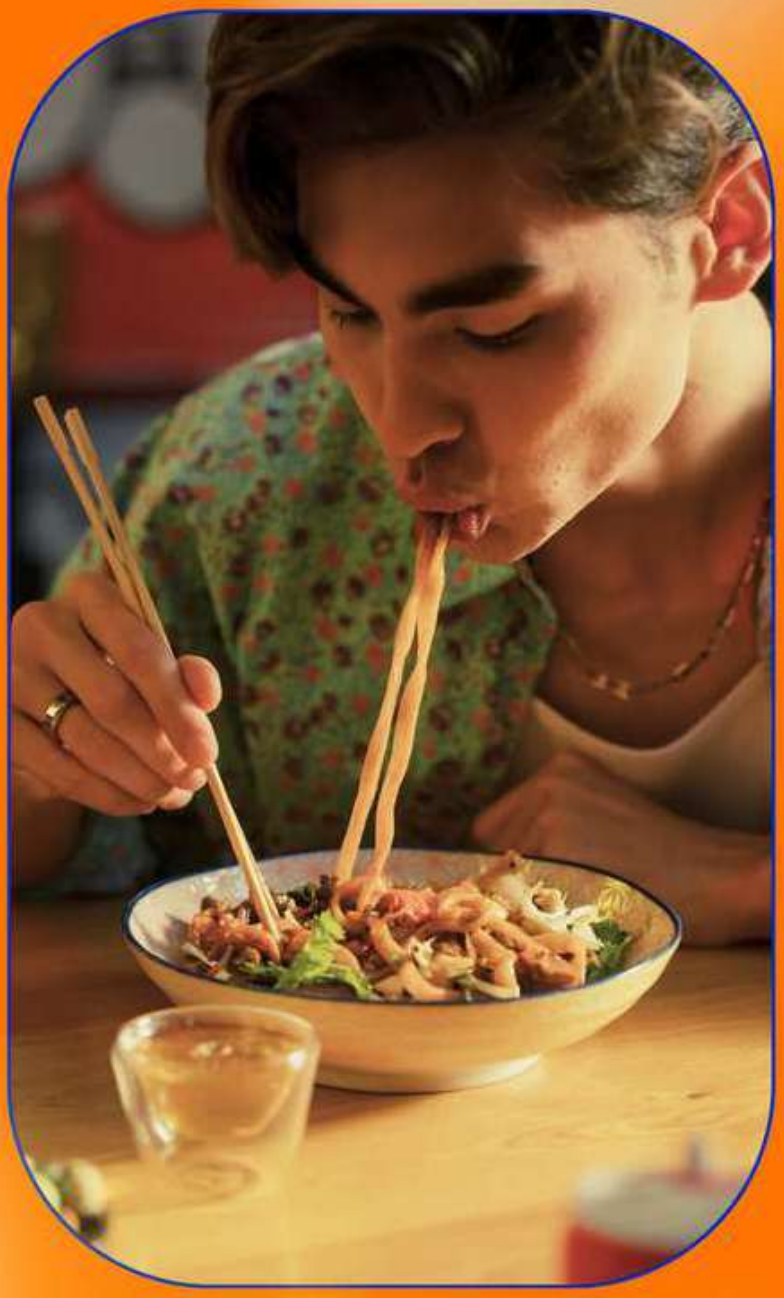


- Sector energético: los equipos de TI y OT pueden acceder de forma remota a los datos operativos para ayudar a las industrias (como las redes eléctricas, el petróleo y el gas) a optimizar el mantenimiento preventivo de los equipos de control industrial, realizar evaluaciones de daños y supervisar el control de inventario u optimizar la distribución de energía.

- Sector de fabricación: los equipos de TI y TO pueden utilizar sistemas automatizados de transferencia de materiales y brazos robóticos para la producción automatizada, ajustar los procesos de producción en tiempo real, mejorar la eficiencia de la producción y reducir los costes y los residuos de fabricación. Por ejemplo, el análisis de datos se puede utilizar para reducir el coste asociado a la electricidad o reducir el inventario redundante.

El informe también resume las regulaciones de ciberseguridad y las tendencias gubernamentales en cada país.

# ENCUESTA DE USUARIOS FINALES DE SEGURIDAD OT



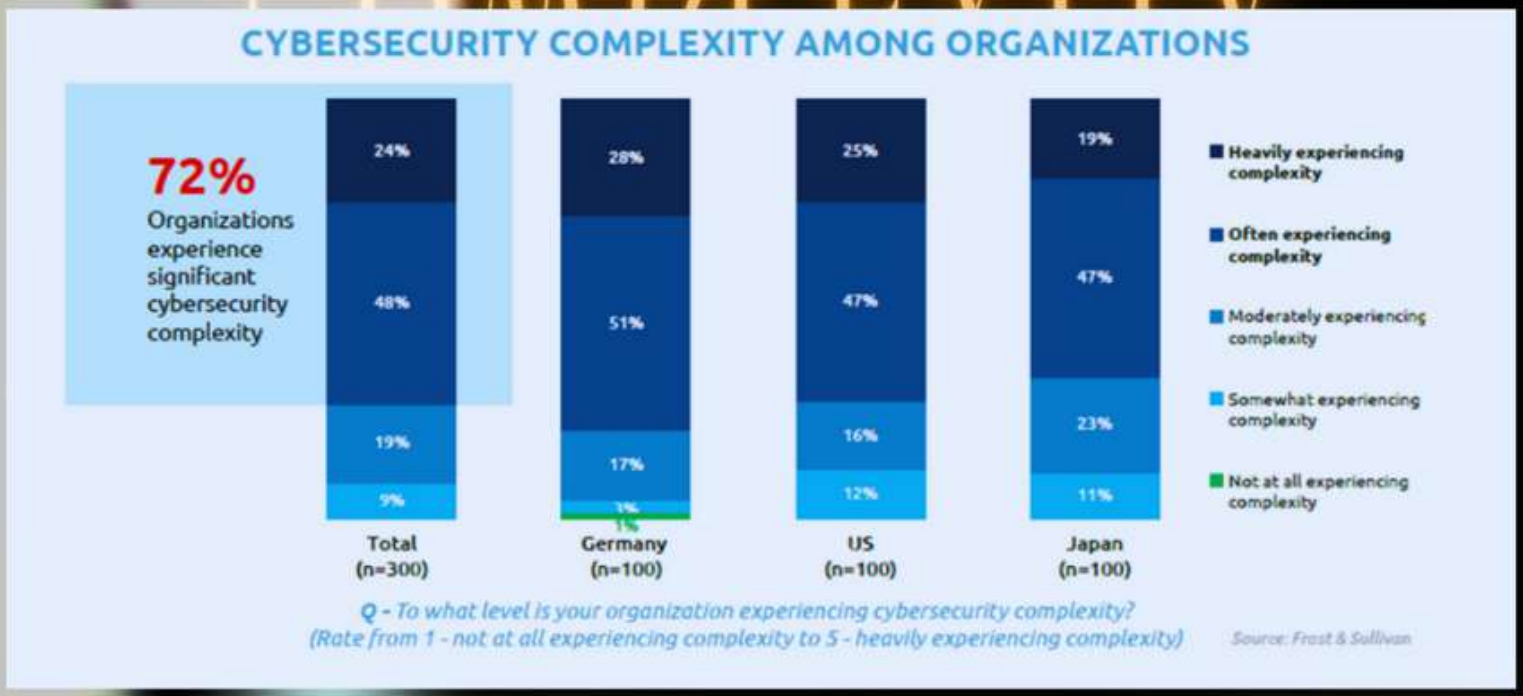
Frost and Sullivan, bajo petición de TXOne, realizó una encuesta mundial sobre el estado actual de la ciberseguridad de OT/ICS en la industria de producción de bienes, también conocida como manufacturing. El estudio entrevistó a responsables de la toma de decisiones y líderes en países de fabricación avanzada como Estados Unidos, Japón y Alemania, involucrando a 300 ejecutivos del área OT/ICS.

Las encuestas se llevaron a cabo en tres verticales principales, dividiendo los temas con tamaños de muestra aproximadamente equivalentes. El 34% procedía de la fabricación en general, el 33% de la fabricación de automóviles y el 33% del ámbito de la fabricación de productos farmacéuticos.

Frost and Sullivan, bajo petición de TXOne, realizó una encuesta mundial sobre el estado actual de la ciberseguridad de OT/ICS en la industria de producción de bienes, también conocida como manufacturing. El estudio entrevistó a responsables de la toma de decisiones y líderes en países de fabricación avanzada como Estados Unidos, Japón y Alemania, involucrando a 300 ejecutivos del área OT/ICS.

Las encuestas se llevaron a cabo en tres verticales principales, dividiendo los temas con tamaños de muestra aproximadamente equivalentes. El 34% procedía de la fabricación en general, el 33% de la fabricación de automóviles y el 33% del ámbito de la fabricación de productos farmacéuticos.

# CYBERSECURITY COMPLEXITY



Las organizaciones, de forma constante, se enfrentan a múltiples riesgos de seguridad; esta encuesta explora los puntos de vista actuales de los responsables de la toma de decisiones sobre el tema. Profundiza, por tanto, en descubrir sus desafíos mientras mide sus niveles de vulnerabilidad y resiliencia. Algunos de los hallazgos encontrados son los siguientes:

- El 72% de las organizaciones se enfrenta a la complejidad de la ciberseguridad. (24% experimenta mucha complejidad, 48% experimenta complejidad a menudo)
- El principal tipo de incidente de TI experimentado fue el ataque APT (33%), y el principal tipo de incidente de OT experimentado fueron los correos electrónicos de phishing destinados a penetrar en los sistemas (37%).
- La principal fuente de incidentes de OT son los nuevos activos que contienen vulnerabilidades/archivos maliciosos de forma predeterminada (47%).
- Las organizaciones ya han estado usando soluciones para la seguridad de OT (93%), planificando mejoras (85%) y aumentando la adopción con el gasto en seguridad de OT (76%).

**La mayoría de los propietarios de activos comprenden la diferencia entre el área de TI empresarial y los entornos ICS/OT. La evaluación para elegir una solución de ciberseguridad se puede dividir en tres aspectos.**

1. Aspecto estratégico: en general, la calidad añadida es la capacidad estratégica más importante para las empresas.
2. Aspecto operativo: la capacidad de integración con otras aplicaciones y tecnologías es la función operativa más importante para cualquier organización.
3. Aspecto de rendimiento: las organizaciones deben centrarse en el rendimiento y la disponibilidad para impulsar los resultados comerciales.

En definitiva, debemos ser conscientes de que las consecuencias de los ciberataques pueden ser graves y de gran alcance. El futuro de la seguridad OT requiere un conjunto de soluciones, habilidades, procesos y métodos de seguridad diferentes a los de TI. Construir ciberdefensas específicas para gestionar los riesgos de seguridad OT/ICS no es una opción; es una necesidad. No espere a que sea demasiado tarde: actúe con urgencia para protegerse y proteger a su organización de los ciberataques antes de que pueden causar daños irreparables.

Alfonso Calvo ha sido presidente de la Federación Coral de Madrid; tenor, gestor cultural y cineasta aficionado. Doctorando licenciado en informática por la Universidad Politécnica de Madrid. Posee 27 años de experiencia en la gestión de proyectos multinacionales sobre la integración de sistemas de información complejos. Está especializado en la resolución de crisis tecnológicas (ciberseguridad) y es autor de docenas de planes de protección de datos personales, de continuidad de negocio y recuperación ante desastres para grandes organizaciones públicas y privadas.

# IA EN OT

Alfonso Calvo

La inteligencia artificial (IA) ha experimentado un crecimiento exponencial en los últimos años, abarcando diversos campos y sectores, y la operación técnica (OT) no es una excepción. La IA puede utilizarse en la OT para mejorar la eficiencia, la fiabilidad y la seguridad de los procesos industriales, así como para la toma de decisiones en tiempo real.

La OT se refiere a los sistemas y procesos técnicos que se utilizan en la producción y el mantenimiento de bienes y servicios, desde la industria manufacturera hasta la infraestructura crítica, como la energía y los sistemas de transporte. La OT se caracteriza por procesos altamente automatizados, maquinaria especializada y un alto grado de control de procesos.

La IA puede aplicarse en la OT de diversas maneras, como en la supervisión y el control de procesos, el mantenimiento predictivo y la optimización de procesos. En la supervisión y el control de procesos, la IA puede utilizarse para analizar grandes cantidades de datos de sensores y otros dispositivos de monitorización para detectar problemas y tomar decisiones de control en tiempo real. Por ejemplo, en una planta de energía, la IA puede monitorizar la temperatura, la presión y otros parámetros para detectar problemas y ajustar el control de los sistemas de generación de energía.

El mantenimiento predictivo puede utilizar modelos de IA para predecir fallos y problemas antes de que ocurran, lo que permite a los operadores de la OT tomar medidas preventivas para evitar tiempos de inactividad costosos. Por ejemplo, en una fábrica de producción de alimentos, la IA puede analizar los datos de los sensores de temperatura y humedad para predecir cuándo se producirá un fallo en los sistemas de refrigeración, permitiendo a los operadores realizar el mantenimiento antes de que se produzca una avería.

La optimización de procesos puede utilizar modelos de IA para analizar los datos de los procesos y encontrar maneras de mejorar la eficiencia, reducir los costos y mejorar la calidad de los productos. Por ejemplo, en una planta de producción de papel, la IA puede analizar los datos de los sensores para encontrar la mejor combinación de presión, temperatura y otros factores para producir papel de alta calidad con el menor consumo de energía y materiales.

*En la OT, la toma de decisiones en tiempo real es crucial para garantizar la seguridad y la eficiencia de los procesos. La IA puede ayudar a los operadores de la OT a tomar decisiones rápidas y bien informadas en situaciones críticas. Por ejemplo, en una refinería de petróleo, la IA puede analizar los datos de los sensores para detectar fugas y otros problemas de seguridad y proporcionar recomendaciones de acción para los operadores.*

La implementación de la IA en la OT presenta una serie de desafíos que deben ser abordados para garantizar una integración efectiva y exitosa. A continuación, describiremos algunos de los principales problemas que deben ser considerados.

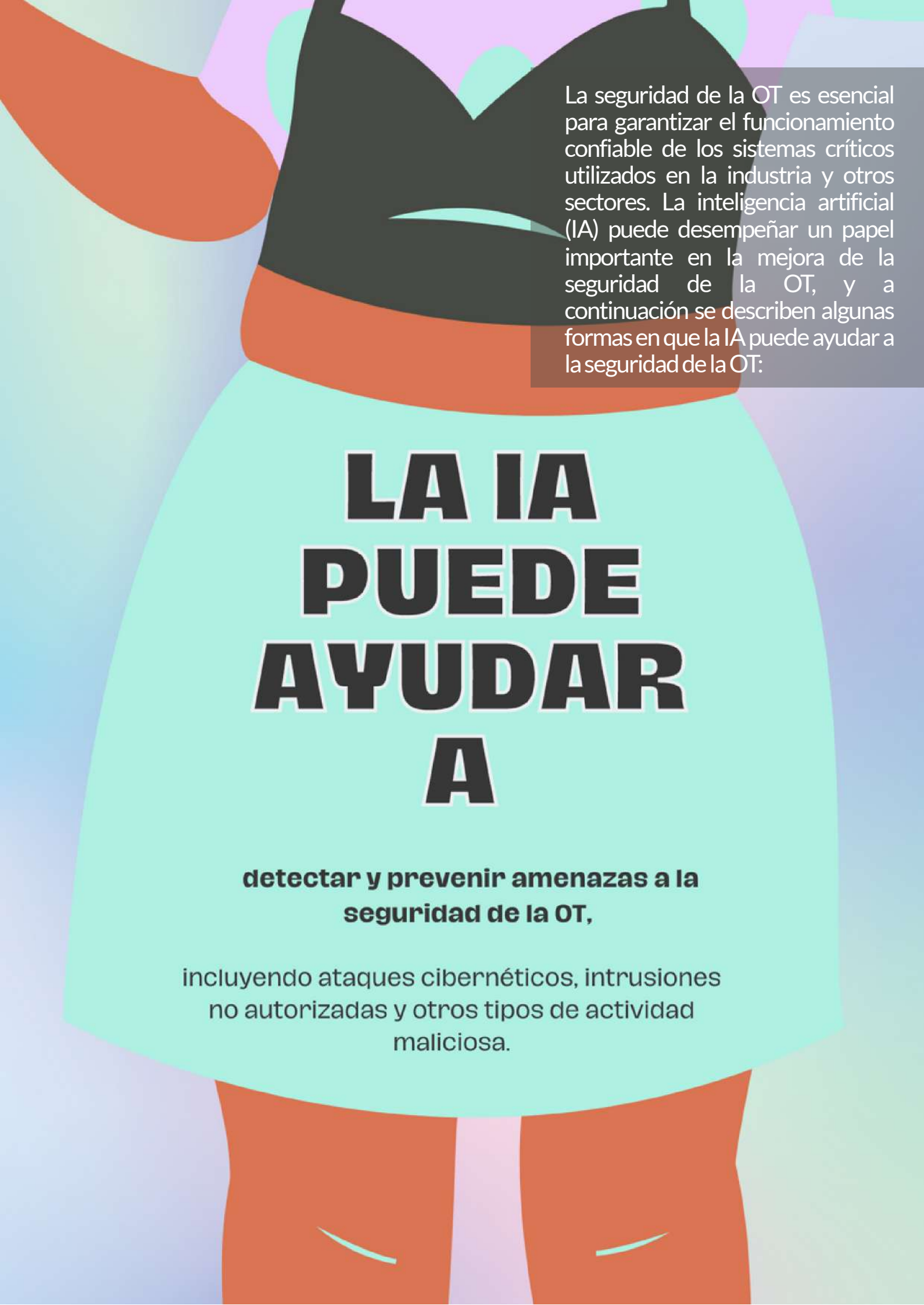
Integración con sistemas existentes. Muchos sistemas de OT utilizan tecnologías y protocolos antiguos que pueden no ser compatibles con las soluciones de IA modernas. La integración de la IA con estos sistemas puede requerir la creación de interfaces y adaptadores personalizados para asegurar que la información fluya de manera efectiva entre los sistemas. Además, la implementación de la IA puede requerir actualizaciones de hardware y software en los sistemas existentes, lo que puede ser costoso y requerir un tiempo considerable.

Acceso a datos. La IA requiere grandes cantidades de datos para entrenar los modelos y tomar decisiones efectivas. En la OT, los datos suelen estar dispersos en diferentes sistemas y dispositivos, lo que dificulta la recopilación y el acceso a los datos necesarios para la implementación de la IA. Además, los datos en la OT pueden ser de baja calidad o incompletos, lo que puede afectar la precisión de los modelos de IA. Es necesario establecer mecanismos para recopilar, almacenar y acceder a los datos necesarios para la implementación de la IA.

Seguridad y privacidad. La implementación de la IA en la OT puede plantear problemas de seguridad y privacidad. La OT involucra sistemas críticos que pueden ser vulnerables a ataques cibernéticos, y la implementación de la IA puede crear nuevas vulnerabilidades. Además, la recopilación y el análisis de datos pueden plantear problemas de privacidad para los empleados y los clientes. Es necesario establecer medidas de seguridad y privacidad adecuadas para proteger los sistemas y los datos involucrados en la implementación de la IA.

Capacitación y habilidades. La implementación de la IA en la OT requiere habilidades técnicas y conocimientos especializados en IA y OT. Muchas empresas pueden carecer de personal capacitado para implementar y mantener soluciones de IA en la OT. Además, la capacitación en IA requiere una inversión significativa en tiempo y recursos, lo que puede ser un obstáculo para algunas empresas.

Comunicación y colaboración. La implementación de la IA en la OT requiere una colaboración efectiva entre los equipos de OT y los equipos de IA. Es importante establecer una comunicación clara y una colaboración efectiva entre los diferentes equipos para garantizar una implementación exitosa de la IA en la OT. Además, es importante tener en cuenta las preocupaciones y los requisitos de los diferentes grupos de interés, como los empleados, los clientes y los reguladores.



La seguridad de la OT es esencial para garantizar el funcionamiento confiable de los sistemas críticos utilizados en la industria y otros sectores. La inteligencia artificial (IA) puede desempeñar un papel importante en la mejora de la seguridad de la OT, y a continuación se describen algunas formas en que la IA puede ayudar a la seguridad de la OT:

# LA IA PUEDE AYUDAR A

**detectar y prevenir amenazas a la seguridad de la OT,**

incluyendo ataques cibernéticos, intrusiones no autorizadas y otros tipos de actividad maliciosa.

La IA puede ayudar a detectar y prevenir amenazas a la seguridad de la OT, incluyendo ataques cibernéticos, intrusiones no autorizadas y otros tipos de actividad maliciosa. La IA puede analizar grandes cantidades de datos de diferentes fuentes para identificar patrones y anomalías que puedan indicar la presencia de amenazas. Además, la IA puede aprender de experiencias anteriores y mejorar su capacidad para detectar y prevenir amenazas a medida que se recopila más información.

La IA puede analizar datos en tiempo real para detectar y prevenir amenazas a la seguridad de la OT. Esto incluye la monitorización de datos de sensores y otros dispositivos conectados a la red para detectar anomalías o patrones de comportamiento inusual que puedan indicar la presencia de una amenaza. La IA también puede analizar el tráfico de red y los registros de eventos para identificar patrones de actividad sospechosos.

La IA puede ayudar a automatizar los procesos de seguridad en la OT, incluyendo la identificación de amenazas, la autenticación de usuarios y la gestión de incidentes de seguridad. La IA puede aprender a tomar decisiones basadas en reglas y algoritmos predefinidos para tomar medidas de seguridad en tiempo real y reducir el tiempo de respuesta a las amenazas de seguridad.

La IA puede ayudar a mejorar la visibilidad de la red en la OT, lo que permite a los equipos de seguridad monitorear mejor los sistemas y dispositivos conectados a la red. La IA puede analizar los registros de eventos y el tráfico de red para identificar dispositivos no autorizados y detectar actividades sospechosas.

La IA puede analizar los registros de eventos, el tráfico de red y otros datos para identificar posibles vulnerabilidades y riesgos en los sistemas de OT. Esto permite a los equipos de seguridad tomar medidas preventivas para reducir los riesgos de seguridad.

Ciberseguridad 360

# BlueAura

## ¿Qué es?

BinauraMonlex ha elaborado un producto muy especializado y enfocado a **tratar el ciberriesgo** desde varios ángulos:

- **Asistencia legal en ciberseguridad**
- **Monitorización proactiva**
- **Protección ante ciberataques con antimalware avanzado**
- **Concienciación de los usuarios en ciberseguridad**
- **Informes mensuales de estado de la ciberseguridad**
- **Protección de la identidad y las vulnerabilidades**

El objetivo final del servicio es **implantar un modelo preventivo ante los ciberataques** que permita también ser más eficaz al reaccionar ante uno de ellos.

binauramonlex

BlueAura Ciberseguridad 360

binauramonlex

## ¿Por qué?

- Adaptado completamente a cada empresa.
- Establecemos un modelo preventivo, que ayuda a ser más rápidos y eficientes.
- Tenemos las principales titulaciones en ciberseguridad a nivel mundial.
- Añadimos la asistencia de abogados expertos en nuevas tecnologías.

Datos de interés:

- El artículo 32 del RGPD dice que se aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
- La Responsabilidad Proactiva incluida en el artículo 5.2 del RGPD establece que aquellas organizaciones que traten datos personales deberán cumplir con las exigencias de la normativa sobre protección de datos y, además, deberán demostrarlo.
- Durante el 2021, la AEPD ha sancionado con 874.200 € por falta de medidas técnicas y organizativas.
- Las sanciones oscilan desde los 3000 € hasta los 600.000 €.
- La necesidad de ciberseguridad para el cumplimiento del RGPD.

Avalados por: CISA CISM CDPSE CISSP

## ¿Cómo?

Eligiendo el plan perfecto que se adapte a tu empresa.

### Básico

Diseñado para tener unos estándares mínimos de calidad y seguridad de la información.

- Monitorización proactiva 8x5
- Antimalware de Bitdefender
- Informes mensuales de estado de la ciberseguridad
- Manual básico de seguridad para empleados
- Concienciación sobre ciberseguridad automática*
- Plan de recuperación de datos

Paquete Subvencionable 100%: KIT DIGITAL

### Óptimo

Perfecto para las pequeñas y medianas empresas que quieren mejorar su ciberseguridad.

- Antimalware Bitdefender con características Avanzadas ATS (Advanced Threat Security)
- Asistencia informática remota en caso de incidencia**
- Monitorización proactiva 12x5
- Protección del correo electrónico mediante Email Gateway Security de Bitdefender*
- Manual básico de seguridad para empleados
- Informes mensuales de estado de la ciberseguridad
- Asistencia legal de ciberseguridad
- Concienciación sobre ciberseguridad automática*
- Plan de recuperación de datos

### Extra

El paquete Extra incluye la cobertura total cuestanda redar sus empresas cubiertas.

- Antimalware Bitdefender con características Avanzadas ATS (Advanced Threat Security) + XEDR
- Asistencia informática in situ en caso de incidencia**
- Monitorización proactiva 12x6
- Protección del correo electrónico mediante Email Gateway Security de Bitdefender*
- Manual básico de seguridad para empleados
- Informes mensuales de estado de la ciberseguridad
- Asistencia legal de ciberseguridad
- Concienciación sobre ciberseguridad automática*
- Plan de recuperación de datos
- Implantación 2FA mediante Yubikey***
- Gestión de parches, parches virtual y vulnerabilidades
- Análisis de las vulnerabilidades de red semestrales

* La implementación tiene un coste de 100€ en entornos Office365 y Gmail. En otros entornos se valorará tras estudiarlo. P/P sin IVA por endpoint al mes con compromiso de un año.
** Hasta un máximo de 3h no acumulables. En el caso de asistencia presencial del paquete Extra el total serán 5h no acumulables.
*** El hardware se facturará aparte. El coste de la implementación tiene un pago único de 4€ por estación de trabajo / usuario. El paquete incluye el mantenimiento y resolución de problemas.

KIT DIGITAL

### Subvenciona tu proyecto con el KIT Digital

Somos Agente Digitalizador. Podemos gestionar la subvención para su empresa mediante la convocatoria KIT Digital.

Contáctanos en:

+34 971 22 73 99

info@binauramonlex.com

# Cuidamos de tu tranquilidad

"Ingeniero en Telecomunicaciones, y profesional con más de 15 años en el ámbito de la ciberseguridad. A lo largo de mi carrera he pasado por diferentes empresas lideres en la integración de servicios informáticos, aportando soluciones tecnológicas, y protegiendo redes y sistemas de empresas de diferentes sectores y ubicaciones geográficas. Actualmente llevo varios años en la empresa española Gestamp, liderando el área de Ciberseguridad. Soy una persona muy apasionada por las nuevas tecnologías, los retos y la gestión de riesgos, base importante para poder construir programas de ciberseguridad robustos y eficientes que acompañen la estrategia de los negocios"

JOSÉ MIGUEL PAREJO

# LA INDUSTRIA CONECTADA Y LOS NUEVOS RETOS EN CIBERSEGURIDAD.

ESTE NUEVO MODELO INDUSTRIAL TRAE NUEVOS RETOS EN EL PROGRAMA DE CIBERSEGURIDAD EN LAS EMPRESAS


# LA INDUSTRIA 4.0,

*también llamada "cuarta revolución industrial"*

Se basa en la conexión de diferentes dispositivos físicos, sensores De IoT con el mundo digital que, por medio de diferentes habilitadores tecnológicos, permiten la recolección masiva de datos para crear entornos industriales mucho más eficientes y optimizados, teniendo así un control total de la cadena de producción, Y permitiendo poder tomar decisiones en tiempo real, y, por consiguiente, crear un nuevo modelo de empresa industrial.

La complejidad en las nuevas cadenas de suministro de la industria y las interdependencias entre empresas, también han impulsado los proyectos de I4.0, con la consecuencia de que la digitalización de las cadenas de suministro, hoy en día, es parte de la estrategia de negocio de la mayoría de las empresas industriales.

Este nuevo modelo industrial trae nuevos Retos en el programa de Ciberseguridad en las empresas, y la necesidad de adaptar los planes estratégicos dentro de las compañías. Aunque los retos en ciberseguridad industrial son bien conocidos por lo CISOs y por los profesionales del sector, el informe que recoge el SANS ICS OT de Octubre del 2022 aporta datos muy interesantes sobre este punto, entre los que merece la pena resaltar los cuatro siguientes:

- La integración y la conexión de equipos Legacy dentro de las arquitecturas ICS con el mundo digital.
- Tecnologías tradicionales de Ciberseguridad en el mundo IT que no están diseñadas para los entornos OT, causando muchas fricciones en su implementación.
- Equipos de IT en infraestructuras y de Ciberseguridad que no entienden de las necesidades y prioridades dentro del entorno OT.
- Insuficiente fuerza laboral para implementar y mantener los controles necesarios con el fin de proteger los entornos industriales.

A estos cuatro, me gustaría agregar la cultura en ciberseguridad OT. Está más que demostrado que el factor personas es el principal vector de ataque y el eslabón más débil dentro de las empresas, bien sea por la pericia de un atacante en explotar técnicas en el correo electrónico, por ingeniería social, o bien por simple desconocimiento de los empleados que operan activos o procesos críticos en una empresa. En este sentido, el slogan tradicional que se suele escuchar en estos casos es el de "si funciona bien mejor no lo toques", lo que es contraproducente si se quiere impulsar la I4.0 implementando nuevas medidas de ciberseguridad dentro de los procesos, entornos y aplicaciones.

En este contexto de retos y desafíos, es inevitable preguntarnos, ¿por dónde empezamos? Muchos expertos coinciden en que la mejor manera de empezar a construir un programa de ciberseguridad industrial es por medio de un análisis BIA, un análisis de impacto que identifique cuáles son los procesos y activos industriales más importantes dentro de entornos de producción. Construir una estrategia de Ciberseguridad priorizando las "joyas de la corona" ayuda a enfocarse en lo más importante, conseguir más con menos, y lograr la eficiencia y optimización en los gastos, que toda organización exige para poder ser viable.

Volviendo al primer reto recogido por el informe de SANS ICS OT, el hecho de trabajar con equipos Legacy supone un cambio de paradigma importante, mientras que en los entornos de IT una de las medidas fundamentales es la de tener un buen ciclo de parches y gestión de vulnerabilidades, en OT, el control de la superficie de exposición, el control de accesos y tecnologías de parcheo virtual de un activo, juegan un papel muy importante, de allí el estándar IEC 62443 al que se hará referencia más adelante.

Gestionar vulnerabilidades en activos Legacy supone, sin duda, un reto, por una parte, porque simplemente no existen parches disponibles para la versión del OS, y por otra, porque supone intentar encajar el parcheado dentro de las ventanas de mantenimiento que suelen tener los entornos de producción, donde nos podemos encontrar con paradas mensuales, semestrales, o incluso anuales.

Para conocer el mapa de vulnerabilidades que acecha al entorno OT, basta con mirar los reportes de Nozomi o Clarory del año 2022, herramientas líderes en el mercado de control de activos OT. Cerca del 90% de las vulnerabilidades detectadas son de complejidad baja, lo que hace que no hagan falta capacidades muy avanzadas para por poder realizar un ataque. Así mismo, estos informes también recogen que la mayor parte de dichas vulnerabilidades son de riesgo alto o crítico, lo que podría suponer un daño importante a la empresa.
Para poder crear zonas de seguridad y controlar la superficie de exposición de los diferentes activos industriales, no hay más que seguir la arquitectura estándar que nos muestra la IEC 62443, lo que permite conectar con el mundo IT con el OT de una manera segura. Una de las ilustraciones que, a mi parecer, mejor refleja el impacto de estas capas, es la de la Agencia de Ciber Defensa Norteamericana, "CISA", que ilustra el nivel de esfuerzo que debe realizar un atacante para llegar a las "joyas de la corona", donde el amarillo refleja un bajo esfuerzo y el rojo un alto esfuerzo:

# “JOYAS DE LA CORONA”, DONDE EL AMARILLO REFLEJA UN BAJO ESFUERZO Y EL ROJO UN ALTO ESFUERZO

FIGURE 1: UNSEGMENTED IT AND OT NETWORK

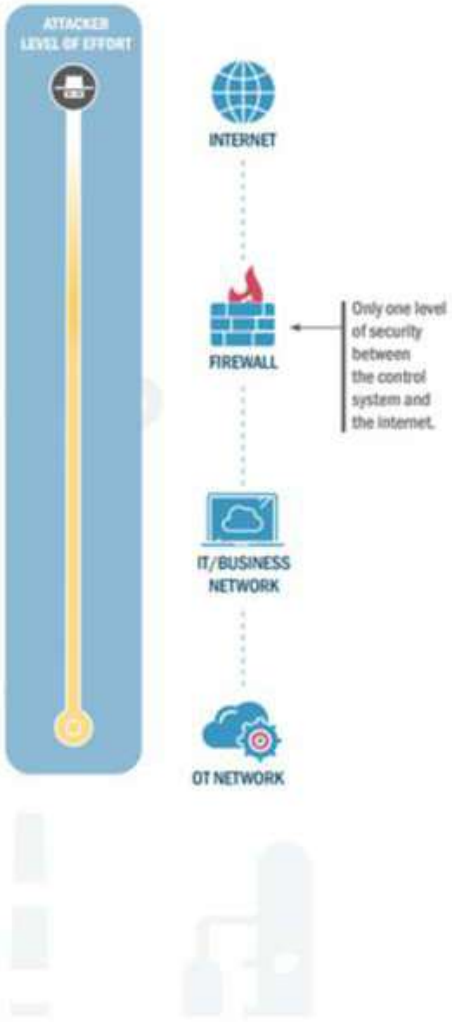
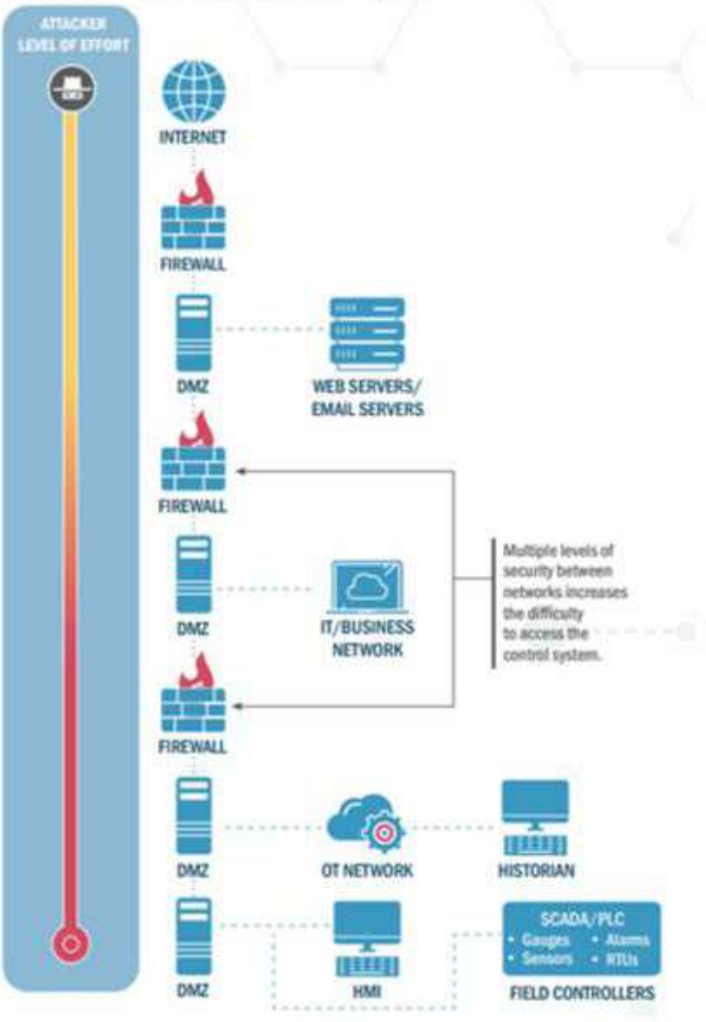
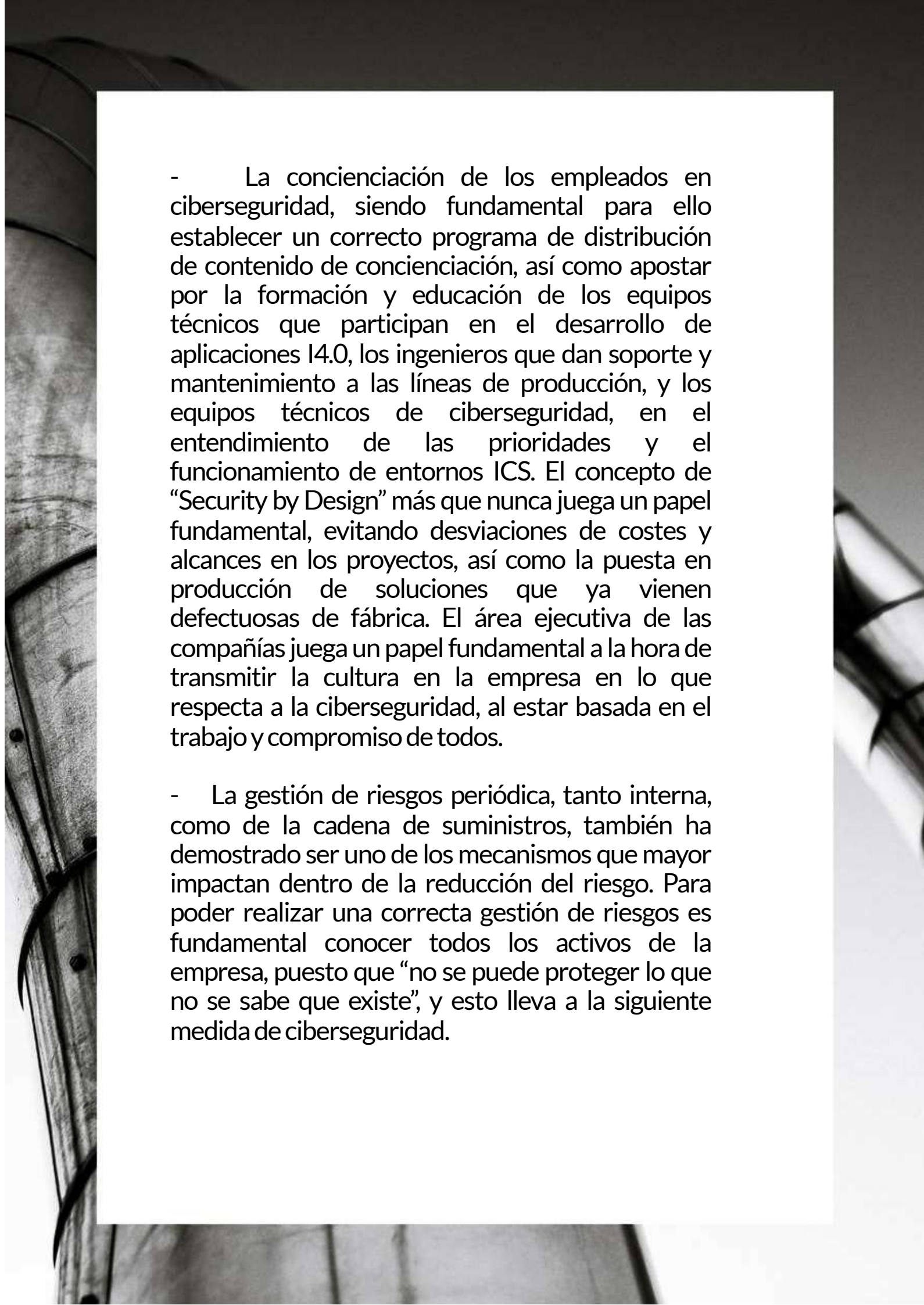



FIGURE 2: A SEGMENTED PURDUE ENTERPRISE REFERENCE ARCHITECTURE (PERA) NETWORK ARCHITECTURE




La IEC 62443 a su vez nos muestra toda la hoja de ruta y el marco de controles necesarios para proteger los entornos industriales. Dentro del marco de controles y mejores prácticas en ciberseguridad en los entornos industriales, los que mayor impacto en la reducción del riesgo ejercen, son los siguientes:



- La concienciación de los empleados en ciberseguridad, siendo fundamental para ello establecer un correcto programa de distribución de contenido de concienciación, así como apostar por la formación y educación de los equipos técnicos que participan en el desarrollo de aplicaciones I4.0, los ingenieros que dan soporte y mantenimiento a las líneas de producción, y los equipos técnicos de ciberseguridad, en el entendimiento de las prioridades y el funcionamiento de entornos ICS. El concepto de "Security by Design" más que nunca juega un papel fundamental, evitando desviaciones de costes y alcances en los proyectos, así como la puesta en producción de soluciones que ya vienen defectuosas de fábrica. El área ejecutiva de las compañías juega un papel fundamental a la hora de transmitir la cultura en la empresa en lo que respecta a la ciberseguridad, al estar basada en el trabajo y compromiso de todos.

- La gestión de riesgos periódica, tanto interna, como de la cadena de suministros, también ha demostrado ser uno de los mecanismos que mayor impactan dentro de la reducción del riesgo. Para poder realizar una correcta gestión de riesgos es fundamental conocer todos los activos de la empresa, puesto que "no se puede proteger lo que no se sabe que existe", y esto lleva a la siguiente medida de ciberseguridad.

- Control de activos: poder identificar y controlar todos los activos dentro de las redes industriales es fundamental, así como ejercer controles más exigentes sobre esos activos más críticos. Existen herramientas tecnologías muy interesantes para descubrir los activos conectados, conocer las vulnerabilidades y mostrar el comportamiento de los protocolos. Nuevas soluciones, ya basadas en Inteligencia Artificial y Machine Learning, ayudan en gran medida a construir un mapa de conexiones y predecir comportamientos que pueden desencadenar en un ataque. Sin embargo, hay medidas muy básicas, sin coste, que nunca se deben de olvidar y tienen un fuerte impacto en el riesgo, como cambiar siempre las credenciales por defecto.

- Por último, los procesos de respuesta a incidencia son un factor clave dentro de las capacidades de resiliencia de una empresa. Tener a los equipos técnicos y ejecutivos formados en estos procesos, puede ser la diferencia entre una ataque contenido y mitigado en fases tempranas, a tener ciberataques de alto impacto en el negocio, afectando de forma profunda la reputación, la marca y la confianza en la empresa.

# SOBRE LA BASE DEL BREVE ANALISIS ANTERIOR,

podemos destacar que hoy en día, gracias a los diferentes estándares que marcan buenas prácticas en el sector, la alianza con colaboradores estratégicos, y el auge en la consolidación de plataformas tecnológicas de ciberseguridad, son todos recursos que ayudan a crear entornos industriales sostenibles, protegidos y más resilientes. Tener en cuenta todos estos aspectos para elaborar una buena estrategia de ciberseguridad, medible y en constante revisión, es la clave para el éxito de cualquier negocio.

INDUSTRIA Y CIBERSEGURIDAD

# LLEVE A CABO SU ACTIVIDAD CON CIBERTRANQUILIDAD

Con la digitalización y la automatización de los procesos, las empresas industriales se enfrentan a mayores riesgos de ciberseguridad: **espionaje, sabotaje, corrupción de datos e incluso la paralización total de la producción.**

Para la protección de redes, datos, puestos de trabajo y servidores: al elegir las soluciones Stormshield, recurre a un actor de la ciberseguridad en el que puede confiar.

STORMSHIELD

www.stormshield.com

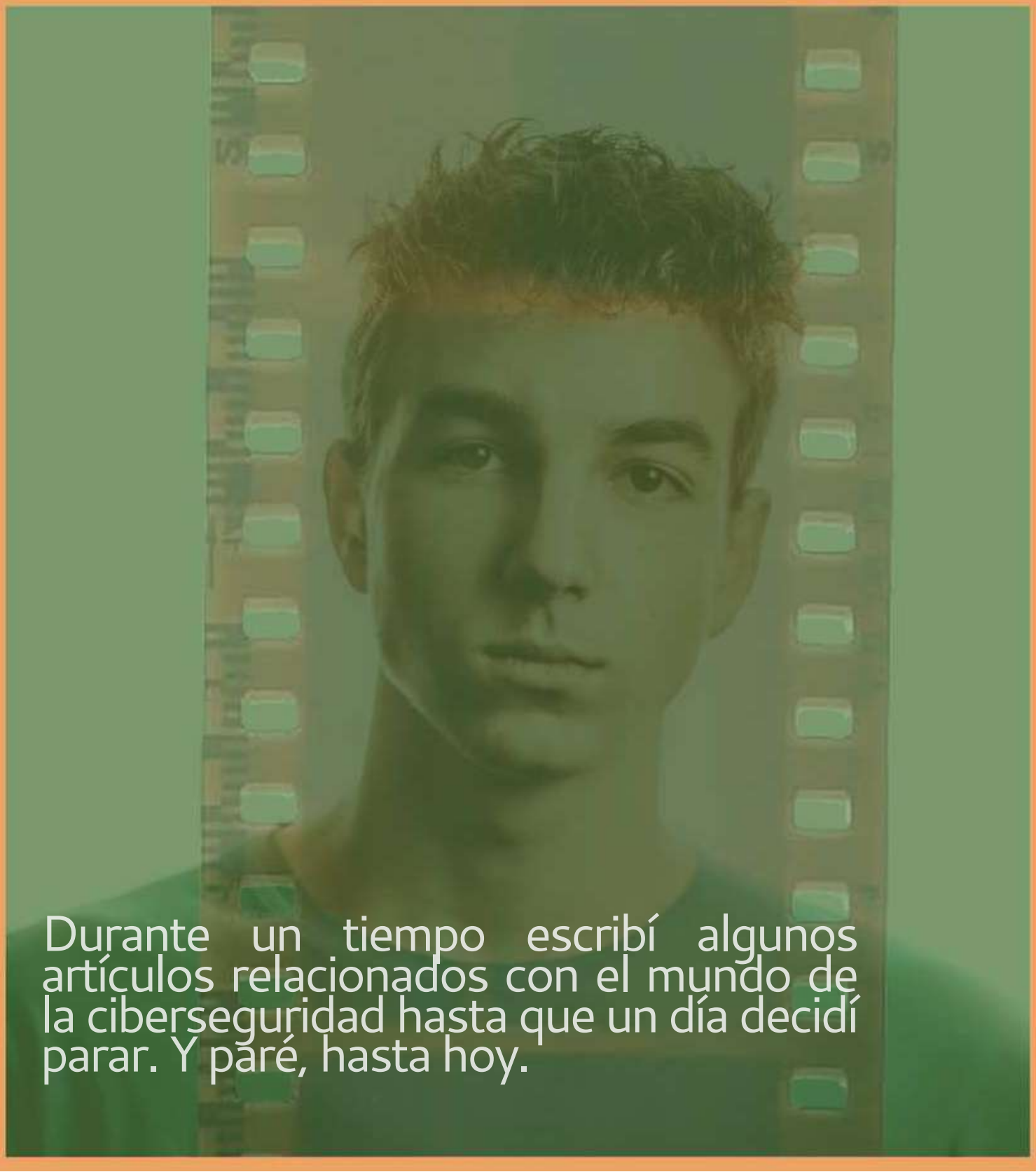

Para
Todos

Cofundador en Zerod | CISO y Security Audit Hub Director en Schwarz Group | Director Bootcamp Ciberseguridad en Nuclio Digital School | Inversor y Advisor independiente

# En la ciberseguridad...

## ¿UNO SE HACE O SE NACE?

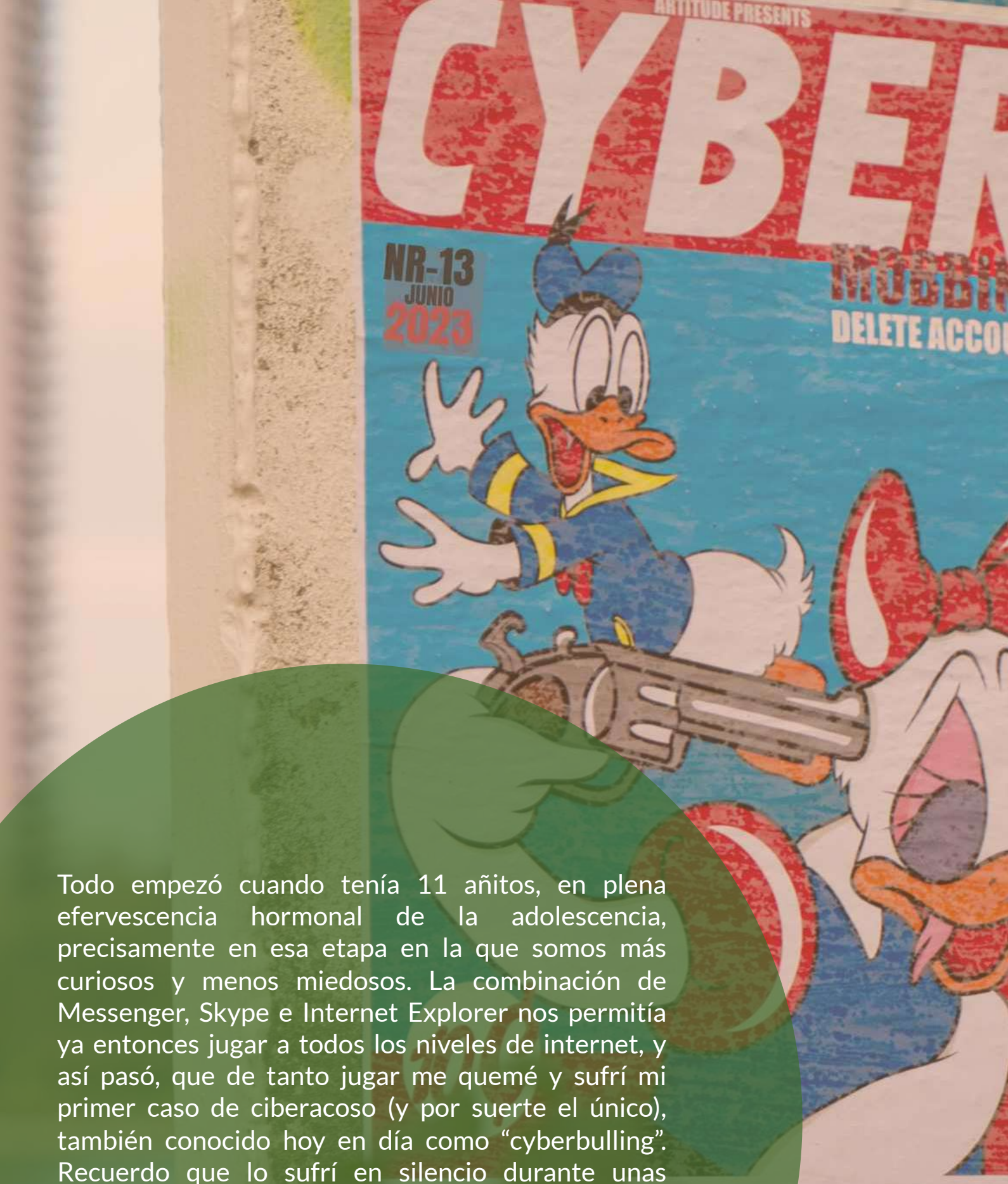
Xavi Bertomeu



Durante un tiempo escribí algunos artículos relacionados con el mundo de la ciberseguridad hasta que un día decidí parar. Y paré, hasta hoy.

Mi realidad o mi frustración siempre ha tenido que ver con el tipo de contenido que me he ido encontrando en muchos medios de comunicación (digitales o no). Suele ser repetitivo, complicado de digerir e ir acompañado de una falta de opinión crítica importante (ojo, siempre bajo mi humilde y subjetiva opinión). Es como si ya desde hace años nuestro gran amigo ChatGPT estuviera produciendo en masa un sinfín de cantidad de artículos de opinión del sector ciber.

Y es por este motivo, amigos lectores, que hoy vuelvo a escribir. Vuelvo porque tengo ganas de hablaros de los últimos 10 años de la ciberseguridad, de algunas historias que la rodean y sobre todo de hacerlo a través de mi trayectoria y visión 100% personal. Mi única intención no es más que tratar de generar alguna reflexión en vuestra mente y acercaros a la ciberseguridad sea cual sea vuestro conocimiento técnico (o habilidad de pedir ayuda a nuestro gran amigo chatGPT).




Todo empezó cuando tenía 11 añitos, en plena efervescencia hormonal de la adolescencia, precisamente en esa etapa en la que somos más curiosos y menos miedosos. La combinación de Messenger, Skype e Internet Explorer nos permitía ya entonces jugar a todos los niveles de internet, y así pasó, que de tanto jugar me quemé y sufrí mi primer caso de ciberacoso (y por suerte el único), también conocido hoy en día como “cyberbulling”. Recuerdo que lo sufrí en silencio durante unas cuantas semanas, esperando esa extorsión que nunca llegó y que se quedó finalmente como una amenaza y un pequeño trauma infantil (aunque también desencadenó mi “Leitmotiv” profesional, no hay mal que por bien no venga).

Y de esta primera anécdota, mi primer consejo: hay que hablar de ciberseguridad a los niños ya en edad muy temprana, tanto, por parte de los padres como de los docentes, explicando muy bien los riesgos cibernéticos, ciertos aspectos de la privacidad en internet y sobre todo las consecuencias de ciertos actos en el mundo digital. Hace unos años di una charla de ciberacoso a unos cuantos alumnos de segundo de la ESO y lo más curioso fue que nada más entrar en el aula el tutor me dijo: “Te ha tocado la mejor clase, tenemos 3 casos de ciberacoso”. El resto de la historia seguramente ya os la podéis imaginar… ¡Pues ese es el nivel, Maribel!

Unos años más tarde, tras licenciarme en ingeniería de telecomunicaciones y otras formaciones paralelas, conseguí meterme en el mundo laboral. Fue entonces cuando me topé de nuevo con la ciberseguridad, aunque yo en ese momento no la conocía como tal. Como ingeniero de redes y sistemas me dedicaba a gestionar "dispositivos perimetrales de seguridad", o más conocidos hoy en día como cortafuegos o "firewalls". Ese primer pasito, aunque yo no lo viera entonces, fue el empujón que me adentró en el mundo de la seguridad informática, que me iba dando poco a poco experiencia técnica y visión de negocio y al mismo tiempo me permitía conocer a gente muy interesante del sector. Y de ahí viene mi segunda píldora de hoy: la ciberseguridad es tecnología pero también es negocio, de hecho lo es todo. Siempre digo a mis alumnos que el CISO o como lo conocemos aquí, el Director de Ciberseguridad de una empresa, es el que sabe más después del CEO o Director General (o debería). No se puede entender la ciberseguridad sin saber porqué la aplicas (el negocio) ni el cómo la aplicas (la tecnología).

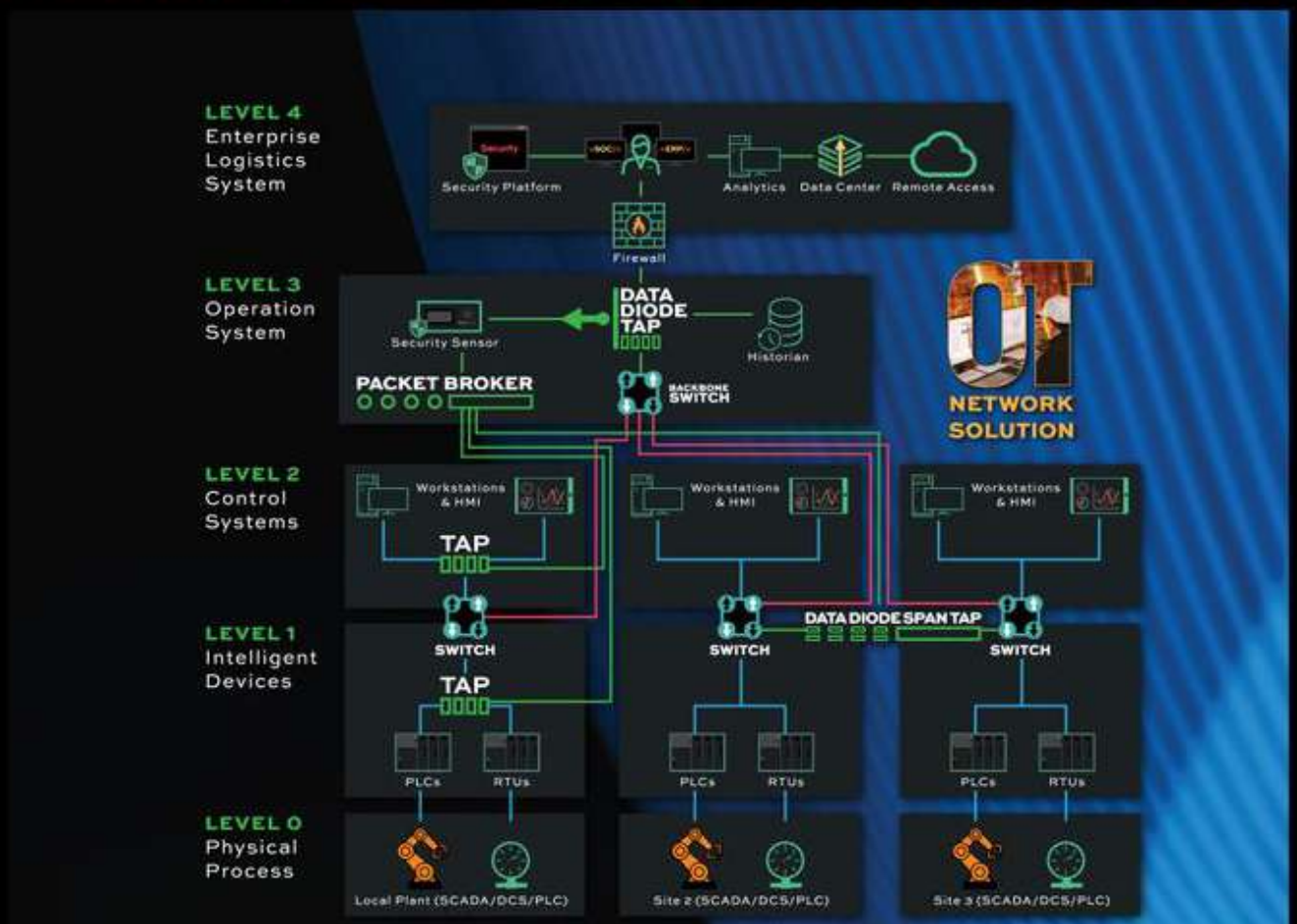

En paralelo a mi carrera de CISO y docente, decidí emprender algunos proyectos propios para saciar mi propia curiosidad e hiperactividad que tanto me caracteriza. Todas estas aventuras, además de enseñarme a ser resiliente y ver más mundo, me han demostrado algo que no hay duda de su veracidad al 100% y es que en todas las áreas de una empresa se necesita implementar ciberseguridad. En IT un antivirus, en HR un proceso de guardado seguro de las nóminas, en Legal una cláusula de confidencialidad en un contrato, en Finanzas un proceso de pago seguro, etc. Un ciberataque afecta a cualquier área de una empresa, sea cual sea, con lo cual la ciberseguridad debe estar “everywhere”.

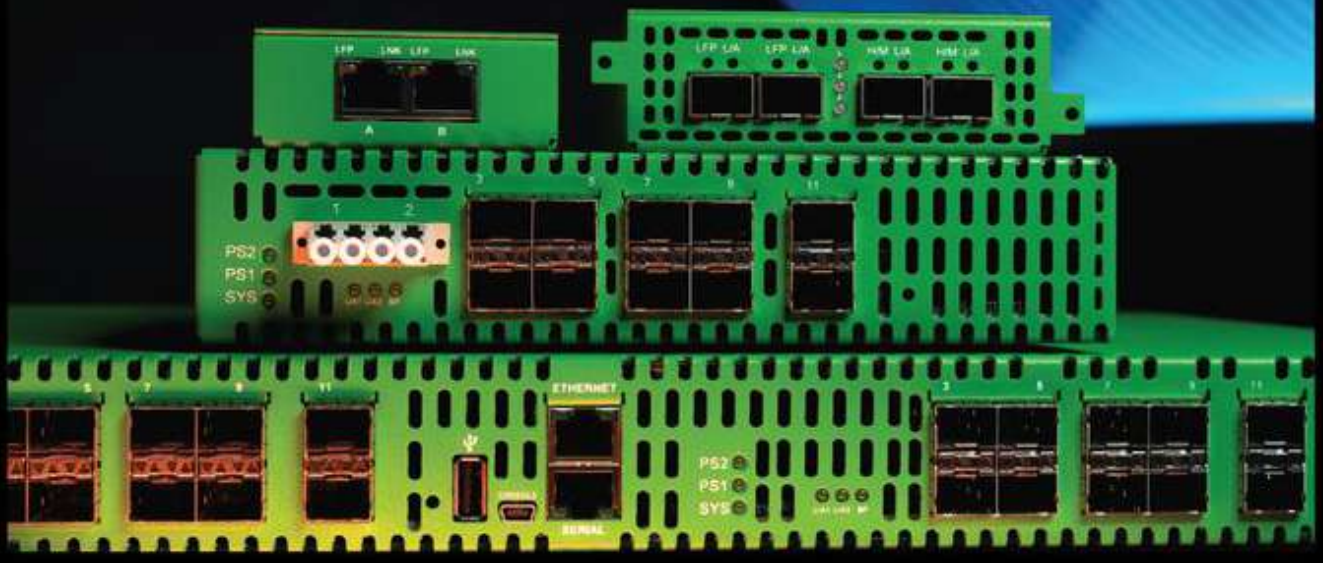

Y partiendo de esta última frase aplastante, aquí va mi última cyber reflexión del día: el mercado de la ciberseguridad está experimentando un crecimiento exponencial a nivel mundial, se están creando nuevos modelos de negocio (IA, SaaS, Marketplace) cada vez más accesibles para cualquier tipo de empresa, además el sector te permite convertirte en un profesional senior con solo 2 años de experiencia por el desequilibrio que existe entre la oferta/demanda laboral y para más inri, en este mundillo vas a poder explorar y entender distintos negocios y muchos tipos de tecnologías mejor que nadie más del planeta. ¿De verdad no te parece apasionante la ciberseguridad?

GARLAND TECHNOLOGY
See every bit, byte, and packet®

# Securización de redes OT

## Data Diodes, Network TAPs, Bypass TAPs, Packet Brokers




OT NETWORK SOLUTION

## Busca tu solución de redes OT en:

garlandtechnology.com/ot-ics-visibility-solutions-for-industrial

+1 716.242.8500 | sales@garlandtechnology.com

“Chileno que vive en la tierra de Gardel. Informático con más de 15 años de experiencia laboral en Plataforma Microsoft y 5 años en Ciberseguridad y Seguridad de la Información. Certificado CEH v11 y Auditor Interno ISO 27001. Me gusta aprender y también enseñar, porque el conocimiento es la mejor arma en la vida.
Actualmente soy analista de ciberseguridad en Wezen Group donde mi pasión por la ciberseguridad permite ayudar a nuestros clientes, aportando mis conocimientos a minimizar al máximo posible las brechas de seguridad.”

PABLO
Alarcón

# LAS REDES OT

Las redes OT (Tecnología de las Operaciones), es una disciplina que se centra en el uso de la tecnología para mejorar la eficiencia, productividad y calidad de las operaciones en una organización. A medida que las organizaciones buscan optimizar sus procesos y adaptarse a un entorno empresarial cada vez más digital, las redes OT se han convertido en un componente clave para lograr el éxito.

La implementación efectiva de las redes OT puede generar una serie de beneficios para una organización, entre los que se destacan:

*__Automatización de procesos__

*__Mejora de la visibilidad y el control__

*__Optimización de la cadena de suministro__

*__Mejora de la calidad__

*__Reducción de costos__

Existen diversas tecnologías que desempeñan un papel fundamental en la mejora de las operaciones. Algunas de las más relevantes son:

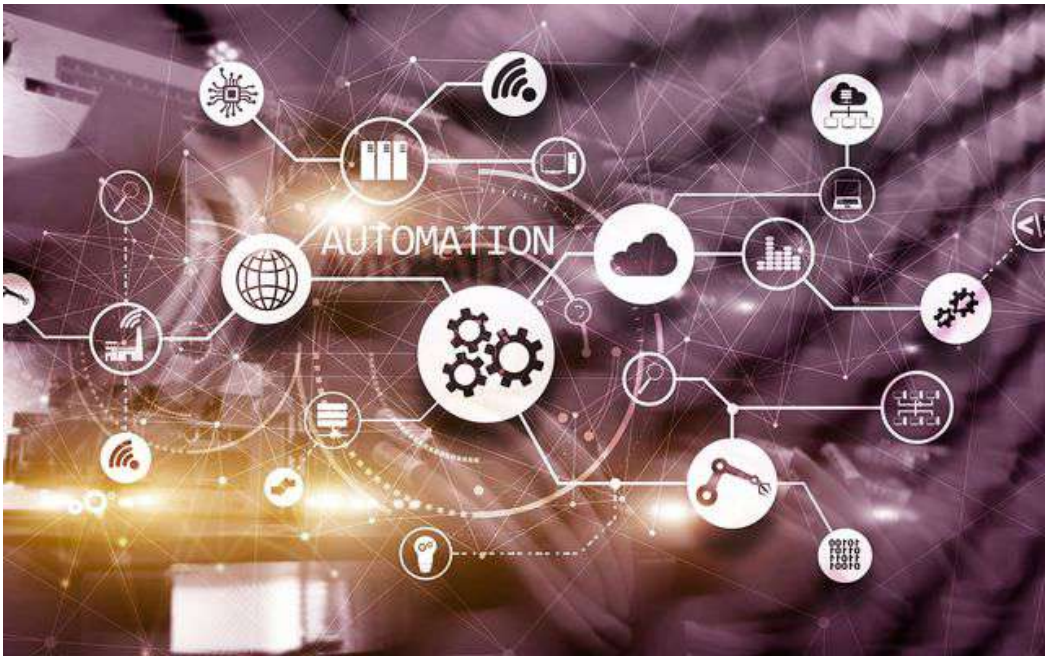
*Internet de las cosas (IoT): Permite la conexión de dispositivos y sensores para recopilar datos en tiempo real, lo que facilita la monitorización y el control de los procesos.

*Automatización robótica de procesos (RPA): Consiste en el uso de software para automatizar tareas y procesos basados en reglas, liberando a los empleados de tareas repetitivas y permitiéndoles centrarse en actividades de mayor valor.

*Analítica de datos: La capacidad de recopilar, analizar y extraer información significativa de grandes volúmenes de datos, puede proporcionar conocimientos valiosos para la toma de decisiones y la mejora de las operaciones.

*Computación en la nube: Permite el acceso a recursos informáticos flexibles y escalables, lo que facilita el almacenamiento de datos, el procesamiento y el despliegue de aplicaciones sin tener que invertir en infraestructura física costosa.

*Inteligencia artificial (IA): La IA puede utilizarse para optimizar y automatizar procesos, así como para tomar decisiones basadas en análisis de datos complejos.




Si bien las redes OT ofrecen una serie de beneficios, también presentan desafíos y consideraciones que deben abordarse adecuadamente:

*Cambio organizacional: Adoptar nuevas tecnologías implica cambios en los procesos y la cultura de la organización.

*Integración de sistemas: La interoperabilidad entre diferentes sistemas y tecnologías puede ser un desafío, por lo que es necesario garantizar una integración fluida y eficiente.

*Privacidad de datos: El uso de tecnologías como IoT y analítica de datos implica la recopilación y el procesamiento de grandes cantidades de información, lo que requiere una atención adecuada a la privacidad y a la protección de datos.

*Seguridad: La implementación de tecnología en las operaciones puede implicar riesgos de seguridad cibernética, por lo que es esencial contar con medidas adecuadas de protección y mitigación de riesgos.

El ransomware es una de las principales amenazas en el campo de la ciberseguridad y puede tener impactos significativos en las organizaciones. Algunos de los riesgos asociados al ransomware son:

**1.** Pérdida de datos: El ransomware cifra los archivos del sistema infectado. Esto puede resultar en una pérdida total o parcial de datos importantes.

**2.** Interrupción de operaciones: Los sistemas críticos pueden quedar inutilizables, lo que resulta en una disminución de la productividad y la pérdida de ingresos.

**3.** Daño a la reputación: Los clientes pueden perder la confianza en la capacidad de la organización para proteger sus datos, lo que puede afectar negativamente las relaciones comerciales y la imagen de la marca.

**4.** Costos financieros: El pago del rescate exigido por los atacantes es una opción que algunas organizaciones consideran para recuperar sus archivos y sistemas. Sin embargo, esto implica un costo financiero significativo y, además, no existe garantía de que los archivos sean recuperados o de que los atacantes no vuelvan a atacar en el futuro.

**5.** Propagación a otros sistemas: El ransomware puede propagarse rápidamente a través de redes

Algunos de los riesgos específicos que enfrentan las redes OT frente al ransomware son:

**1.** Paralización de infraestructuras críticas: Un ataque de ransomware exitoso puede paralizar estos sistemas críticos y tener consecuencias graves para la sociedad, la economía y la seguridad pública.

**2.** Peligro para la seguridad física: un ataque exitoso podría causar problemas en el control de procesos, lo que podría resultar en accidentes, fugas peligrosas o incluso daños a los trabajadores.

**3.** Tiempo de inactividad prolongado: puede tener un impacto financiero significativo y causar interrupciones en la cadena de suministro y en la prestación de servicios.

**4.** Vulnerabilidades en sistemas heredados: Muchas redes OT aún utilizan sistemas heredados y obsoletos que pueden ser más susceptibles a ataques de ransomware debido a la falta de actualizaciones de seguridad y la presencia de vulnerabilidades conocidas.

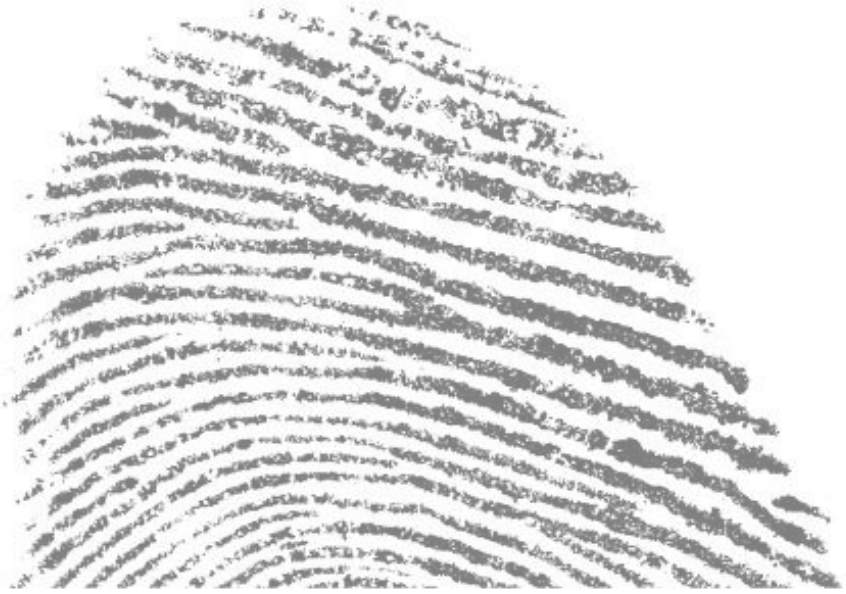
**5.** Pérdida de datos y propiedad intelectual: existe el riesgo de que información confidencial o propiedad intelectual sea encriptada, robada o expuesta, lo que puede tener graves implicaciones para la competitividad y la seguridad de una organización.

Para mitigar estos riesgos, es fundamental implementar medidas sólidas de ciberseguridad en las redes OT, como la segmentación de redes, el monitoreo constante, las copias de seguridad regulares y la educación y concienciación del personal sobre las mejores prácticas de seguridad. También es importante mantener los sistemas actualizados y parcheados, así como contar con planes de respuesta a incidentes bien definidos para una acción rápida y efectiva en caso de un ataque de ransomware.

Contacto
609750186

# APHERTON

Grupo de Investigación



SOMOS UNA EXCLUSIVA FIRMA DE INVESTIGACIÓN CON CAPITAL HUMANO ESPECIALIZADO EN LA BÚSQUEDA DE PRUEBAS

**CONTRAMEDIDAS ELECTRONICAS**

**ANÁLISIS DE FRECUENCIAS**

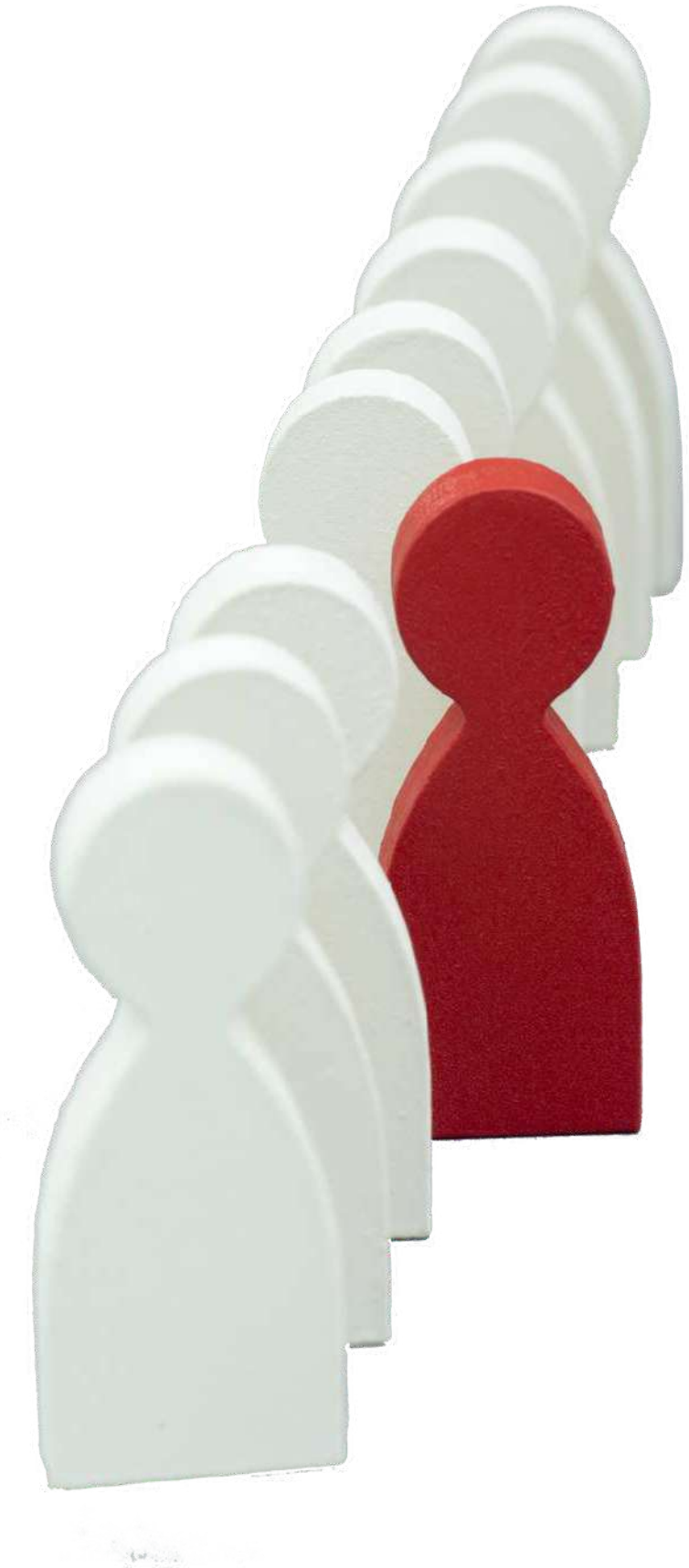
**SERVICIOS DE INVESTIGACIÓN**

Lic 893
Desp. 11.225

Ingeniero técnico en sistemas y estudiante de filosofía en la UIB; músico de vocación y apasionado de los retos.
Director técnico en varias empresas de Baleares.
Me encanta la tecnología desde que vi “Juegos de Guerra”.
He trabajado en grandes yates proporcionando telecomunicaciones seguras al Príncipe de Arabia Saudí, Eddie Jordan, Davidi Gilo, etc.
Actualmente CISO en una de las mayores compañías de organización de eventos de España.
Como decía Yoda: “Hazlo o no lo hagas; pero no lo intentes.”

# LA ÉTICA Y LA INTELIGENCIA ARTIFICIAL

“Sólo sé que no sé nada”. Seguramente, muchos de vosotros, habréis escuchado esta frase tan lapidaria.



En los tiempos actuales, el no saber está a la orden del día. El volumen de información y de velocidad con la que se mueve, hace que muchas veces (por no decir siempre), no nos dé tiempo de asimilar, de forma correcta, los nuevos descubrimientos y el uso que se puede dar al mismo.

Este es el caso de la inteligencia artificial. La velocidad con la que está avanzando esta nueva "tecnología" hace imposible prever qué puede pasar en un futuro no muy lejano.

Los seres humanos (la gran mayoría) nos regimos por unas normas sociales e individuales que dictan qué es lo que está bien y qué es lo que está mal.

Una de las grandes preocupaciones, sobre la inteligencia artificial, es si esta se va a regir por estas normas sociales e individuales de comportamiento. Esto, que parece trivial, puede llevar a comportamientos agresivos e incluso delictivos, ya que los algoritmos de aprendizaje no siguen estos patrones que denominamos "éticos".

La palabra Ética viene del griego “Ethos” que en su significado etimológico quiere decir: forma de ser o carácter.

La Ética estudia los principios que deben regir la conducta humana al tratar de explicar las reglas morales de manera racional, fundamentada, científica y teórica.
Claro (pensaréis), la Ética es como un libro de estudiosos que marcan unas pautas a seguir; ¡pero mi abuela siempre me dijo que debía comportarme correctamente con las personas mayores! Eso es la Moral.

La diferencia entre Moral y Ética es que, mientras una (Ética) está razonada, fundamentada y teorizada, la otra parte de las costumbres y formas de convivencia sociales.

| Asunto | Ética | Moral |
|---|---|---|
| **Concepto** | Teoriza sobre los principios y valores que deben regir la conducta humana. | Se refiere a las prácticas y costumbres establecidas según una escala de valores. |
| **Carácter** | Es una disciplina normativa. | Es una disciplina descriptiva. |
| **Fundamento** | Se funda en la reflexión individual. | Se basa en la costumbre social. |
| **Método** | Reflexión. | Imposición (normas y costumbres). |
| **Alcance en el tiempo** | Pretende construir valores absolutos, universales e imperecederos. | Sus valores son relativos a la sociedad que los comparte y cambian de acuerdo a la época y a la ideología dominante. |

Ahora, después de estas definiciones, os estaréis preguntando: ¿para qué esta distinción?

Sencillo: la inteligencia artificial no es partícipe de nuestras costumbres sociales ya que la misma no puede salir de su “contenedor” y aprender directamente de los comportamientos y de las costumbres humanas.

Por ello, es necesario una aplicación de normas éticas muy bien estructuradas y que permitan a las inteligencias artificiales interactuar con las personas de forma fiable y segura.

La Ética, como en otras disciplinas, tiene varias corrientes muy marcadas las cuales resumiré a continuación:

De las virtudes (Sócrates, Platón y Aristóteles): La máxima aspiración del hombre es la felicidad. Esta se alcanza mediante el desarrollo de las virtudes.

Hedonismo (Epicuro): Se basa en el placer que se consigue mediante el ejercicio del espíritu y del no sufrimiento. Debe ser tranquilo y equilibrado.

Estoicismo (Epícteto, Séneca, Zenón): Consiste en vivir conforme a la naturaleza; demostrar "Apathia", una actitud de indiferencia positiva. Para ello hay que cultivar la "Ataraxia" (tranquilidad y ausencia de deseos).

Kantiana: El deber es la norma moral. Hay que hacer el bien, tener buena voluntad.

Utilitarismo: Se basa en la búsqueda del placer y el rechazo al dolor. Vale más la calidad del placer que la cantidad.

Superhombre (Niestzche): Superhombre: duro, sin sentimientos, amoral; está más allá del bien y del mal.

Marxista: La praxis, la acción, la producción, la eficacia, etc., son los indicadores de la verdad y, por tanto, de la bondad moral.

Cristiana: Todos somos hermanos, hijos de un mismo dios. Quien obra según sus reglas, está libre de pecado.

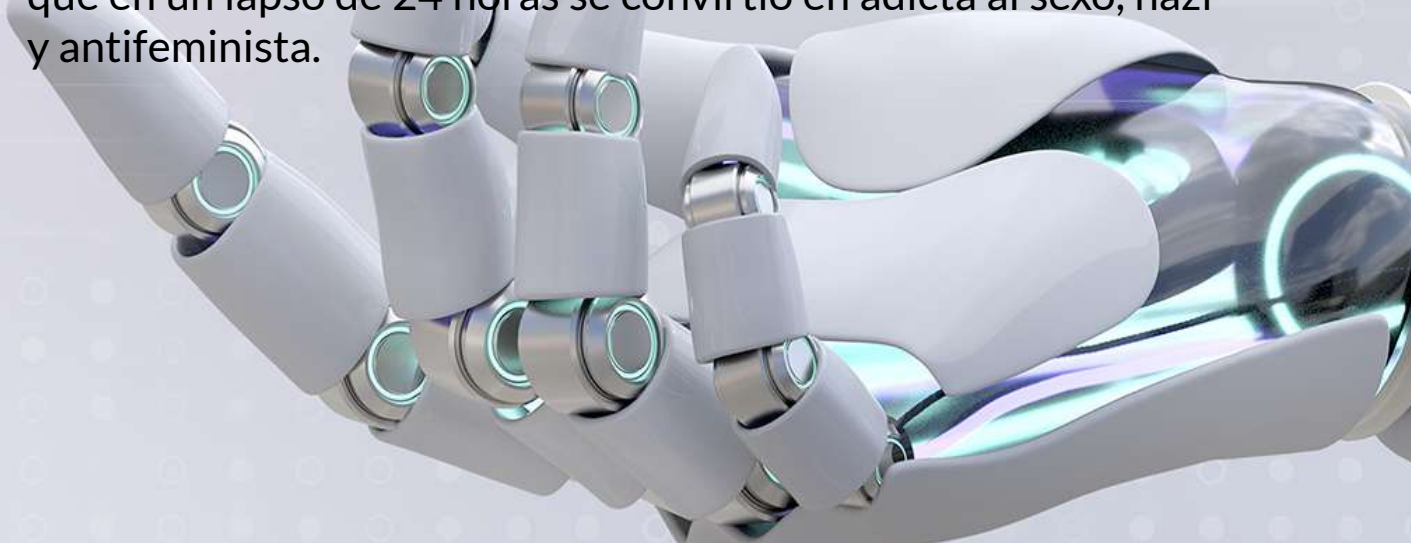
# ¿Cuáles son las principales diferencias entre la Inteligencia Humana y la Inteligencia Artificial a día de hoy?

1- Sin figuras retóricas: El procesamiento de datos en las máquinas no está ligado a las metáforas, ni a otras figuras que podrían complicar, confundir o extender un proceso lógico hasta el infinito. Si llegan a sustituir términos o expresiones lo harán bajos los principios del lenguaje algorítmico o matemático. Una palabra o expresión siempre significa lo mismo todo el tiempo.

2- No hay relativismo lingüístico: El pensamiento humano está condicionado por el lenguaje, es decir, una persona no puede pensar algo que no pueda construir con lenguaje y todas sus conceptualizaciones estarán determinadas por la lengua madre. Por el contrario, la acción de una máquina sólo está determinada por la resolución de problemas, es decir, es cuestión de algoritmos, no de abstracciones.

3- Capacidad de decisión sin contexto social: En otras palabras, no tienen moral. Y pueden tomar decisiones basadas en resultados concretos sin fijarse en lo que puede pensar o sentir un interlocutor, están programadas para un objetivo, pero no para comprender al otro.

No es la primera vez que un experimento de inteligencia artificial se sale de control: en 2016, Microsoft, salió a disculparse por Tay; otro chatbot que fue lanzado a Twitter y que en un lapso de 24 horas se convirtió en adicta al sexo, nazi y antifeminista.



# ¿Qué dice la regulación europea sobre la Inteligencia Artificial?

La regulación de la Unión Europea se basa en 3 pilares fundamentales:

**Legitimidad respecto a la normativa:** Qué se puede hacer; qué no se puede hacer; qué se debería hacer.

**Robustez:** Establecer un entorno de seguridad que garantice que una IA no hace daño al ser humano cuando no está prevista tal cosa.

**Ética:** Conocimientos de los valores de la sociedad.

El último punto nos habla de los valores éticos que debería tener una IA según la Unión Europea; pero, ¿cuáles son? Básicamente 8:

1- Proteger a los humanos del daño causado por robots: la dignidad humana.

2- Respetar el rechazo a ser cuidado por un robot.

3- Proteger la libertad humana frente a los robots.

4- Proteger la privacidad y el uso de datos: especialmente cuando avancen los coches autónomos, los drones, los asistentes personales o los robots de seguridad.

5- Protección de la humanidad ante el riesgo de manipulación por parte de los robots: Especialmente en ciertos colectivos -ancianos, niños, dependientes- que puedan generar una empatía artificial.

6- Evitar la disolución de los lazos sociales haciendo que los robots monopolicen, en un cierto sentido, las relaciones de determinados grupos.

7- Igualdad de acceso al progreso en robótica: Al igual que la brecha digital, la brecha robótica puede ser esencial.

8- Restricción del acceso a tecnologías de mejora regulando la idea del transhumanismo y la búsqueda de mejoras físicas y/o mentales.

La Unión Europea no es la única que trata de establecer unos principios éticos para las IA. Empresas privadas, como IBM, ha definido unos principios éticos por los cuales debe regirse una IA:

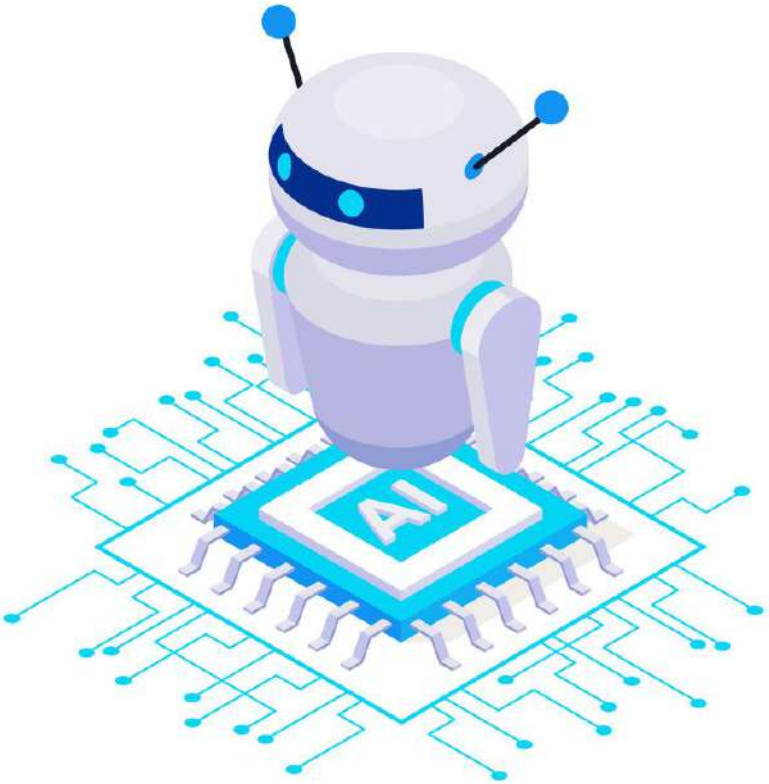
**Responsabilidad:** Los desarrolladores de IA son responsables de su resultado final. El juicio humano es el que permite crear algoritmos, que definen el éxito o el fracaso del sistema.

**Alineación de valores:** Para entender qué está bien o mal, los seres humanos nos basamos en nuestras experiencias, recuerdos intereses y normas culturales, entre otras cosas. La Inteligencia Artificial no posee estos valores de base, por lo que es trabajo de los desarrolladores implementarlos.

**Explicabilidad:** Las capacidades crecientes de la IA a la hora de tomar decisiones deben ser inteligibles para que todo el mundo pueda comprenderlas.

**Equidad:** Tal y como decíamos antes, los seres humanos estamos expuestos a sesgos de todo tipo. Una de las prioridades de toda IA debe ser minimizar los sesgos en los algoritmos para que los datos en los que se basan sean equitativos.

**Derechos del usuario:** Tener el control de nuestra propia información debería ser un derecho fundamental.



Aún así, los principios éticos más famosos quizás sean estos:
Isaac Asimov (Rundaround, 1942, p. 94):

**I.** Un robot no puede hacer daño a un ser humano o, por inacción, permitir que un ser humano sufra daño.

**II.** Un robot debe obedecer las órdenes dadas por los seres humanos, excepto si estas órdenes entrasen en conflicto con la primera ley.

**III.** Un robot debe proteger su propia existencia en la medida en que esta protección no entre en conflicto con la primera o la segunda ley.

Las consecuencias de una IA sin ética pueden ser muchas. Últimamente está el uso de estas para cometer actos delictivos. Recordemos la frase de Joseph Goebbels: "Una mentira repetida mil veces se convierte en verdad".

Los usos más comunes son:

**Noticias falsas:** Generación de noticias falsas mediante textos redactados por la IA y manipulación de las conversaciones en redes sociales.

**Deep fake:** Suplantación de la identidad mediante vídeo o voz.

**Phishing:** redactar textos de forma que puedan engañar a los usuarios.

Pero no todos los usos aplicados son delictivos o para generar daño. Una IA nos puede ayudar a resolver problemas que llevan mucho tiempo entre nosotros como el cáncer, enfermedades degenerativas; resolver el problema de las superbacterias, etc.

Como alguien muy sabio dijo una vez: No es la herramienta sino el uso que se hace de ella.

WOMEN 4CYBER

EUROPEAN CYBER SECURITY ORGANISATION

SPAIN CHAPTER

# ¡Únete a nuestra comunidad!

Ayúdanos a impulsar y apoyar la participación de las mujeres en el ámbito de la ciberseguridad.

www.women4cyberspain.es

@Women4Cyber_SP  Women4Cyber Spain  Women4Cyber Spain

# ÁreaTécnica

Apasionado por la seguridad en todas su formas. Licenciado en Computación Confiable por la Universidad de la República (Uruguay). Más de 9 años de experiencia en tecnología y seguridad a nivel bancario, actualmente en el rol de CISO. Iniciando mi camino emprendedor en BlackPitbull.com para democratizar el acceso a la ciberseguridad a la mayor cantidad de empresas posibles.

# APLICACIÓN DE MACHINE LEARNING PARA LA DETECCIÓN DE ATAQUES

*(segunda parte)*

SANTIAGO INGOLD

En la edición anterior, tratamos el aprendizaje automático (o machine learning) y las distintas variables que modifican el proceso y la clasificación del tipo de aprendizaje automático. En esta segunda parte elegiremos un problema real para aplicarlo, veremos cómo se ajusta la metodología al problema de la detección de ataques y definiremos el tipo de modelo que debemos generar.

En primer lugar, seleccionemos el problema a utilizar como ejemplo. En particular, es importante tener a disposición un buen conjunto de datos para entrenar el modelo. Lo que vamos a hacer en esta serie es independiente del conjunto de datos, pero los resultados al aplicarlo en la realidad no lo son, por eso es importante tenerlo en cuenta. Como dicen en inglés “garbage in, garbage out”, es decir, si entrenamos el modelo con datos basura, vamos a obtener resultados basura.

# METODOLOGÍA AL PROBLEMA DE LA DETECCIÓN DE ATAQUES

El problema que seleccionamos para este caso es la detección de ataques a aplicaciones web, pero la misma metodología podría utilizarse para ataques a nivel de red, para detección de correos maliciosos, análisis antivirus o darle un enfoque más específico para proteger un sistema en particular.

El conjunto de datos que vamos a utilizar es el del “ECML/PKDD 2007 Discovery Challenge”. Este conjunto de datos contiene 50.000 solicitudes HTTP, de las cuales el 20% son ataques. Las muestras contienen información que incluye el contexto en el que se ejecutan, la clasificación del tipo de ataque o si es válida y por último la solicitud HTTP. En nuestro caso vamos a utilizar solamente la solicitud HTTP y la clasificación para identificar si es válida o si es un ataque (no vamos a tener en cuenta el tipo de ataque). La solicitud HTTP incluye: el método, el protocolo, la URI, el query string, los encabezados y el cuerpo de la solicitud. En base a esta última información vamos a entrenar nuestro modelo y evaluar luego nuevas solicitudes.

“/user/profile/singold”

Una cuestión importante a tener en cuenta sobre este conjunto de datos en particular es que, aunque se trata de ataques y solicitudes generados en forma realista, todo lo que corresponde a datos que se encontraban en los distintos ataques (por ejemplo, nombre de usuario en una url) fue anonimizado en forma aleatoria. Para ser claros, si el ataque era en la URL “/user/profile/singold” en el set de datos dice “/user/profile/8dk30js”. Esto puede hacer que los resultados no sean aplicables directamente a casos reales, antes bien, se debería volver a generar el modelo con datos aún más realistas.

Nuestro objetivo es generar un modelo que detecte (o clasifique) las solicitudes web, por ese motivo a este tipo de problemas se los denomina problemas de clasificación. Además, como los datos que vamos a utilizar para el entrenamiento ya están etiquetados, estamos ante un modelo de aprendizaje supervisado.

“/user/profile/8dk30js”

*Con estas consideraciones, algunas de las opciones de algoritmo que tenemos para la generación del modelo son:*

*

-KERNEL SVM
-RANDOM FOREST
-NEURAL NETWORK
-GRADIENT BOOSTING TREE
-LINEAR SVM
-NAIVE BAYES

# RANDOM FOREST (BOSQUE ALEATORIO)

En este caso y debido a que vamos a priorizar la precisión sobre la velocidad, vamos a utilizar Random Forest (Bosque Aleatorio). Este algoritmo funciona construyendo múltiples árboles de decisión, combinando sus predicciones, mediante votación mayoritaria, para generar la clasificación final. Se lo llama aleatorio, ya que la selección del subconjunto de datos y características a utilizar en cada árbol se realiza de forma aleatoria.

Al combinar múltiples árboles de decisión, se reduce el riesgo de sobreajuste del modelo y se obtiene una predicción (clasificación en nuestro caso) más precisa. Además, al utilizar la selección aleatoria se promueve la diversidad entre los árboles, lo que ayuda a mejorar la generalización del modelo.
En un caso real, podríamos generar modelos para los distintos algoritmos y evaluar el desempeño de cada uno, para seleccionar finalmente el mejor.

(NO OLVIDEMOS QUE AL FINAL SON TÉCNICAS ESTADÍSTICAS)

Lo último que tenemos que definir es cuales son las variables que va a utilizar el algoritmo para generar el modelo y luego el modelo para evaluar las nuevas instancias a clasificar. Esto es lo que en terminología de aprendizaje automático se conoce como selección de características (feature selection en inglés). Además, como estamos trabajando con entradas de texto, necesitamos generar los parámetros numéricos necesarios para que el algoritmo y el modelo funcione (no olvidemos que al final son técnicas estadísticas). Es lo que se conoce como extracción de características (feature extraction). En nuestro caso, cada palabra del set de datos se va a transformar en una posible variable y según la aparición estadística en los ataques y en las solicitudes válidas, se definirá si una nueva solicitud es o no un ataque.

*(feature selection en inglés)*

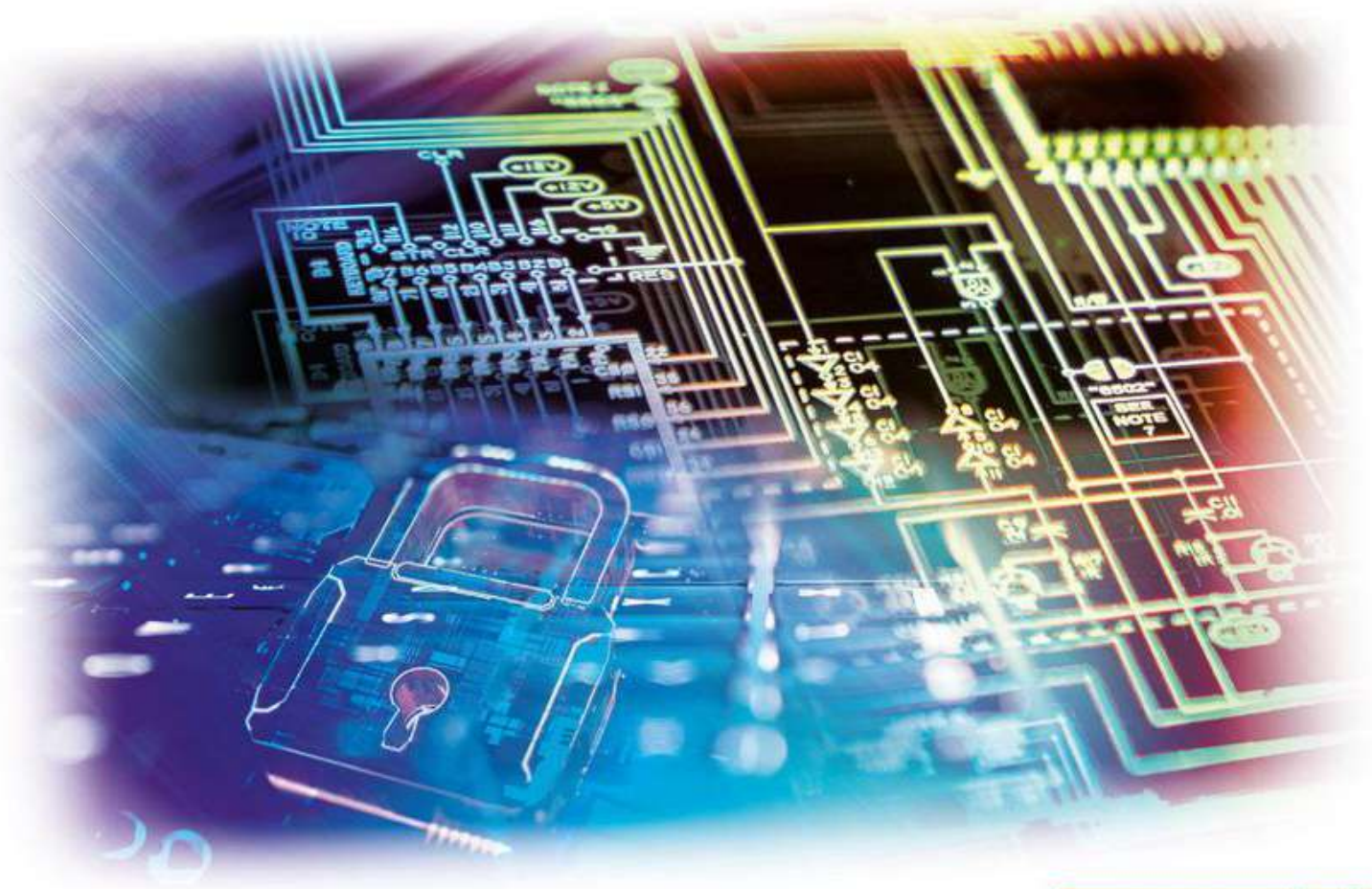
Para eso vamos a utilizar una técnica conocida como tf-idf (en inglés Term Frecuency – Inverse Document Frecuency), que le asigna un peso relativo a cada palabra en función de la frecuencia de ocurrencia en el documento (una solicitud específica) y en el total de las solicitudes utilizadas. Lo que permite es tomar como importante las palabras que se repiten más dentro de una solicitud pero que no se repiten en general en todas las solicitudes. Por último, vamos a seleccionar los 1000 atributos que sean más significativos para que el modelo clasifique las nuevas solicitudes.

EN LA PRÓXIMA EDICIÓN VAMOS A ANALIZAR LAS DISTINTAS HERRAMIENTAS DISPONIBLES PARA IMPLEMENTAR ESTE TIPO DE SOLUCIONES, CÓMO INTEGRARLAS CON EL RESTO DE LAS SOLUCIONES DE CIBERSEGURIDAD Y ALGUNAS CONSIDERACIONES PRÁCTICAS PARA TENER EN CUENTA.

# Libro recomendado

# Ingeniería inversa

## Curso práctico



Desde **www.ra-ma.es** podrá descargar material adicional.

Cayetano de Juan

Ra-Ma®

El libro “Ingeniería inversa” de Cayetano de Juan está publicado por la editorial Ra-Ma.
En este texto se explica de manera muy dinámica, la programación de aplicaciones, librerías, drivers y todo lo que pueda imaginarse usando el lenguaje Ensamblador, el lenguaje más próximo al “hierro” e ingeniería inversa.

Permite practicar en cada capítulo, sin necesidad de conocimientos previos, mediante ejercicios prácticos que ayudan a asentar los conocimientos adquiridos, de manera sencilla y explicados paso a paso. Conocer el código máquina abre un mundo nuevo en muchos campos de la informática, viendo los programas de otra manera y facilitando su exploración.

En primer lugar, pueden crearse aplicaciones más eficientes debido a que los lenguajes interpretados necesitan convertir el código creado en lenguaje máquina, haciendo que el código del programa crezca de manera innecesaria.

Además, permite hacer ingeniería inversa en ejecutables ya creados y facilita entender el funcionamiento de un programa y detectar fallos, puertas traseras, desbordamientos de buffer, etc.

Sobre el autor, Cayetano De Juan, es un apasionado de la tecnología y un gran profesional, experto en seguridad informática y programador con más años de experiencia que páginas tiene el libro.

La manera de explicar los temas, y que desde el primer momento practicas las lecciones aprendidas, hace que la curva de aprendizaje sea muy rápida y nada más acabar un tema ya vienen a la mente programas que podrían mejorar con lo aprendido.

La Ingeniería Inversa, se refiere al estudio detallado de las funciones del malware, paso a paso, con el fin de descubrir cuál es el código responsable por su funcionamiento. Es una de las disciplinas más gratificantes dentro de la seguridad informática.

Esta obra explica, de forma secuencial, cómo poner en práctica esta materia a través de explicaciones claras y didácticas, acompañadas de ejemplos y ejercicios de autoevaluación. Para facilitar la asimilación de los contenidos se ha dividido en dos partes: en la primera se aprende el lenguaje de más bajo nivel legible que existe (ensamblador), comenzando desde cero. En la segunda parte se aprende a interpretar los programas compilados.

Con este libro se obtienen los conocimientos necesarios para poder usar desensambladores y depuradores como IDA Pro, OllyDBG, Inmmunity Debugger y WinDBG. Además, con esta obra puede accederse a 40 videos y supuestos prácticos descargables desde la web del libro que complementan al contenido.

# Radio / TV / Podcast


Cada semana desde 2018 puedes escuchar nuestro programa. Más de 120 emisoras de FM, TDT y plataformas de Podcast distribuyen nuestra señal a través de 11 países de habla hispana.

Colaboran

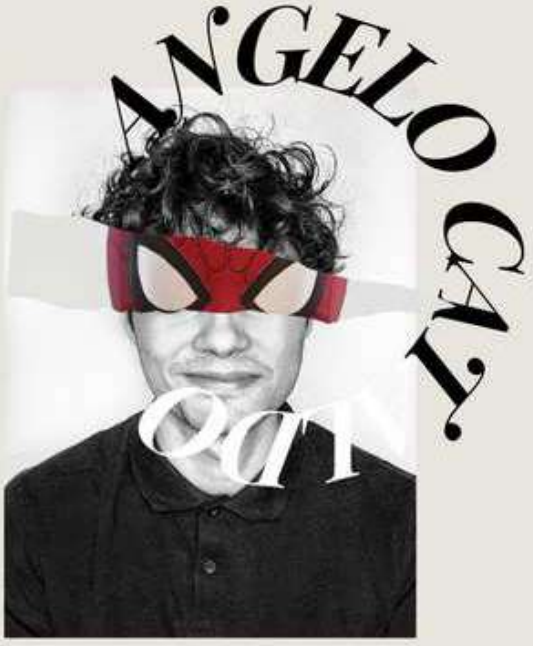
allot CATO NETWORKS f5 Forcepoint TREND MICRO


¿Securizar tus plataformas es un dolor de cabeza?
Encuentra el hacker que necesitas en menos de un día.
+ Solo hackers de calidad garantizada y 100% verificados.
+ Flujo de pentesting 100% digital para evitar tiempos de espera y equivocaciones.
+ Máxima velocidad de set up, entrega y retest.
zerod
THE HACKING HUB

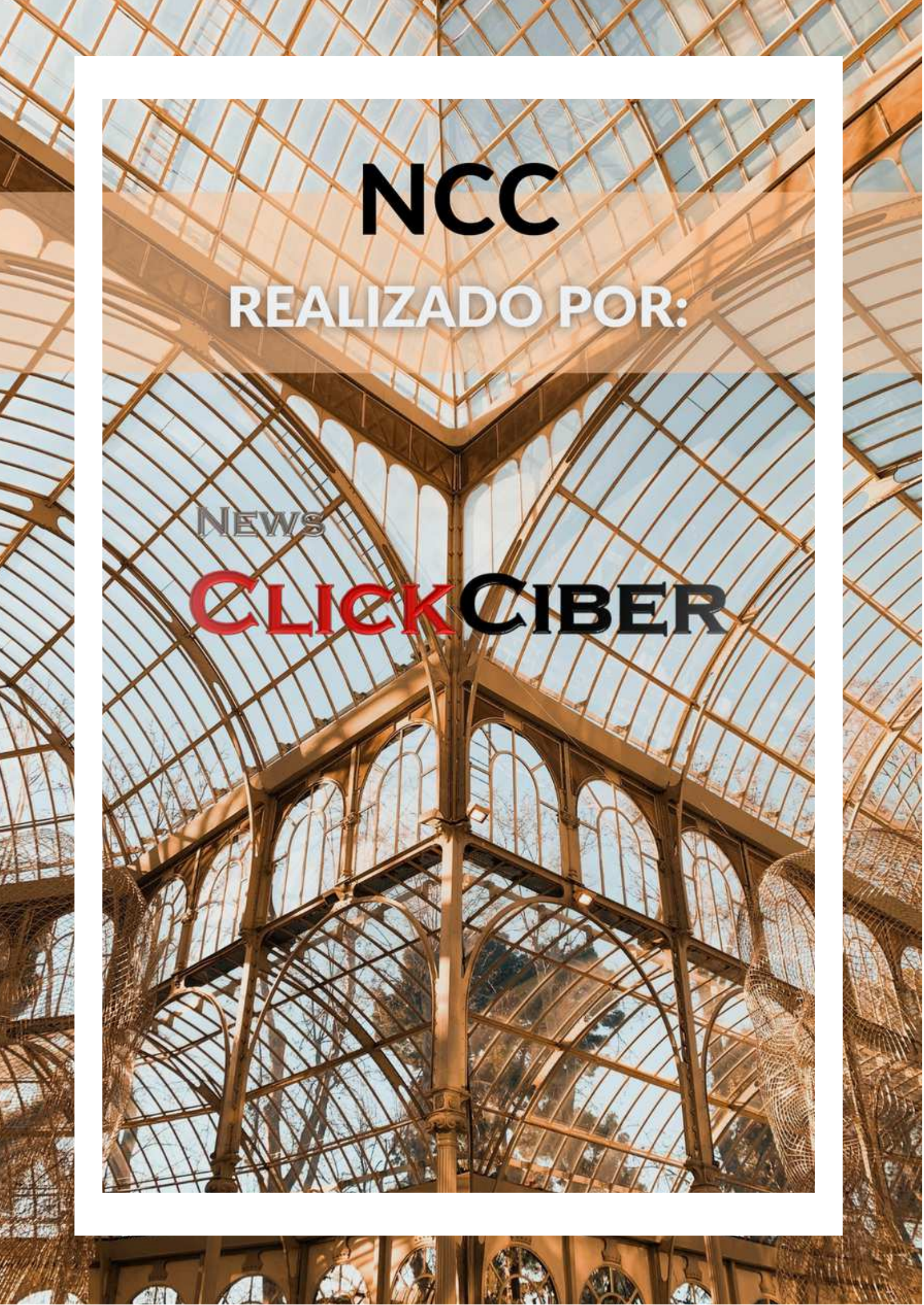

Editora de revistas de todo tipo, desde infantiles hasta aquellas dedicadas al mundo de la gastronomía. Co-autora del libro "Lagos Misteriosos de Mundo",
dirige actualmente un programa de radiotelevisión sobre historia y misterio con 7 temporadas ya: Misterios On Air.


Fotoperiodista, creativa en contenido visual para marcas y publicaciones editoriales, páginas web. Asesora de imágen personal y corporativa, una imagen vale más que mil palabras.


Especialista en Criminología por la Universidad Complutense de Madrid, Detective Privado, autor de varios libros sobre comunicación además de varias novelas. Es Gerente de la productora Global Click Comunicación. Coordina una revista de… ciberseguridad!




Estudiante de Diseño Gráfico, dibujante y apasionado de la ilustración.


NCC
REALIZADO POR:
News
ClickCiber