Nº2 · JUNIO 2018

Nº2 · JUNE 2018

IoT & ELEVATORS

JOSÉ RAMÓN MONLEÓN
Manager Seguridad Información Corporativa en Orange España

JOSÉ RAMÓN MONLEÓN
Corporate CISO at Orange Spain

Ciberseguridad
en la era de la hiperconexión

Cybersecurity
in hyper-connectivity times

Internet of Things
Retos de un sector en constante innovación

Internet of Things
Challenges of an industry innovating constantly

Nayar Systems
Innovación, conectividad y talento

Nayar Systems
Innovation, connectivity and talent

Performance

Innovación tecnológica para el futuro de las empresas

Technological innovation for the future of companies

Soluciones globales de comunicación
Global communication solutions

Soluciones de IoT y Big Data
IoT and Big Data solutions

Soluciones de seguridad y cloud
Security and cloud solutions

Transformación digital al servicio de las empresas

Digital transformation at the service of companies

Más información en: grandes.clientes@orange.com
Further information at: grandes.clientes@orange.com

orange™

DEPÓSITO LEGAL / LEGAL DEPOSIT:
CS 758-2017

NAYAR SYSTEMS
Calle Taxida, 10
12003 CASTELLÓN (Spain)
(+34) 964 066 995
info@nayarsystems.com
www.nayarsystems.com

COORDINACIÓN Y DISEÑO / COORDINATION AND DESIGN:
RESPIRA COMUNICACIÓN
Calle San Isidro Labrador, 15 · Bajo
12004 CASTELLÓN (Spain)
(+34) 964 22 00 43 · (+34) 654 85 60 46
info@agenciarespira.com
www.agenciarespira.com

FOTOGRAFÍA DE PORTADA / COVER PHOTO:
Nicolás Arias

IMPRESIÓN / PRINTING:
DIPUTACIÓ D E CASTELLÓ
www.dipcas.es
Impreso en España
Printed in Spain

IOT & ELEVATORS

Índice

Index

IoT&Elevators, la divulgación del conocimiento

IoT&Elevators, the dissemination of knowledge

Tras el éxito del anterior número presentado en Interlift 2017, hoy podemos daros de nuevo la bienvenida al **segundo número de IoT&Elevators.** En Nayar Systems nos esforzamos diariamente por fomentar la divulgación del conocimiento entorno a la innovación tecnológica y el Internet of Things, y por eso creamos este medio de forma totalmente gratuita, tanto para las empresas participantes como para los lectores.

En esta ocasión, este número gira alrededor de una disciplina cuyo crecimiento está exponencialmente al alza en los últimos años: **la ciberseguridad.** Cada vez son más los dispositivos conectados a la red, y el Internet of Things se ha extendido por todos los sectores industriales, otorgando numerosas ventajas y beneficios para su desarrollo. Sin embargo, la gestión de la información en un entorno cibernético implica una serie de nuevos riesgos y amenazas que no podemos obviar, y es aquí donde la ciberseguridad juega un papel crucial para **garantizar la seguridad de nuestras empresas en este nuevo contexto.**

Esta publicación incluye artículos de interés y entrevistas a grandes profesionales, por lo que esperamos ayudar entre todos a enriquecer la cultura de la ciberseguridad. Desde Nayar Systems seguimos apostando por la innovación y la investigación, por **hacer de lo ordinario algo extraordinario.**

Espero que disfrutes de la lectura.

Un fuerte abrazo,

JOSÉ LUIS SANCHIS
CMO de Nayar Systems

Following the success of the previous issue presented at Interlift 2017, today we are able to give you a new welcome to the **second issue of IoT&Elevators.** In Nayar Systems we make a daily effort to encourage the dissemination of knowledge related to technological innovation and the Internet of Things. For this reason we create this media completely free for the participating companies as well as for its readers.

On this occasion, this issue addresses a subject that has been growing exponentially during the last years: **cybersecurity.** More and more devices are getting connected to the network, and the Internet of Things has spread through all industrial sectors, giving many advantages and benefits for its development. However, information management in a cybernetic environment involves a series of new risks and threats that we cannot omit. And here cybersecurity plays a crucial role **to ensure our companies are safe in this new context.**

This publication includes articles of interest and interviews with great professionals, so we expect to help enrich cybersecurity culture between all of us. From Nayar Systems we continue to believe in innovation and research, in **making the ordinary extraordinary.**

I hope you enjoy the reading.

A big hug,

JOSÉ LUIS SANCHIS
CMO at Nayar Systems


EXTRA
ORDIN
ARIO
EXTRAORDINARY
En Nayar Systems sabemos que las personas
tienen la capacidad de transformar lo ordinario en extraordinario.
Estamos construyendo nuestras nuevas oficinas, que reunirán en sus más de
1.500 m2 **investigación**, **innovación**, **conectividad** y **talento**.
At Nayar Systems we know that people
hold the capacity to transform the ordinary into extraordinary.
We are building our new headquarters, which will host in more than 1,500 m2
research, **innovation**, **connectivity** and **talent** .
MAKE THE ORDINARY
EXTRAORDINARY
NAYARSYSTEMS
72 horas
M2M TECHNOLOGIES
ADVERTISIM
net4machines
www.nayarsystems.com

Entrevista a José Ramón Monleón: “En ciberseguridad, estamos obligados a ser creativos”

Interview with José Ramón Monleón: “In cybersecurity we are forced to be creative”

¿Cómo se inició en el mundo de la seguridad de la información?, ¿qué es lo que le atrajo de este campo?

Fue en el año 2006 cuando se creó el Grupo Orange en España tal y como ahora lo conocemos, englobando todas las empresas del grupo en España bajo una única marca “Orange”.

Fue entonces cuando se creó la **figura de responsable de Seguridad Global**, era una forma diferente de ver la seguridad, hasta ese momento la Seguridad de la Información era una disciplina que se trataba solo dentro del área de IT.

La visión global de la Seguridad de la Información, **transversal a toda la organización** y **desde un punto de vista global** era un concepto muy novedoso para aquella época, sin embargo el Grupo Orange lo tenía como modelo que aplicaba a todos los países.

Era una disciplina que siempre me había atraído, sobre todo **la capacidad de poder analizar los sistemas informáticos y encontrarles defectos o vulnerabilidades** para poder protegerlos. Entonces se hablaba muy poco del tema y, además, el proyecto que me propusieron para crear todo el departamento desde cero, con una visión transversal a toda la organización me resultó muy atractivo y con un gran futuro. Suponía todo un reto, sin embargo contaba con la ayuda de todo un grupo en Francia. Ahora, al verlo con cierta perspectiva, y con el camino recorrido, puedo confirmar que **fue una decisión muy acertada.**

How did you end up in the world of information security? What drew you to this field?

The Orange Group as we now know it - a number of companies in Spain brought together under the common name of "Orange" - was created in the year 2006.

2006 was also the year in which the **figure of a person in charge of Global Security** was created. It was a different way of approaching security. Until then, information security had been a discipline only practiced within the field of IT.

This global view of information security, **transverse throughout the whole organization and from a global perspective**, was something quite new in those days, and yet, the Orange Group was already applying this model to all the countries it was active in.

It was a discipline that had always attracted me, especially because of **its ability to analyse computer systems and finding their faults and vulnerabilities** in order to protect the systems against them. You didn't hear much about this subject at the time, and I found the project that was offered to me - creating the whole department from scratch, with a cross-sectional view of the whole organization - very appealing and very promising. It was quite a challenge, but I had the support of a big group in France.

¿Cómo se le presenta la oportunidad de comenzar a trabajar en la multinacional Orange?

Fue en el año 2000, **tras el famoso "efecto 2000"** y que finalmente no fue para tanto, durante el año anterior estuve como consultor en una entidad financiera adaptando los medios de pago para que llegada esa fecha los sistemas siguieran funcionando como siempre.

Me contrataron en Amena (una de las empresas que formaron Orange en España) como consultor para el Área de Sistemas de Información y al año siguiente me propusieron formar parte de la plantilla.

¿Qué tipo de obstáculos se ha encontrado en su trayectoria profesional hasta llegar a ser Corporate CISO en Orange España?

Como he comentado anteriormente, la creación de una figura de Seguridad de la Información a nivel corporativo, transversal a toda la Organización era un concepto muy novedoso, **las organizaciones y las personas que lo componían no estaban preparadas para esta figura**, entonces los modelos eran muy jerárquicos, se trabajaba mucho por silos. Para poder avanzar en la función **había que romper esas barreras.**

Por otro lado la función de la Seguridad de la Información ha cambiado mucho, **entonces el ámbito de aplicación era mucho más reducido**, las aplicaciones apenas se externalizaban y todo estaba mucho menos interconectado.

Sin embargo, el hecho de que el Grupo aplicara la misma estructura en todos los países facilitó mucho el trabajo, además de todo el apoyo en normativas y proyectos.

Vela por la seguridad de la información corporativa de un gran gigante como es Orange España. ¿Se considera un "ciberhéroe"?

No, para nada, lo que sí **me considero es uno de los afortunados que empezaron hace muchos años en esta disciplina.** Durante estos años he tenido la fortuna de conocer a muchos colegas que empezaron a finales de los 90 - principios del 2000, ellos fueron unos pioneros, nos sirvieron de ejemplo a los demás, entonces el tema era mucho más reducido y la figura de CISO en España se reducía a una docena de profesionales. Ahora me siento orgulloso de estar a su lado.

Dedicándose al mundo de la seguridad de la información, ¿cómo sentirse seguro en Internet?

Buena pregunta, como todo en la vida, **no hay nada seguro al 100%**. Internet es como la calle de nuestras ciudades, la calle de la mayoría del mundo, por lo que tienes que tener las mismas precauciones o cuidados.

How did you get the opportunity to start working for the multinational company Orange?

It was back in 2000, **after the famous Y2K** that turned out to be not such a big deal. During the previous year, I had been working in a financial institution as a consultant, adapting its means of payment so they would keep working normally when the big date arrived.

I was hired by Amena (one of the companies that formed Orange in Spain) as a consultant for the computer department, and the next year they offered me the opportunity to work for them as an employee.

What obstacles did you encounter in your career path leading up to Corporate CISO at Orange Spain?

As I mentioned earlier, the creation of a figure in charge of information security at the corporate level and transverse throughout the organization was a very novel concept at the time. **The organizations and people making up the group were not prepared for such a figure**; the models were very hierarchical and people worked very much in silos. In order for me to advance in my position, **those barriers had to be broken**.

Furthermore, the function of information security has changed a lot over time. **In those days its field of application was much smaller**, applications were hardly ever externalized, and everything was much less interconnected.

However, the fact that the group applied the same structure in all its countries made my job much easier, in addition to all the support I received with regulations and projects.

You look after corporate information security at a giant multinational like Orange Spain. Do you consider yourself a cyberhero?

No, not at all. **I do consider myself to be one of few lucky people to have started working in this field many years ago**. During those years I had the good fortune of meeting many colleagues who started around the turn of the century. They were pioneers serving as role models for us. The field was much smaller and in all of Spain there were no more than a dozen CISOs. Now I feel proud to be standing alongside them.

As an expert in information security, can you tell us how to feel safe on the Internet?

That is a good question. As in life, **nothing is 100% safe.** Internet is like the streets of our cities, the streets of most of the world, so you need to be equally careful and take the same precautions.

Lo más importante es **dejarse guiar por el sentido común**, "que es el menos común de los sentidos", aplicar las mismas reglas del mundo físico, desconfiar de aquello que no vemos claro.

Sin embargo, **con la aparición de las redes sociales, las personas se han relajado**, ponen toda la información en público en manos de terceros, sin darse cuenta que se están desnudando en público.

Algunos consejos que se pueden dar:

- **Desconfía de los correos que no has solicitado** y que tienen remitentes o enlaces desconocidos.
- **No des a nadie tus contraseñas,** ni por teléfono ni contestando a un correo.
- **Navega por sitios confiables.**

¿Cómo se mantiene al día Orange de posibles ataques de los cibercriminales?

Disponemos de un **Centro de Operaciones de Seguridad**: es un equipo organizado y altamente cualificado cuya misión es **proteger y defender los activos de la compañía y mejorar continuamente la situación de seguridad de Orange.** Trabajamos en diferentes vías: prevención, protección y detección.

Para la parte de prevención trabajamos en colaboración con **el desarrollo de aplicaciones y servicios para que estos tengan la definición de la seguridad por defecto**. Disponemos también de elementos de protección de activos, en especial los que están expuestos a internet.

¿Qué soluciones ofrece Orange en materia de ciberseguridad?, ¿es una de sus prioridades estratégicas?

Actualmente nuestros servicios de seguridad se engloban bajo la marca **Orange Security Suite.** Se trata de una solución de **Seguridad Perimetral**, compuesta por los siguientes servicios, disponibles de forma independiente:

The most important thing is **to use common sense**, which is "the least common of the senses", and to apply the same rules you would in the real world, to not trust when you have any doubts.

However, **the emergence of social media has led people to relax**, and they now place all their information in the hands of third parties, not realizing that they are essentially opening up in public.

Some advice:

- **Be wary of unsolicited emails**, those that have no reply address and those containing unknown links.
- **Give your passwords to no one**, neither on the phone, nor in reply to an email.
- **Surf trusted sites**.

How does Orange stay abreast of possible attacks by cybercriminals?

We have a **Security Operations Centre**, an organized and highly qualified team whose mission is **to protect and defend the company's assets and to continuously improve Orange's security situation**. We work on different fronts: prevention, protection and detection.

Regarding prevention, we help developers of **applications and services incorporate security measures in their products by default**. We also use elements for asset protection, especially those exposed to the Internet.

What solutions does Orange offer in matters of cybersecurity? Is it one of their strategic priorities?

Currently, our security services are all grouped under the name **Orange Security Suite**. Orange Security Suite is a **perimeter security** solution composed of the following services, which are available independently:

- PS/IDS
- Web Filtering
- Antivirus

It is a security service offered directly through the net, aimed at companies, that **does not require any devices to be deployed on clients' premises, no software to be installed on their computers, and no specialized computer-security team.**

Furthermore, **it is a modular package** that can cover clients' security needs selectively without them having to pay for services they do not need.

It is also flexible and can provide reliable protection for data-transfer rates from 2 to 200Mbps **without any need for costly hardware acquisition or equipment**

- IPS/IDS
- Web Filtering
- Antivirus

Se trata de un Servicio de Seguridad ofrecido directamente desde la red dedicada a Empresas que **no requiere despliegue de dispositivos en las dependencias de cliente, ni la instalación de SW en los PCs del cliente, ni un equipo especializado de seguridad IT.**

Además **es una oferta modular**, ya que permite cubrir los servicios de Seguridad que necesitan los negocios de los clientes, sin ser necesaria la contratación de funcionalidades que no aportan valor.

También es flexible, y permite proteger caudales con una capacidad de 2 hasta 200Mbps garantizados, **sin la necesidad de adquisición de costoso Hardware ni cambio de equipamiento**. Todo ello con una Plataforma de Seguridad actualizada diariamente con las últimas firmas de Seguridad, mantenida y operada por nuestros expertos Orange y con la posibilidad de Gestión delegada en Orange o de Autogestión.

Es evidente que **se trata de una prioridad estratégica para nosotros**, por lo que estamos trabajando en ampliar nuestro porfolio para los clientes, apoyados en el SOC interno (Centro de Operaciones de Seguridad) y ofrecer servicios con un SOC para clientes.

Háblenos de iSec4IoT (Intelligent Security for IoT - Orange Lab) y en qué medida promueve la excelencia en cuanto a desarrollo e implementación de soluciones de ciberseguridad.

El **centro de excelencia de Routers e IoT** nace como respuesta a las amenazas que comenzaron a surgir en este ámbito en el año 2016, con el objetivo inicial de **proteger los routers que suministramos a nuestros clientes, detectar incidentes de seguridad y realizar pruebas de seguridad de routers** en un entorno controlado, idéntico al de un cliente.

En el caso de los routers, se trata del elemento que une a los clientes con internet expuesto a las amenazas de la red. Hay que tener en cuenta que, en la mayoría de los casos, se encuentra encendido las 24 horas del día y "expuesto", **siendo la diana potencial de ataques informáticos**, bien sean puntuales o como parte de campañas elaboradas con diferentes propósitos, como puede ser dejar sin servicio al usuario, robar la identidad o credenciales. Hay numerosos ejemplos recientes de ataques masivos a routers, en algún caso con gran repercusión.

Desde el laboratorio de seguridad de Orange España **se replican los escenarios "tipo" de clientes de Orange en los que se monitoriza la actividad que ese router recibe desde internet.**

change. All of this with a security platform updated daily with the latest virus signatures, maintained and operated by our own Orange experts, and either remotely managed by Orange or self-managed.

This is obviously **a strategic priority for us**, and we are working on expanding our portfolio with the help of our internal SOC (Security Operations Centre), which allows us to offer clients services with a SOC.

Tell us about iSec4IoT (Intelligent Security for IoT – Orange Lab) and the extent to which it promotes excellence in the development and implementation of cybersecurity solutions.

The Routers and IoT centre of excellence was created in reply to the threats that started appearing in this field in 2016. Its initial objective was **to protect the routers we provide to our clients, detect security incidents, and perform security tests on routers** in controlled environments identical to those of our clients.

On the one hand we have routers, the element connecting clients to the Internet which is, as such, exposed to web threats. Turned on and "exposed" twenty-four hours a day in most cases, **they are the potential targets of cyberattacks**, either isolated

Por otro lado, están los **dispositivos IoT** que están entrando en nuestro hogar y empresas. Cada vez es más frecuente encontrarse con **nuevos dispositivos capaces de conectarse a Internet y permitir al usuario un control y manejo de forma remota** desde cualquier parte del mundo, pero esto no ha hecho más que comenzar.

Por eso, en 2017 ampliamos el Centro a estos dispositivos con el fin de **adelantarnos a las amenazas del futuro.** El mayor riesgo que tiene un dispositivo IoT es que en la mayoría de los casos **ha sido diseñado sin seguridad**, por lo que resultan muy vulnerables y apetecibles para los ciberdelincuentes. Una vez analizado y vulnerado un dispositivo, el ciberdelincuente tiene miles o millones de dispositivos idénticos conectados a internet a los que puede atacar. Desde el laboratorio pretendemos certificar los dispositivos IoT para que **cumplan con un mínimo de nivel de seguridad**, elaborar medidas de protección y de detección que eviten los ataques y ser capaces de detectar cualquier amenaza que pueda afectarlos.

¿Cuál es su misión principal como miembro de GSMA IoT Security?, ¿qué tipo de iniciativas lleva a cabo?

La GSMA es la asociación que engloba a todas las empresas del sector de la telefonía móvil, Orange como operador forma parte de ella. Entendemos que

ones or campaigns organized for different purposes, such as denying customers service, or stealing their identity or credentials. There are many recent examples of massive attacks on routers, some of them with serious repercussions.

Orange Spain's security laboratory **replicates typical client scenarios to monitor the activity received from the Internet.**

And then there are the **IoT devices** that are entering our homes and businesses. It is increasingly common to find **new devices capable of connecting to the Internet and allowing users to remotely control** them from anywhere in the world, but this is just the beginning.

For this reason, in 2017 we expanded our centre to include these devices in order **to anticipate the threats of the future**. The biggest risk with IoT devices is that in most cases **they are designed without security**, which makes them very vulnerable and appealing to cybercriminals. Once a device has been analysed and its weaknesses discovered, cybercriminals have thousands or millions of identical targets connected to the Internet that they can launch attacks on. We want our laboratory to certify IoT devices so **they meet at least some basic security requirements**, and we also want to design protection and detection measures capable of avoiding attacks and detecting any threat that may affect them.

What is your main mission as a member of GSMA IoT Security? What type of actions do you take?

The GSMA is the association that brings together all the companies in the mobile industry. Orange, as an operator, is a member. It is our understanding that, in order to design and protect IoT devices, **we need to work together with the sector**, sharing knowledge and defining common rules and regulations that must be applied by default in all devices. Our mission is to support and cooperate with this team to help the different lines advance toward the objective of protecting devices.

The GSMA, together with the mobile industry, has designed a range of resources to guide companies in matters of security **to face the challenge of securing the connected future.** A guide with security guidelines has been developed. Drawing on its wide experience in security, the GSMA, together with the mobile industry, has created a set of IoT **Security Guidelines**, backed by an IoT security assessment framework, to provide a robust, tested approach to ensuring end-to-end security. This guide is free and is available on the Internet at:
https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

para poder diseñar y proteger dispositivos IoT **debemos trabajar en colaboración con el sector**, compartiendo conocimiento y definiendo reglas y normas comunes que se apliquen por defecto en los dispositivos. Nuestra misión es la de apoyar y colaborar en este equipo de trabajo para que las diferentes líneas avancen hacia el objetivo de protección de los dispositivos.

La GSMA, junto con la industria móvil, ha diseñado una gama de recursos que puedan dar una orientación en Seguridad a las empresas **con el desafío de asegurar el futuro conectado.** Se ha elaborado una guía con las directrices de seguridad. Basándose en esta amplia experiencia en seguridad, la GSMA, junto con la industria móvil, ha creado un conjunto de **Pautas de Seguridad para IoT**, respaldadas por un esquema de evaluación de seguridad IoT, para proporcionar un enfoque probado y robusto para disponer de seguridad de extremo a extremo. Esta guía es gratuita y está disponible en internet:
https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

¿Qué perfiles se necesitan en el sector de la seguridad de la información?

Actualmente **existe una carencia de perfiles en el ámbito de la Ciberseguridad,** en todas sus ramas. El aumento de ciberataques, y la proliferación de nuevas amenazas con un grado de sofisticación elevado y creciente, conducen a la necesidad de incorporar profesionales expertos en Ciberseguridad para cubrir puestos de trabajo especializados en distintos tipos de organizaciones.

Los perfiles más demandados son los que tienen conocimientos técnicos o provienen de carreras técnicas. **La característica más difícil de encontrar es la experiencia**, el número de profesionales con años de experiencia en el sector es muy reducido.

¿Qué le diría a una persona joven que, por desconocimiento, no se plantea una trayectoria laboral en el sector de la Ciberseguridad?, ¿qué experiencia se requiere?

Si le gusta el tema, este es su momento. Si lo desconoce, lo primero es **acercarse a las diferentes asociaciones** que hay en todo el territorio nacional que trabajan en la materia de Ciberseguridad, ellas le podrán asesorar e iniciar en este sector. Además de **asistir a los diferentes congresos que se celebran durante todo el año**, seguro que hay uno cerca de su lugar de residencia. De esa forma podrá conocer más en detalle este sector y plantearse una trayectoria profesional en él.

Sobre todo se requieren **personas con conocimientos técnicos y mucha creatividad**. En Ciberseguridad,

What profiles are currently needed in the information security sector?

There is a shortage of profiles in the field of cybersecurity, in all its branches. Because of the rise in cyberattacks and the proliferation of highly and ever more sophisticated new threats, qualified expert professionals are needed to fill specialized positions in cybersecurity in different types of organizations.

The most in-demand profiles are those with technical expertise or studies. **The most difficult to find characteristic is experience**; the number of professionals with years of experience is very small.

What would you say to a young person who, through lack of awareness, does not consider a career in the cybersecurity sector? What experience is required?

If they like the subject, this is their moment. If they are unfamiliar with it, the first thing to do is **to consult the different associations** in Spain that work in the area of cybersecurity, which can give advice and introduce them to the sector. **Different conferences are held throughout the year**, too, and there is sure to be one close to where they live. This will allow them to get to know this sector better and to consider starting a professional career in it.

What is especially required is **people with technical knowledge and a lot of creativity**. Those of us working **in cybersecurity are forced to be creative,** it is the best way to find solutions to the complex problems in our sector. Being able to think laterally and "out of the box" is very important. Finding professionals with experience in cybersecurity is difficult, so **any professional who is an expert in systems and communications and is creative can join this sector.** We will take care of training them so they learn the peculiarities of cybersecurity in the environments they are already familiar with.

estamos obligados a ser creativos, es la mejor forma de poder encontrar soluciones a los problemas complejos de nuestro sector. Las habilidades de pensamiento lateral y pensamiento "out of the box" resultan muy importantes.

Es difícil encontrar profesionales con experiencia en Ciberseguridad, por lo que **cualquier profesional que sea experto en sistemas y comunicaciones, con las habilidades de creatividad, puede unirse a este sector,** nosotros nos encargamos de formarle para que conozca las particularidades de la Ciberseguridad en entornos que ya conoce.

¿Cuál es su visión sobre el estado de la ciberseguridad empresarial en 2018?, ¿cómo cree que evolucionará en un futuro próximo?

Se encuentra en un estado inicial. Si lo comparamos con otros sectores, **los sistemas industriales carecían de las medidas de seguridad necesarias, que sí se estaban aplicando a los sistemas informáticos.** El principal riesgo viene a interconectarlos a las redes internas de las empresas o incluso a internet. Afortunadamente es un sector en el que se empezó a trabajar hace unos años.

En ese aspecto **destacar la labor del INCIBE** con la

What is your opinion about the state of corporate cybersecurity in 2018? How do you think it will evolve in the near future?

It is in the initial stages. Compared with other sectors, **industrial systems did not have the necessary security measures that computer systems did have incorporated into them**. The main risk lies in interconnecting them with the internal networks of businesses or even with the Internet. Fortunately, the sector started paying attention to cybersecurity a few years ago.

The INCIBE has done a great job here with the creation of the **National Network of Industrial Laboratories**, a platform that brings together industrial laboratories that have the capacity to experiment and research solutions that increase security in our national industrial infrastructures.

We have joined this year, contributing a complementary, differentiating factor: **protecting the communications and perimeters of businesses**, thereby providing a protection that, together with internal protection measures, raises security levels. **Things are going to be evolving very quickly** because companies will start adopting these security and protection measures, which means they will be needing products and services that protect them against Internet threats. **The next few years will see constant evolution** taking place, especially with IoT devices entering industrial processes as well as the daily life of any corporate process: air conditioning, cleaning, logistics, etc.

Are companies really aware of the importance of protecting their corporate information? Does this field receive sufficient attention?

Nowadays it does. **All companies are aware of the importance of the information they possess** and that any threat that might affect that information is a risk for the organization. **Especially when we are talking about personal data,** which are the subject of new legislation that is coming into effect this very month.

The challenge now is to make the change to cybersecurity: **it is no longer just about protecting information, but also the interconnected device containing it.** The threats we are now facing do not so much attempt to seize control of information as they do of devices, after which they may obtain the information or compromise other devices. This is the goal of cybercriminals who want to monetize their attacks with or without access to information.

What essential cybersecurity advice would you give to companies?

creación de la **Red de Laboratorios industriales**, es una plataforma que reúne a los laboratorios industriales con capacidad para la experimentación e investigación de soluciones que aumenten los niveles de seguridad de las infraestructuras industriales nacionales.

Nosotros nos hemos incorporado este año aportando un factor complementario y diferencial, **proteger las comunicaciones y el perímetro de las empresas** dando una protección que, unida a las medidas de protección internas, aumentan los niveles de seguridad. **La evolución va a ser muy rápida**, ya que las empresas van a comenzar a adoptar estas medidas de seguridad y protección, por lo que van a necesitar productos y servicios que les protejan de las amenazas de internet. **Los próximos años van a ser de evolución constante**, sobre todo con la aparición de los dispositivos IoT tanto dentro de los procesos industriales como dentro de la vida diaria de cualquier proceso de la compañía: climatización, limpieza, logística, etc.

¿Las empresas están concienciadas de la importancia de la seguridad de su información corporativa?, ¿se le presta suficiente atención a este campo?

Actualmente sí, **todas son conscientes del valor de la información que posee** y que cualquier amenaza que pueda afectar a la misma supone un riesgo para la organización. **En especial si hablamos de datos personales**, para lo cual hay dedicada una legislación completa que entra en vigor este mes.

El reto es el cambio a la ciberseguridad: **ya no es solo proteger la información sino el dispositivo que la contiene y que está interconectado.** Las amenazas a las que nos enfrentamos tratan de tomar el control del dispositivo, no de la información, que posteriormente nos pueden conducir a la obtención de la información o a comprometer otro dispositivo, esto lo tienen en cuenta los ciberdelincuentes que ven la forma de monetizar sus ataques con o sin acceso a información.

¿Qué consejo imprescindible de Ciberseguridad le daría a una empresa?

Que **contrate a un experto** o **contacte con una empresa especialidad** para que le ayude a proteger sus activos. También que **elabore un plan de protección** que le garantice un nivel de seguridad que le proteja de las amenazas que están surgiendo. Se trata de una inversión para evitar que su negocio pueda sufrir un ataque que afecte a su continuidad.

Suele decirse que la información es poder, ¿es la información el capital más importante de una empresa?

Es uno de los más importantes, dependiendo del tipo

To hire an expert or contact a specialized company to help them protect their assets. Also **to draw up protection plans** that guarantee a level of security that protects them against the threats that are emerging. It is an investment on the part of companies meant to avoid an attack that may affect their continuity.

It is often said that knowledge is power. Is information a company's most important capital?

It is amongst the most important ones, depending on the company's type and sector. **With the emergence of "Big Data", data have become the new raw material**; they are bought, sold, processed and transformed, and they generate services around them, a whole new industry.

Many companies have realized they possess a valuable raw material. Starting from this, they have embarked on different paths, some quickly monetizing information by selling it, others turning it into a revenue-generating service without getting rid of their asset.

What are the main threats and challenges facing companies regarding the security of their corporate information?

The principal threats stem from a **company's exposure to the outside**: its communications, email correspondence and Internet browsing are the route of entry from the outside.

Currently, the main threats are malware (including ransomware), attacks on web applications, phishing, spam, denial of service, botnets, etc. All these threats **may put the continuity of the company's activity at risk, causing economic losses.**

Companies must develop cyberintelligence capabilities to understand the threat environment they are exposed to and thus anticipate the corresponding

o sector de empresa. **Con la aparición del "Big Data", el dato se ha convertido en la nueva materia prima**, se compra, se vende, se procesa, se transforma y se generan servicios alrededor, toda una nueva industria. Muchas empresas se han dado cuenta de que poseen una materia prima que tiene valor. A partir de ahí cada uno ha seguido un camino distinto, los primeros la han monetizado rápidamente con su venta, otros la han convertido en un servicio que les da ingresos sin desprenderse de su activo.

¿Cuáles son las principales amenazas que pueden sufrir las empresas y cuáles son los retos principales de las compañías en materia de seguridad de su información corporativa?

Las principales amenazas vienen derivadas de **la exposición de la empresa al exterior**: el correo electrónico, sus comunicaciones, la navegación por internet, son la vía de entrada desde el exterior.

Actualmente las principales amenazas son el malware (incluido el Ransomware), ataques a aplicaciones web, phising, spam, denegación de servicio, botnes, etc. Todas estas amenazas **pueden poner en riesgo la continuidad de la actividad, provocando pérdidas económicas.**

Las compañías deben desarrollar capacidades de ciberinteligencia para conocer el entorno de amenazas al que están expuestas y anticipar, así, los riesgos correspondientes. **El análisis de riesgo debe ser una herramienta fundamental en todos los procesos de negocio**. Se debe realizar formación y concienciación de los empleados en Ciberseguridad. Se debe **definir un plan de seguridad** que permita proteger sus comunicaciones, su equipos informáticos, el correo, su navegación en internet y mitigar los ataques de denegación de servicio.

¿Algún sistema es invulnerable?

Al igual que en el mundo físico, no hay sistema invulnerable, **todo depende del nivel de especialización del atacante y los medios con los que cuenta.** Lo que tenemos que hacer **es subir el nivel de protección de nuestros activos** en función de las amenazas a las que estamos expuestos y disponer de un sistema de detección en el caso que estos sean superados.

Con respecto al escándalo Facebook, ¿le preocupa esa fuga de información personal?

Lo que me preocupa es **la facilidad con que la gente le da sus datos a estas empresas**. No tendrían esos datos si la gente no se los diera. Inicialmente tenemos **una**

risks. **Risk analysis must be an essential tool in all business processes**. Employees must receive training in cybersecurity and be made aware of its importance. **A security plan must be designed** that makes it possible to protect communications, computer systems, email correspondence and web browsing, in addition to mitigating denial-of-service attacks.

Is there such a thing as an invulnerable system?

As in the physical world, no system is invulnerable. **Everything depends on the attacker's level of specialization and the means at their disposal.** What we have to do is **to raise the level of protection of our assets** based on the threats facing us and have a detection system in place in case it is overcome.

Regarding the Facebook scandal, are you worried about this personal information leak?

What worries me is **the ease with which people give their data to these companies**. If people didn't give them their data, these companies wouldn't have them. So at the source of everything lies this **voluntary leak of information** where people give information to these companies that offer their services for free.

We need to make society aware of this situation and explain that **when something is free, you are the product.** Also, this creates problems for the rest of companies that do make responsible use of information.

When a society becomes more and more interconnected, does that make it more vulnerable?

Obviously, t**he definition of perimeter security has been lost,** because today all kinds of networks and systems are interconnected.

On the one hand, **this is good and necessary for improving users' communication** and information-access

si la gente no se los diera. Inicialmente tenemos **una fuga voluntaria** de la información de las personas hacia estas empresas que ofrecen sus servicios gratuitos.

Tenemos que concienciar a la sociedad de esta situación y explicar que **cuando algo es gratis el producto eres tú.** El problema lo genera al resto de empresas que hacen un uso responsable de la información.

El hecho de que una sociedad cada vez esté más interconectada, ¿la hace más vulnerable?

Obviamente, **se ha perdido la definición de perímetro de protección**, ya que hoy están interconectados todo tipo de redes y sistemas.

Por un lado, **esto es bueno y necesario para mejorar las capacidades de comunicación y acceso a la información por parte de los usuarios** y es un servicio que estamos potenciando.

Sin embargo, por otro lado, **se están interconectando sistemas que no deberían estar accesibles desde otros puntos**, solo a los sistemas o personas responsables de los mismos.

Deberíamos plantearnos la idea de **disponer de redes independientes para procesos diferentes**, segregar en función de los servicios y necesidades.

El concepto Internet of Things está cada vez más latente en la sociedad. ¿Nuestros datos corren peligro?, ¿cómo será nuestra vida cuando todo esté conectado a Internet?

A medida que vamos conectando más dispositivos en nuestro hogar vamos aumentando el nivel de riesgo, principalmente **porque desconocemos las capacidades y riesgos asociados a estos dispositivos.** Por otro lado está la **privacidad**, cómo las empresas hacen un uso responsable de los datos que pueden recoger de nosotros.

Para esto estamos impulsando la **creación y aplicación de certificados de seguridad de productos y servicios**, sobre todo los IoT, que garanticen al usuario un nivel de seguridad de forma que no se tenga que preocupar cuando instale uno de ellos, es lo que estamos haciendo en la GSMA, **diseñar para que el futuro sea seguro**. Va a ser un factor diferencial.

El futuro se presenta muy interesante, con nuevos servicios y capacidades, que nos facilitarán la vida. Y **todos estos dispositivos estarán interconectados de forma segura**. Es en lo que estamos trabajando ya para que esté disponible a nuestros clientes cuando lo necesiten.

capabilities, and it is a service that we are promoting.

On the other hand, however, **systems are being connected that should not be accessible from other points** but only from the systems and by the people responsible for them.

We should consider the idea of **having independent networks for different processes,** of segregation based on services and needs.

The concept of the Internet of Things is becoming ever more deeply embedded in our society. Are our data at risk? What will our lives be like when everything is connected to the Internet?

As we connect an increasing number of devices in our homes, we also raise the risk level, mainly **because we are unaware of the capabilities and risks associated with these devices.** Then there is the issue of **privacy**, of how companies make responsible use of the data they gather about us.

To this end we are advocating **the creation and application of security certificates for products and services**, especially IoT, that guarantee users a level of security sufficiently high so they do not have to worry when installing one of these devices. This is what we are doing in the GSMA, **designing to make the future safe**. This is going to be a differentiating factor.

The future looks very interesting, with new services and capabilities that will make life easier for us. And **all these devices will be safely interconnected.** We are working on this already so that when our clients need it, it is available to them.

Seguridad y conectividad para una comunicación global: net4machines, la VPN propia de Nayar Systems

Security and connectivity for global communication: net4machines, Nayar Systems' own VPN

ALEXIS NADAL | Vivimos en un mundo cada vez más conectado y ello nos hace **más vulnerables a posibles intrusiones maliciosas**. En Nayar Systems, a la vez que comenzábamos a conectar a Internet dispositivos instalados en un ascensor, surgió la necesidad de que dicha conexión fuera lo más segura posible. No cabía duda, **debíamos utilizar una VPN** (Virtual Private Network).

Las VPN nacieron en 1995, debido a la necesidad de las empresas de **conectar bidireccionalmente y de forma segura distintas sedes dispersas geográficamente**. Hasta ese momento, la única solución segura era invertir en costosas infraestructuras punto a punto, por lo que la mayor parte de las sedes funcionaban de manera aislada.

Una VPN soluciona la conexión de forma segura utilizando Internet, por lo que evita tener que desplegar esas costosas infraestructuras punto a punto. Básicamente consiste en crear **una red local**, pero en vez de usar cables de datos, se utilizan **túneles informáticos cifrados a través de Internet**.

El usuario no percibe que una impresora pueda estar ubicada a cientos de kilómetros de distancia. Con los permisos de red correctos podrá enviar una impresión como a cualquier otra impresora de su oficina. Otra aplicación muy extendida consiste en que varios usuarios

ALEXIS NADAL | We live in an increasingly connected world and that makes us **more vulnerable to possible malicious intrusions**. At the time we started connecting to the Internet devices installed in lifts, at Nayar Systems we discovered the need of making that connection as secure as possible. Without a doubt, **we had to use a VPN** (Virtual Private Network).

VPNs were born in 1995, due to the companies' need of **connecting bidirectionally and securely different offices geographically scattered.** Until then, the only secure solution was to invest in expensive infrastructures point to point, so most of the offices were working in isolation.

A VPN solves the secure connection by using the Internet, thus avoiding having to deploy those expensive infrastructures point to point. It basically consists in creating a **local network**, but instead of using data cables, it uses **encrypted computer tunnels through the Internet.**

The users do not notice that a printer can be located hundreds of kilometres away. With the right network privileges, they can send a printout as they would to a printer in their office. Another widely used application is that many users can play online from different geographical points.

puedan estar jugando online desde diversos puntos geográficos.

Por todo lo que estoy indicando, es obvio que en Nayar Systems necesitábamos una VPN para poder **conectar de forma segura las pantallas de Advertisim a nuestros servidores**. En el mercado teníamos dos opciones:

1. **VPN proporcionada por un operador móvil.** Los operadores de telecomunicaciones móviles pueden proporcionar una VPN que únicamente funciona con sus tarjetas SIM. Como requisitos, se precisa una interconexión y una configuración especial por cada uno de los operadores. Incluso con algunos operadores se puede complicar teniendo que desplegar un server Radius.

2. **VPN basadas en software.** Una opción sencilla que requiere que en la parte del dispositivo remoto se pueda ejecutar un software o configuración. Existen muchas opciones en el mercado, pero destaca OpenVPN, una herramienta de conectividad basada en software libre.

Nuestra principal necesidad era poder conectarnos al dispositivo remoto a través de Internet desde cualquier operador de telecomunicaciones del mundo, independientemente de que se tratara de ADSL, cable, 4G, satélite, WiMAX, etc. La primera de las opciones no cumplía con este requisito, puesto que se deviene imposible tener una configuración e interconexión con todos los operadores mundiales, por lo que la única alternativa sería **utilizar un operador móvil global.** Esta última es una opción demasiado cara hoy en día y más para manejar archivos multimedia; además, la complicación aumenta por tener que manejar con el mismo operador distintas tarifas según la zona.

Una VPN basada en software era nuestra única alternativa, pues puede funcionar prácticamente con cualquier operador de telecomunicaciones del mundo (salvo puntuales excepciones legislativas locales)

For all I am pointing out, it is obvious that at Nayar Systems we needed a VPN to be able to securely **connect Advertisim screens to our servers**. There were two options in the market:

1. **VPN provided by a mobile operator.** Mobile telecommunications operators can provide a VPN which only works with their SIM cards. Interconnection and a special configuration are required for each of the operators. Even with some operators it can get harder by having to deploy a Radius server.

2. **VPN based on software.** A simple option that requires the execution of a software or configuration in the remote device. There are many options in the market, but OpenVPN stands out. It is a connectivity tool based on open source software.

Our main necessity was being able to connect with the remote device through the Internet from any telecommunications operator in the world, regardless of whether it was ADSL, cable, 4G, satellite, WiMAX, etc. The first option did not meet this requirement, since it is impossible to have a configuration and an interconnection with all of the world's operators, so the only choice was **to use a global mobile operator.** This option is too expensive nowadays, especially to manage multimedia files; furthermore, it gets more complicated by having to deal with different rates depending on the area with the same operator.

A software-based VPN was our only option, since it can work practically with any telecommunications operator in the world (with unusual local legislative exceptions) and Advertisim has enough power as to being able to execute the VPN software.

At Nayar Systems we started testing tons of VPN services from the market. All of them carried out their task, but **the differences in data consumption were huge** and at the same time very worrying for us, because **the one with the least data consumption was too large to be in a M2M SIM card.**

The thing is that **none of the VPN services had been designed to work with machines.** As I have already mentioned, the main applications serve to connect offices, play online or even breach the Chinese firewall. None of these cases has worrying data consumption, considering that they use broadband connections with practically unlimited rates.

In the industrial world, machines generally send very little and repetitive data. The problem lays in the fact that VPNs encapsulate those data in complex structures where just the head of the message is usually two hundred and fifty times larger than the data itself.

y Advertisim tiene la suficiente potencia como para poder ejecutar el software de VPN.

En Nayar Systems comenzamos a probar multitud de servicios VPN existentes en el mercado. Todos cumplían con su cometido, pero **las diferencias en el consumo de datos eran enormes** y a la vez muy preocupante para nosotros, porque **el que menos consumo de datos tenía era demasiado para estar detrás de una tarjeta SIM M2M.**

La causa es que **ninguno de los servicios VPN se había diseñado para trabajar con máquinas.** Como ya he comentado, las principales aplicaciones son para conectar oficinas, jugar online e incluso saltarse el Cortafuegos Chino. En ninguno de esos casos el consumo de datos es preocupante, dado que se utilizan conexiones de banda ancha con tarifas prácticamente ilimitadas.

"Una VPN basada en software era nuestra única alternativa, pues puede funcionar prácticamente con cualquier operador de telecomunicaciones del mundo"

En general, en el mundo industrial las máquinas suelen enviar muy pocos datos y muy repetitivos. El problema radica en que las VPN encapsulan esos datos en complejas estructuras donde únicamente la cabecera del mensaje suele ser doscientas cincuenta veces más pesada que el propio dato.

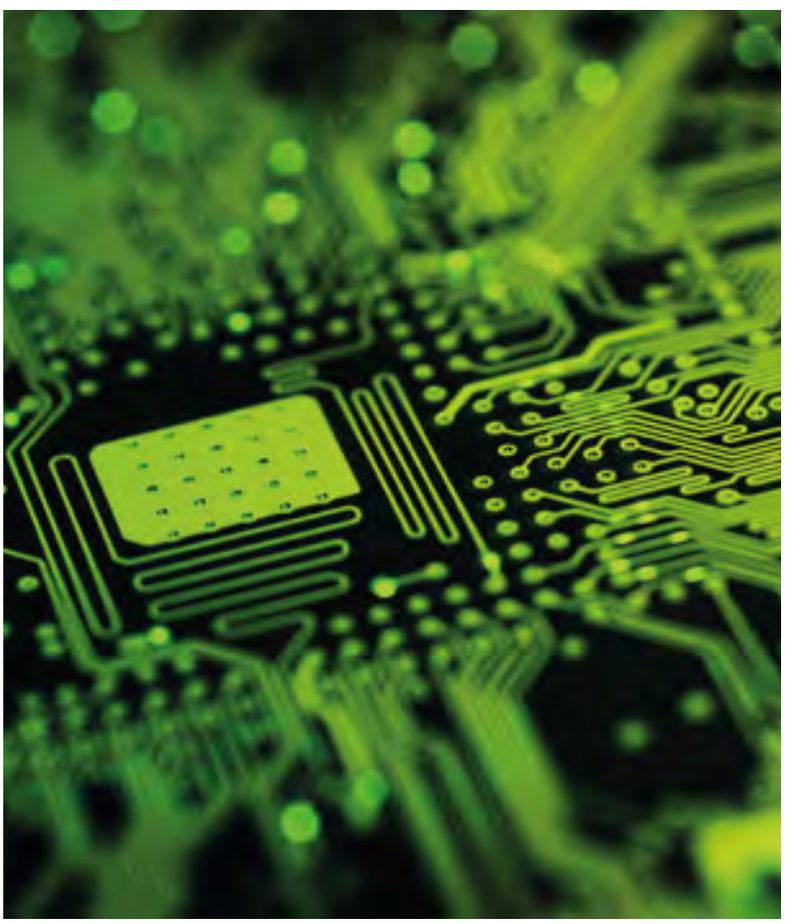
Tras esta prospección del mercado concluimos que **no existían VPN diseñadas y especializadas en el mundo M2M, que minimizaran el consumo de datos enviados a Internet.**

En ese momento advertimos la necesidad y la oportunidad de desarrollar **el primer servicio de VPN por software diseñado y desarrollado para funcionar en entornos de IoT industrial**. Previamente, en un taller de innovación se detectaron aspectos de mejora técnicos sobre las VPN tradicionales y tras un exhaustivo análisis se decidió mejorar los siguientes aspectos:

- **Bajo consumo de RAM por conexión**, de forma que la escalabilidad y estabilidad de los servidores se simplifica enormemente.
- **Compresión de datos en streaming**, dado que los datos enviados por las máquinas son muy repetitivos, conseguimos rangos de compresión muy superiores que en la compresión por paquetes tradicional.
- **Creación de una capa superior a la configuración de red, que permite organizar los dispositivos en dominios y subdominios**. Esta capa, además de facilitar el uso frente a configuraciones de red con IP y máscaras de red, permite las siguientes ventajas:

After this market research we concluded that **there were no VPNs designed and specialized in the M2M world, which minimised the consumption of data sent to the Internet.**

"A software-based VPN was our only option, since it can work practically with any telecommunications operator in the world"



At that moment we observed the need and the opportunity to develop **the first VPN service through software designed and developed to work in industrial IoT environments.** Previously, in an innovation workshop, technical improvement areas over traditional VPNs were detected and after a thorough analysis it was decided to improve the following areas:

- **Low consumption of RAM per connection**, so that the servers' scalability and stability is tremendously simplified.
- **Streaming data compression**, as the data sent by machines are very repetitive, we achieve compression ranges much higher than those of traditional compression in packages.
- **Creation of a layer over the network configuration that allows for organizing devices in domains and**

- **No es necesario reservar rangos de IPs para segmentar usuarios**. Utilizando los dominios y los subdominios, las IPs se pueden utilizar consecutivamente y pertenecer a usuarios distintos.
- **Ejecución de las reglas de visibilidad en la nube en vez de en el dispositivo remoto**. Especificando permisos de acceso y visibilidad en la nube aumenta considerablemente la seguridad en la red. Si un hacker malicioso pudiera capturar físicamente un dispositivo remoto y descifrara el usuario y la contraseña, podría hacerse pasar por dicho dispositivo y acceder con total libertad al resto de la VPN. Dado que las reglas de visibilidad están en la nube, se puede ejecutar una simple regla para que un dispositivo no pueda ver a otros dispositivos, por lo que aunque el hacker consiguiera descifrar el usuario y la contraseña, a pesar de hacerse pasar por el dispositivo, se le negaría el acceso.

"Concluimos que no existían VPN diseñadas y especializadas en el mundo M2M"

El servicio se completa con una plataforma web que:

- **Gestiona de forma ágil y sencilla las cuentas**, usuarios, dominios, estructura, permisos, compresión de datos, etc.
- **Monitoriza el estado de los dispositivos en tiempo real** como online/offline, tráfico generado, nivel de cobertura, número de conexiones, etc.
- **Establece alertas con avisos vía mail o SMS** que informen ante eventos inesperados como desconexiones, excesivo uso de red, etc.
- **Accede a los dispositivos sin tener que recordar su IP**, ya que todos reciben un nombre de host mapeado en Internet en nuestros DNSs.
- **Permite organizar los dispositivos en dominios y subdominios**, y especificar permisos de acceso y visibilidad para una total seguridad en la red.
- **Ofrece estadísticas horarias**, **diarias, mensuales y anuales** de cada dispositivo, relativas a los datos consumidos y cantidad de conexiones.

De este modo nace **net4machines**, la VPN propia de Nayar Systems, que lleva **más de cinco años conectando miles de dispositivos de forma simultánea en los cinco continentes**, con una alta disponibilidad, estabilidad y rendimiento; haciendo de lo ordinario algo extraordinario.

subdomains. This layer, apart from facilitating the use in IP network configurations and netmasks, offers the following advantages:

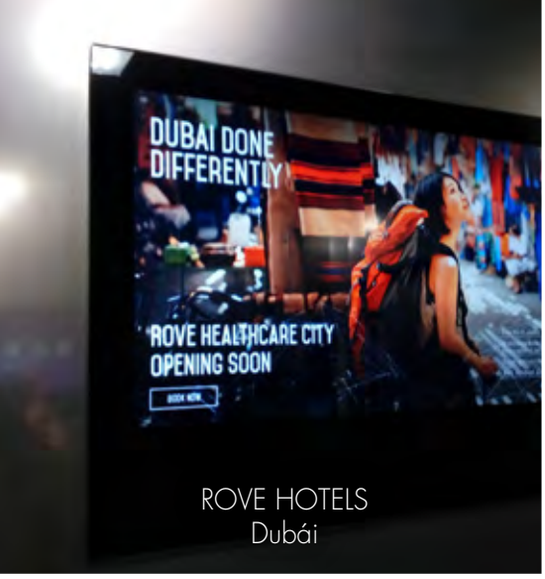
- **It is not necessary to reserve IP ranges to divide users into segments.** By using domains and subdomains, IPs can be used consecutively and belong to different users.
- **Visibility rules can be executed in the cloud instead of the remote device.** Specifying access and visibility privileges in the cloud considerably increases network security. If a malicious hacker could physically take a remote device and decrypt the user and password, he could pretend to be that device and with total freedom gain access to the rest of the VPN. Since visibility rules are in the cloud, a simple rule can be executed so that a device cannot see other devices. Thus, although the hacker could decrypt the user and password, he would not gain access even when pretending to be the device.

"We concluded that there were no VPNs designed and specialized in the M2M world"

The service is completed with a web platform that:

- **Manages, in a flexible and easy way, the accounts**, users, domains, structure, privileges, data compression, etc.
- **Monitors the devices' real-time state** such as online/offline, traffic generated, level of coverage, number of connections, etc.
- **Sets alerts with mail or SMS** warnings that report unexpected events such as deactivations, excessive network use, etc.
- **Gains access to devices without having to remember its IP**, since all of them receive an Internet mapped host name in our DNSs.
- **Allows for organizing devices in domains and subdomains**, and for specifying access and visibility privileges for a complete network security.
- **Offers hourly, daily, monthly and yearly statistics** for each device, relative to the consumed data and the amount of connections.

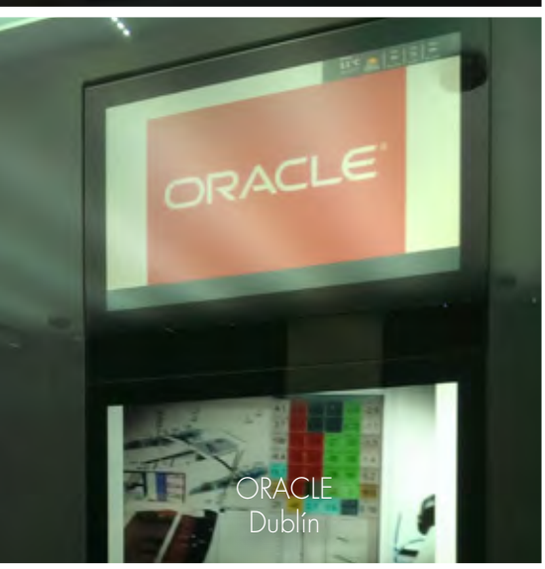
This is how **net4machines** is born. It is Nayar Systems' own VPN, **which has been simultaneously connecting thousands of devices in the five continents for more than five years**, with high availability, stability and performance; making the ordinary extraordinary.



ROVE HOTELS
Dubái

TORRE PWC
Madrid

HOTEL TRYP VALENCIA AZAFATA 4*
Valencia



ORACLE
Dublín

HOTEL MARRIOT AUDITORIUM
Madrid

HOTEL EMPERADOR 4*
Madrid

ONLY YOU HOTEL ATOCHA
Madrid

EDIFICIO
San Sebastián

HOTEL ROOM MATE PAU
Barcelona

HOTEL INDIGO
Madrid

EDIFICIO
San Sebastián

ESPAITEC
Castellón

HOTEL ROOM MATE ÓSCAR
Madrid

HOTEL NEPTUNO 4*
Valencia

“Los retos de las compañías irán relacionados con la dependencia tecnológica y la madurez en ciberseguridad”

“The challenges for companies will relate to their level of technological dependence and maturity in terms of cybersecurity”

¿Cuáles son las principales áreas que se trabajan desde INCIBE en el área de ciberseguridad?

El **Instituto Nacional de Ciberseguridad** es una entidad pública adscrita al Ministerio de Energía Turismo y Agenda Digital a través de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital. Su misión fundamental es **prestar servicios públicos de ciberseguridad a los ciudadanos y al sector privado en España**, con atención especial a los **operadores privados de infraestructuras críticas** gracias a un convenio de colaboración con el Ministerio del Interior, a través de su Centro Nacional para la Protección de las Infraestructuras y la Ciberseguridad (CNPIC) y fruto del cual se constituye un CERT (Centro de Respuesta ante Incidentes).

El primer enfoque de nuestro servicio público se basa en la **prevención**, en **concienciar a ciudadanos y empresas sobre el uso seguro de las tecnologías**, humanizando la ciberseguridad, es decir, acercándola cada vez más a nuestros ciudadanos y pymes. En segundo lugar, buscamos la capacidad de **detectar de forma proactiva ciberincidentes o ciberataques** que sucedan en España y que afecten a sus ciudadanos y a su sector privado para detectarlos, analizarlos y ponerlos en conocimiento de los afectados.

What are the main areas INCIBE works on in the field of cybersecurity?

The **Spanish National Cybersecurity Institute** is a public entity attached to the Ministry of Energy, Tourism and the Digital Agenda through the Secretary of State for the Information Society and the Digital Agenda. Its core mission is **to provide public cybersecurity services to the citizens and the private sector in Spain**, with special attention to **private operators of critical infrastructures** thanks to a collaboration agreement with the Ministry of Home Affairs through its National Centre for the Protection of Infrastructures and Cybersecurity (CNPIC), agreement that led to the creation of a CERT (Computer Emergency Response Team).

The first focus of our public service is based on **prevention**, on **teaching people and companies about the safe use of technologies** by humanizing cybersecurity, i.e., by bringing it closer to our citizens and SMEs. Secondly, we work to develop the capability **to proactively detect cyberincidents or cyberattacks** taking place in Spain and affecting its citizens and private sector in order to detect them, analyse them and inform the people affected by them.

¿Qué tipo de actuaciones lidera INCIBE en materia de ciberseguridad?

INCIBE lidera actuaciones dirigidas a ciudadanos, empresas y menores. Se centra en el aspecto preventivo ofreciendo **herramientas gratuitas**, **formación online y charlas en centros educativos**, entre otras. También presta servicios de **soporte y ayuda** ante un incidente de ciberseguridad, a través de CERTSI.

Además, **fomenta y desarrolla la ciberseguridad**, tanto a nivel nacional, como internacional. Para ello, se coordina con múltiples organismos como la Organización de Estados Americanos (OEA) y con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

INCIBE apoya el **emprendimiento y busca el talento** con múltiples iniciativas como **Ciberemprende**, con el objetivo de crear una comunidad de emprendedores en ciberseguridad. Organiza eventos como **ENISE** (Encuentro Internacional de Seguridad de la información), **Cybersecurity Summer BootCamp** (iniciativa internacional de capacitación en Ciberseguridad para Técnicos, Fuerzas y Cuerpos de Seguridad del Estado y Policy Makers) y **CyberCamp** (ayudar a la generación del talento en ciberseguridad).

¿Cómo luchan contra el cibercrimen? ¿Qué tipo de ayudas tecnológicas proporcionan para luchar contra el ciberdelito?

Desde INCIBE podemos destacar la colaboración con nuestras **Fuerzas y Cuerpos de Seguridad del Estado** en la lucha contra el ciberdelito apoyándoles en el desarrollo de tecnologías.

¿Cómo es la relación de INCIBE con las empresas?

Desde el año 2014, INCIBE comenzó a desarrollar servicios de ciberseguridad especialmente diseñados para empresas (**https://www.incibe.es/protege-tu-empresa**), aunque desde el 2008 viene desarrollando iniciativas para mejorar la ciberseguridad de este colectivo. En este sentido, INCIBE tiene una relación de coordinación y cooperación con las empresas estratégicas en lo relativo a la información de amenazas específicas y respuesta a incidentes a través del CERT.

Además, gracias a la creación el pasado 2017 del **servicio de respuesta a incidentes para pymes**, cada vez son más las que nos notifican aquellos relativos a ciberseguridad que detectan, aunque llevan años haciendo uso de los servicios del CERT de INCIBE. También desde el Instituto estamos a disposición de las compañías para ofrecerles **acciones de formación y concienciación** de cara a mejorar la seguridad, sobre todo de los empleados, con el objetivo de reducir el impacto de los problemas de ciberseguridad que

What actions does INCIBE perform in the field of cybersecurity?

INCIBE performs actions for citizens, companies, and minors, focusing on prevention and offering **free tools, online training, and talks in schools**, among others. Through CERTSI, it also provides **support and assistance** for those affected by cybersecurity incidents.

In addition, **it promotes and develops cybersecurity** both in Spain and abroad. It does this in coordination with numerous organizations, including the State security forces and law enforcement agencies, and the Organization of American States (OAS).

INCIBE supports **entrepreneurship and scouts talent** through many initiatives, like **Ciberemprende**, with the aim of creating a community of cybersecurity entrepreneurs. It organizes events such as **ENISE** (International Meeting on Information Security), **Cybersecurity Summer BootCamp** (an international cybersecurity training initiative for CERT technicians, State security forces and law enforcement personnel, and policy makers) and **CyberCamp** (helping create cybersecurity talent).

How do you fight cybercrime? What type of technological help do you provide in the fight against cyberdelinquency?

One prominent thing we do at INCIBE is to collaborate with **Spanish State security forces** and law enforcement agencies in the fight against cybercrime by supporting them in the development of technologies.

How is INCIBE's relationship with companies?

During 2014, INCIBE started developing cybersecurity services specially designed for companies (**https://www.incibe.es/en/protect-your-business**), although it had already been working on initiatives to improve cybersecurity for this collective since 2008. In this regard, INCIBE coordinates and works together with strategic companies in matters of threat reporting and incident response through the CERT.

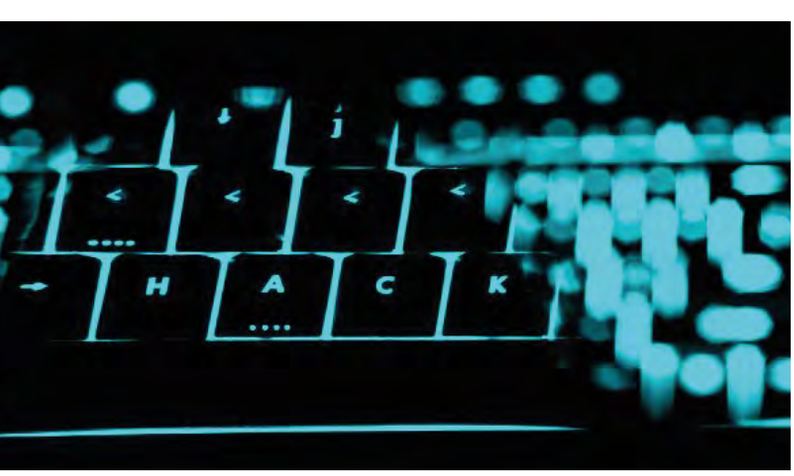
Furthermore, thanks to the creation in 2017 of the **incident-response service for SMEs**, more and more of them are reporting cybersecurity incidents to us, although they have been using the services of INCIBE's CERT for years. The Institute also offers companies **training and awareness-raising activities** aimed at improving security, especially for their employees, in order to reduce the impact of the cybersecurity problems they sometimes generate. Also worthy of note are our relations with the **Chambers of Commerce and the main business associations**, which disseminate information about our services and contents.

estos podrían generar. Mencionar que además estamos en contacto con las **Cámaras de Comercio y Asociaciones de Empresarios** más importantes para que faciliten la divulgación de nuestros servicios y contenidos.

¿Qué tipo de incidentes en materia de seguridad de la información suelen encontrarse más a menudo?

El mayor problema radica en aquellas organizaciones cuyos empleados **no estén concienciados en ciberseguridad** o tengan un perfil de "insider" (empleado descontento). Serán estos, los que con sus acciones probablemente puedan generar la mayor cantidad de incidentes, bien de **manera inconsciente** (ejecutando algún archivo, accediendo a algún enlace, etc) o **de manera intencionada** (robando información o haciéndola pública). No hay que olvidar los sistemas y las tecnologías que también suelen ser un objetivo de los ciberdelincuentes. Eludir las actualizaciones o mantener las configuraciones por defecto suele conllevar numerosos problemas a la larga.

Además, el año 2017 será recordado por un tipo de malware, **el ransomware** que infecta los equipos de empresas, sus servidores web, etc. Este malware **toma el control de los equipos y cifra**, «secuestra», l**a información, pidiendo un rescate, a menudo en bitcoins, a cambio de liberarla**. La gran difusión que se hizo a través de los medios de comunicación del ataque de WannaCry y Petya ha servido para que muchas empresas y usuarios tomen conciencia en relación a los riesgos del uso de las tecnologías.



¿Las empresas están realmente concienciadas de la importancia de la seguridad de su información corporativa? ¿Se le presta suficiente atención a este campo?

Cada vez más organizaciones son conscientes de los riesgos a los que se exponen y actúan para no verse afectadas por incidentes de ciberseguridad. Se trabaja cada vez más en la **gestión del riesgo**,

What type of incidents relating to information security do you encounter most often?

The biggest problems usually come from organizations with employees who **are not aware of cybersecurity** or are disgruntled ("insiders"). Through their actions, they will probably be responsible for generating the highest number of incidents, either **unconsciously** (by running a file, following a link, etc.) **or deliberately** (by stealing information or making it public). Computer systems and technologies are also often targeted by cybercriminals. Not installing updates or maintaining default configurations usually causes many problems in the long run.

Moreover, the year 2017 will be remembered for a type of malware called **ransomware**, which infects companies' terminals, web servers, etc. This type of malware **takes over computers and encrypts or "hijacks" information, demanding a ransom, often in bitcoins, in exchange for decrypting the information.** The extensive media coverage of the WannaCry and Petya attacks helped making many companies and users aware of the risks associated with the use of technologies.

Are companies really aware of the importance of protecting their corporate information? Does this field receive sufficient attention?

More and more organizations are aware of the risks they are exposed to and take action to avoid being affected by cybersecurity incidents. More effort is being put into **risk management** and cybersecurity policies for businesses are being developed, but there is still much work to be done: **strengthening these policies**; improving companies' capability **to detect and stop cyberattacks**; **investing more money in cybersecurity**; hiring **better and more specialized professionals**; having **business continuity plans** and recovery plans for when disasters and incidents occur, etc.

We strongly recommend having in-house experts in cybersecurity who also have **technical knowledge**. When no such employees are available, the best thing companies can do is going to specialists or external companies. INCIBE offers a **catalogue with all kinds of cybersecurity** firms that offer these services.

What are the main challenges for companies regarding cybersecurity threats? And what are the challenges for the information-security sector?

INCIBE's position on this is that the challenges for companies or businesses will relate to **their level of technological dependence and maturity in terms of cybersecurity**. For example, in the case of SMEs,

desarrollando políticas de ciberseguridad ligadas al negocio, pero aún hay mucho por hacer: **reforzar estas políticas**; fortalecer las capacidades de las empresas para **detectar y frenar ciberataques**; **invertir más dinero en la ciberseguridad**; dotarse de **mejores profesionales** y más especializados; disponer de **planes de continuidad de negocio** y de planes de recuperación frente a desastres e incidentes, etc.

Es muy recomendable tener expertos en ciberseguridad que dispongan de **conocimientos técnicos**. Si no contamos con ese personal entre nuestros empleados lo mejor es acudir a especialistas o empresas externas. Desde INCIBE ofrecemos un **catálogo de empresas de ciberseguridad** de todo tipo que prestan esta clase de servicios.

¿Cuáles son los retos principales de las compañías para hacer frente a las amenazas en materia de ciberseguridad que puedan recibir? Y, ¿cuáles son los retos a los que se enfrenta el sector de seguridad de la información?

Desde INCIBE expresamos que los retos de las compañías o empresas irán relacionados con la **dependencia tecnológica** y la **madurez en ciberseguridad** que hayan adquirido. Por ejemplo, si nos referimos a pymes, habrá que analizar la actividad a la que están dedicadas, ya que se trata de uno de los **"públicos" más afectados por los incidentes de ciberseguridad** en gran medida por la ausencia de políticas, procedimientos y buenas prácticas que no suelen implementar en sus procesos de negocio. La preparación y formación del personal de las empresas es esencial para hacer frente a las amenazas, por ello **las labores de concienciación deberían ser una primera línea de defensa**, ya que como es bien conocido, **el usuario es una de las principales vías de generación de incidentes en las empresas**. La falta de presupuestos para la inversión en ciberseguridad es otra de las cuestiones que entra en juego cuando nos referimos a los retos. Las empresas, sobre todo las más pequeñas, no ven en muchas ocasiones la necesidad de invertir en herramientas y soluciones en ciberseguridad que por otro lado, a veces no requieren de grandes cantidades económicas para implementar medidas.

El otro punto de vista lo podemos encontrar en las empresas que se dedican a **ofrecer productos o servicios de ciberseguridad.** El mundo de la ciberseguridad es un campo que se encuentra en **evolución permanente**. A esta evolución hemos de añadirle además la **diversificación y la complicación** que suponen los escenarios tecnológicos y la manera de usarlos por parte de las compañías. Si echamos una mirada hacia la década de los 90, poco o nada tiene que ver a cómo se protegen actualmente los activos. La nube, los smartphones, el IoT y numerosas tecnologías incipientes hacen que los expertos en ciberseguridad y las compañías que ofrecen servicios de protección estén **continuamente en alerta** con el objetivo de tratar de

their activity needs to be analysed, because they are one of the **groups most affected by cybersecurity incidents**, largely because of their procedures and because they don't have any policies and usually don't implement good practices in their business processes. Preparing and training employees is essential in dealing with threats. **Awareness-raising should be the first line of defence** because, as it is well known, **users are one of the primary causes of incidents in companies**. Another challenge is the lack of funding for investments in cybersecurity. Companies, especially smaller businesses, often do not see a need for investing in cybersecurity tools and solutions that sometimes do not actually require large amounts of money to implement measures.

Then there is the other perspective, the one of the companies **offering cybersecurity products or services**. The world of cybersecurity is **constantly evolving**. Add to this the **diversification and sophistication** of all the different technologies that are out there and the ways in which they are being used by companies. The way things were in the nineties has little or nothing to do with how assets are protected nowadays. The cloud, smartphones, the IoT, and numerous emerging technologies make it necessary for cybersecurity experts and companies that offer protection services **to always be on the alert** to try and maintain security. This forces them **to constantly research** the threats that arise daily on the Internet in order to reduce or mitigate the risk they pose.

What are the basic rules that both companies and citizens should follow to protect their information?

Although the list grows by the day as Internet services evolve and new ones appear, there are some basic recommendations that should always be considered:

1. **Protect devices well with security tools**. Have anti-malware software and a firewall at the very least.
2. Update terminals with the latest **patches and security updates** recommended by manufacturers

mantener la seguridad. Esto les obliga a realizar una **investigación permanente** en relación a las amenazas que cada día surgen en Internet, para buscar mecanismos que permitan reducir su riesgo o mitigarlo.

¿Qué normas básicas deben cumplir tanto las empresas como los ciudadanos para velar por la seguridad de su información?

Aunque la lista crece día tras día a medida que evolucionan y aparecen nuevos servicios en Internet, algunas recomendaciones básicas que siempre se deben tener en cuenta serían:

1. **Dispositivos bien protegidos con herramientas de seguridad**. Al menos un antimalware y un cortafuegos.
2. Equipos "al día" con los últimos **parches y actualizaciones de seguridad** que recomienda el fabricante (del dispositivo y de las aplicaciones).
3. Realizar **copias de seguridad** (backups) en base a nuestras necesidades y cifrar la información.
4. Estar informado sobre los **últimos incidentes o estafas que se han producido.**
5. **Usar el sentido común**, para que al igual que nos ayuda en situaciones cotidianas, lo haga también cuando navegamos por Internet, con el objetivo de detectar situaciones sospechosas en las que el ciberdelincuente trate de engañarnos (ingeniería social) para que pinchemos en un enlace, abramos un adjunto, etc.

De qué forma difunden la necesidad de que los menores hagan un uso seguro y responsable de la tecnología?

INCIBE, bajo el liderazgo y coordinación de la Secretaría de Estado para la Sociedad de la Información y Agenda Digital, gestiona el **Centro de Seguridad en Internet para menores**, Internet Segura For Kids (IS4K), que tiene por objetivo la **promoción del uso seguro y responsable de Internet y las tecnologías entre niños y adolescentes.**

Dentro de las líneas de acción que el centro tiene encomendadas están la **sensibilización y formación,** así como ayudar a **reducir el contenido criminal en Internet** y proporcionar desde septiembre de 2017 el servicio telefónico de la línea de ayuda de IS4K sobre un uso seguro y responsable en Internet por los menores.

Las principales líneas de actuación que ejecuta IS4K son:

Crear conciencia y capacitación, a través del desarrollo de campañas, iniciativas y programas en todo el país como el de Cibercooperantes o las Jornadas escolares.

(of the device and the applications).
3. **Make backups** according to your needs and encrypt the information.
4. Be up to date on **the latest incidents or scams**.
5. **Use common sense** on the Internet the same way you would in real life to detect suspicious situations where cybercriminals try to trick us (using social engineering) into following a link, opening an attachment, etc.

How do you disseminate the need for underage people to use technology safely and responsibly?

INCIBE, under the leadership and coordination of the Secretary of State for the Information Society and the Digital Agenda, manages **IS4K (Safe Internet for Kids)**, an Internet security centre for minors whose objective is **to promote the safe and responsible use of the Internet and technologies among children and teenagers.**

The lines of action that our centre has been entrusted with include **awareness-raising and training**, in addition to helping **reduce criminal content on the Internet** and, since September 2017, running the IS4K hotline providing advice on the safe and responsible use of the Internet by minors.

IS4K's main courses of action are:

Awareness-raising and training, by developing campaigns, initiatives and programmes in all of Spain, such as the cybervolunteers and the school talks.

The IS4K's hotline offers **advice and help** on how to face Internet's risks through a team of psychologists. IS4K **is present in events all over Spain** and participates actively in events such as CyberCamp and Safer Internet Day in Spain.

IS4K **contributes to reducing criminal content** on the Internet, mainly child sexual abuse, by providing support to State security forces and law enforcement agencies.

How does INCIBE support Spain's cybersecurity industry? What are its main contributions?

INCIBE works closely together with Spain's cybersecurity industry to enhance:

- **Its development**, that is, helping it develop products and services that meet existing global demand.
- **Its internationalization**, since it needs to step outside its national borders to offer its services to the global sector in which it operates.
- **Its competitiveness**, but also R&D&I. INCIBE has invested a lot of resources in **promoting R&D&I** at the global level, in building teams that research,

La Línea de ayuda de IS4K ofrece **consejos y asistencia** sobre cómo enfrentar los riesgos de Internet a través de un equipo de psicólogos. IS4K tiene **presencia en eventos de toda España** y participa en eventos como CyberCamp y el Día de Internet Segura en España.

IS4K **contribuye a reducir el contenido criminal en Internet**, principalmente de abuso sexual infantil, dando soporte a las Fuerzas y Cuerpos Seguridad (FCSE).

¿Cómo apoya el INCIBE a la industria nacional de ciberseguridad? ¿Cuáles son sus principales aportaciones?

INCIBE trabaja intensamente junto con la industria nacional de ciberseguridad en:

- **Su desarrollo**, es decir, en que desarrollen productos y servicios que satisfagan la demanda mundial que existe.
- **Su internacionalización**, puesto que es un sector global, que tiene que salir fuera a dar a conocer sus servicios.
- **En la competencia**, pero también trabajando en la I+D+i. INCIBE ha invertido muchos recursos en **potenciar la I+D+i** en el ámbito internacional, en constituir equipos que investiguen, desarrollen e innoven aquellas soluciones que incorporan nuestras empresas a corto plazo y que les hará más competitivas.

INCIBE, en su apuesta por el desarrollo de nuevas empresas de base tecnológica en el ámbito de la ciberseguridad, organizó en 2017 la primera edición de su Programa Internacional de Aceleración, **Cybersecurity Ventures**. Un programa que ofreció un apoyo intensivo durante cuatro meses a 10 start ups seleccionadas, en forma de capacitación, mentorización y vinculación con inversores, con el objetivo de **madurar los negocios para atraer inversiones y ayudarlos a captar los primeros clientes.** Esta aceleradora es fundamental para convertir a España en **un país innovador a nivel europeo e internacional** y refuerza el compromiso de INCIBE con los emprendedores de empresas con base tecnológica y con la captación y promoción de talento en ciberseguridad.

Cuál es la visión del Instituto Nacional de Ciberseguridad sobre el estado de la ciberseguridad empresarial en 2018? ¿Cómo creen que evolucionará en un futuro próximo?

Para dar respuesta a la primera cuestión tenemos que considerar al menos dos variables clave dentro de las empresas. En primer lugar, **la dependencia tecnológica** de la organización en relación al número de servicios y tecnologías que usa; en segundo lugar, **la madurez en ciberseguridad** que determinará el nivel de concienciación y las herramientas de las que

develop and innovate short-term solutions for our companies that will make them more competitive.

INCIBE, as part of its support for the development of new tech-based companies in the field of cybersecurity, organized the first edition of its International Acceleration Programme, **Cybersecurity Ventures**, in 2017. A four-month programme that offered ten specially selected start-ups intensive support in the form of training, mentoring and contacts with investors, with the objective of **helping those businesses mature and thus attract funding and getting their first clients**. This accelerator plays an essential part in transforming Spain into an **innovative country in Europe and internationally,** and it strengthens INCIBE's support for entrepreneurs of tech-based companies and commitment to the recruitment and promotion of cybersecurity talent.

What is INCIBE's view on the state of corporate cybersecurity in 2018? How do you think it is going to evolve in the near future?

To answer the first question we need to consider at least two key variables within companies. The first one is **the organization's technological dependence**, measured in the number of services and technologies it uses, and the second one is **its cybersecurity maturity**, which will determine its level of awareness and the tools it has to face cyberincidents. These variables could tell us that companies with a high level of technological dependence are usually better prepared than those with a low level, although the sector they belong to also plays a crucial role.

To give an idea of the impact of cyberthreats, here are INCIBE's data concerning the number of incidents managed by the CERTSI. There were 17,943 in 2014; 50,106 in 2015; 115,488 in 2016, and more than 123,000 in 2017.

As these numbers show, **cyberincidents are on the rise, growing year after year and evolving**. This rise in the number of registered attacks reflects their existence

dispone para hacer frente a los ciberincidentes. Teniendo esas variables podríamos determinar que una empresa con alta dependencia tecnológica suele estar más preparada que una que tiene baja dependencia, aunque también es determinante el sector al que pertenecen.

Para tener una referencia del impacto de las ciberamenazas, debemos hacer referencia a los datos que INCIBE tiene en relación al número de incidentes gestionados desde el CERTSI. En 2014 fueron 17.943, 50.106 en 2015, 115.488 para 2016 y más de 123.000 en 2017.

Como indican los números, **los ciberincidentes van en aumento, crecen año tras año y evolucionan**. Este incremento de ataques registrados refleja su existencia y nos ofrece la oportunidad de conocer su tipología o el público al que van dirigidos.

¿Cuáles son las fortalezas y oportunidades de la industria nacional en materia de seguridad de la información?

Aún a pesar de los avances que ha supuesto la tecnología en términos de ciberseguridad, en un lado de la balanza aún encontramos algunos escollos que poco a poco parece que vamos salvando. Sin ir más lejos, en todo lo relativo a la seguridad industrial que afecta a las empresas, podemos ver cómo, a pesar del gran trabajo que se está realizando, aún quedan cuestiones por resolver como **la falta de certificaciones de tecnologías** que garanticen los procesos de operación de estas empresas; **falta de normativa específica**; **desarrollo de aplicaciones y hardware sin o con un bajo nivel de seguridad implementada "por defecto"** y **una legislación o normativa lenta**, entre los más importantes.

En el otro lado, podemos encontrar las fortalezas y las acciones e iniciativas que se están llevando a cabo en la actualidad y que favorecerán el progreso en este campo. Por enumerar alguna, destacamos: **el gran impulso que se está realizando a través de las organizaciones públicas**, así como **la innovación que se está produciendo en el sector industrial** en términos de ciberseguridad; la normativa y legislación concerniente a aquellas infraestructuras denominadas como críticas, así como la **concienciación en ciberseguridad** que se está llevando a cabo en este tipo de empresas; organización de cientos de foros que permiten **extender la cultura de ciberseguridad**, así como informar de los últimos avances; la creación de **centros de respuesta a incidentes** (CERTs) específicos para cada ámbito (pymes, industria, etc).

Desde el INCIBE llevan a cabo iniciativas internacionales como los International CyberEx o los CyberSecurity Summer BootCamp, entre otros encuentros. ¿Qué propósitos persiguen?

and allows us to learn more about the different types and their targets.

What are the strengths and opportunities of Spain's industry in matters of information security?

Even with all the advances obtained thanks to cybersecurity technology, there are still some obstacles facing us, although it looks like they are slowly being overcome. Without going any further, all the aspects of industrial security that affect companies show us that, in spite of all the effort being invested, there are still important matters to be resolved, such as **a lack of certified technologies** that guarantee these companies' operating processes, a l**ack of specific regulation, applications and hardware that are developed with no or little default security, and slow legislation or regulation, among the most important ones.**

Now, there are also strong points. Actions and initiatives are currently being carried out that will facilitate progress in this field. To name but a few: **the strong momentum being generated by public organizations** and **the innovation in cybersecurity taking place in the industrial sector**; regulations and legislation concerning infrastructures considered to be critical, as well as the growing **awareness of cybersecurity** in this type of companies; the organization of hundreds of forums that help **extend the culture of cybersecurity** and report on the latest advances known; and the creation of **incident-response centres** (CERTs) specific to every area (SMEs, industry, etc.).

INCIBE carries out international initiatives like the International CyberEx or the CyberSecurity Summer BootCamp, among others. What are the objectives?

We have the parameters and conditions to be an international centre of reference. **Cybersecurity has become a primary objective for many countries**, which are investing many resources and also want to be leaders in the sector. It is safe to say that **INCIBE is a reference in many countries that are of commercial interest to Spain**, for example, in Latin America. An example is the **Cybersecurity Summer BootCamp** initiative, organized in collaboration with the Organization of American States (OAS), which provides free training for cybersecurity technicians, judges, prosecutors and policemen. Last year, 300 people from 30 countries attended, and this year we want to have more than 400 attendees from an also greater number of countries. **We have an important corporate network in the field of cybersecurity.**

Furthermore, we have compiled a list of more than 200 companies in Spain that offer cybersecurity products or services, and some of them **are already competing on the international market.**

Tenemos los parámetros y las condiciones para poder ser un centro de referencia internacional. **La ciberseguridad se ha convertido en un objetivo fundamental de muchos países**, que están invirtiendo muchos recursos y también quieren liderar este sector. Podemos decir que **INCIBE es un referente en muchos países de interés comercial para España**, por ejemplo, de Latinoamérica. Un ejemplo es la iniciativa **Cybersecurity Summer BootCamp**, organizada en colaboración con la Organización de Estados Americanos (OEA) por la que se capacita de forma gratuita a expertos en ciberseguridad de carácter técnico, a jueces y fiscales y a policías. El pasado año se contó con 300 personas de 30 países y nuestro objetivo este año es superar las 400 y aumentar el número de países. **Tenemos un tejido empresarial en el ámbito de la ciberseguridad importante.**

Además, tenemos contabilizadas más de 200 empresas que tienen producto o servicio de ciberseguridad en nuestro país y algunas de ellas **ya están compitiendo en el mercado internacional.**

¿Qué perfiles se necesitan en el sector de la seguridad de la información?

No se demandan perfiles únicamente técnicos, sino que van apareciendo **nuevas profesiones relacionadas**, como por ejemplo: abogados especializados en privacidad, responsables de datos de ficheros, peritos informáticos, economistas que permitan a las grandes compañías de seguros hacer frente mediante nuevas pólizas de ciberriesgos, a los ciberataques. Tenemos que indicar que en la parte técnica se ha notado un incremento en el número de ofertas laborales relacionadas con **la "inteligencia" de los datos**, que permiten prevenir ciertas amenazas o detectarlas a tiempo. Europa está demandando una gran cantidad de profesionales en este campo y sin duda **es un gran nicho de mercado** tanto para empresas como profesionales que estén interesados en especializarse en ciberseguridad.

Qué experiencia se requiere para trabajar como profesional en el área de ciberseguridad?

No cabe duda que los profesionales de la ciberseguridad, en un alto porcentaje, provienen de **estudios y carreras eminentemente técnicas**, aunque poco a apoco y por el **carácter multidisciplinar** que está adquiriendo este campo, cada vez más son necesarios perfiles de otra índole como el derecho, marketing, etc. No obstante dependerá en gran medida de la especialización que se busque, ya que hace un par de décadas un experto en ciberseguridad podía tener conocimientos en un amplio abanico de servicios, pero con el aumento de estos, en la actualidad es necesario establecer límites en la experiencia de los profesionales que se dedican a la seguridad de la información.

What profiles are currently needed in the information security sector?

Not only technical profiles are in demand, but also **new related professions**, like attorneys specialized in privacy law, file-data managers, IT experts, and economists who design new cyber-risk policies that allow insurance companies to deal with cyberattacks. In the technical field, we have noticed an increase in the number of job offers related with **data intelligence**, which allows the prevention or early detection of certain threats. Europe needs an ever increasing number of professionals in this field and it is without a doubt **an important market niche** for companies and professionals interested in specializing in cybersecurity.

What experience is required to work as a professional in the field of cybersecurity?

A large percentage of cybersecurity professionals undoubtedly come from **very technical studies and careers**. It is becoming a **multidisciplinary field**, however, and there is a growing demand for different profiles, such as law, marketing, etc. Everything will still largely depend on the specialization that is required, though, because a couple of decades ago, it was possible for a cybersecurity expert to know about a wide range of services, but these days there are so many that one really has to limit the experience required from professionals in the field of information security.

It is possible to access strategic positions in the world of cybersecurity **provided one knows the company's goals and has a clear view of the risks it may be exposed to.**

On the one hand, we have the technical side of things, with professionals who make systems secure, conduct safe development of applications, do technical security audits, and perform many more tasks. So one has to have a knowledge of operating systems, technologies and such, but **at a much deeper level than conventional users.**

Dentro del mundo de la ciberseguridad, es posible acceder a puestos de carácter estratégico **siempre que se conozcan los objetivos de la empresa y se tenga una visión en relación a los riesgos a los que pueda estar expuesta una organización.**

Por un lado, en la parte más técnica podemos encontrar profesionales que se encargan de la securización de sistemas, el desarrollo seguro de aplicaciones, la realización de auditorías de seguridad de carácter técnico y un largo etcétera. Por ende, habrá que tener conocimientos en sistemas operativos, tecnologías y demás, pero **con un nivel de profundidad superior al de los usuarios convencionales.**

Por otro, también será necesario la participación de personal **experto en legislación** y temas similares, ya que serán los encargados de adecuar, de manera normativa, todos los aspectos que afectan a la privacidad, auditorías para velar por la protección de datos, cumplimiento legal en materia de ciberseguridad, etc. Prácticamente todos ellos han de tener **destrezas y conocimientos relacionados con las Tecnologías de la Información y con el manejo de datos** y como vemos, únicamente no es necesaria la capacitación en los aspectos más técnicos, si no que el Derecho, entre otras disciplinas, también es necesario.

¿Con qué aportaciones concretas apoyan al talento?

Consideramos que tenemos que trabajar para que nuestra industria de ciberseguridad crezca y sea competitiva a nivel internacional, **incidiendo en la promoción del talento**, pues ya a día de hoy existe una demanda de profesionales difícil de satisfacer. Existen estudios sobre la demanda no satisfecha de profesionales de ciberseguridad en Europa, que es considerable. Y en España también. Desde INCIBE estamos desarrollando iniciativas para **promover el interés entre los jóvenes por dedicarse a este sector, identificar talento y establecer el contacto con las empresas.** Queda mucho por hacer, pero creo que vamos por buen camino. Muestra de ello es la competición europea de ciberseguridad, **European Cybersecurity Challenge**, donde el equipo español, formado por 10 jóvenes talentos, fue el campeón de Europa el año pasado. Esto demuestra que en España hay talento y que las actividades que estamos llevando a cabo están dando sus frutos

¿Cómo será nuestra vida cuando, gracias al Internet of Things, todo esté conectado a Internet? ¿De qué forma la seguridad de nuestra información puede verse afectada?

Principalmente, el problema al que los dispositivos IoT se enfrentan en la actualidad es **la falta de una correcta gestión de la seguridad tanto a nivel de confidencialidad/integridad** (comunicaciones y acceso), **como de aplicación**

On the other hand, there is also a need for personnel **specialized in legislation** and similar subjects, because they will have to adjust all the privacy-related rules, the audits covering data protection, the legal enforcement of cybersecurity, etc. All of the above require **skills and knowledge related to information technologies and data management**, but it is not enough to master the more technical aspects alone; law and other disciplines are also needed.

How do you support talent?

We consider that we have to help our industry grow and be competitive at the international level **by promoting talent**, because at the moment there is demand for qualified professionals and it is not being met adequately. There are studies about the unmet demand for cybersecurity professionals in Europe, and they show it is considerable. So it is in Spain. INCIBE is developing initiatives **to motivate young people to work at this sector, to identify talent, and to establish contact with companies**. There is a lot to be done, but I believe we are on the right track. Proof of this is that last year's **European Cybersecurity Challenge**, the European cybersecurity competition, was won by the Spanish team, composed of ten young talents. This goes to show that there is talent in Spain, and that the activities we are carrying out are bearing fruit.

When everything is connected to the Internet thanks to the Internet of Things, what will our lives be like? How can this affect the security of our information?

First and foremost, the problem currently facing IoT devices is **a lack of adequate security management both at the confidentiality/integrity** (communications and access) **and the application/update** (software and hardware) levels. We must bear in mind that **many of these devices connect to the Internet, sharing potentially sensitive data about ourselves**

y actualizaciones (software y hardware). No debemos olvidar que **muchos de estos dispositivos se conectan a Internet y dejan datos que pueden ser sensibles sobre nosotros o nuestro entorno**, por lo que los riesgos en privacidad son importantes si no están bien protegidos o no se toman las medidas adecuadas. Es frecuente el uso de **contraseñas débiles o fijadas por defecto**, **la transmisión de datos sin cifrar, protección insuficiente** tanto del sistema como de los datos que se manejan, etc. Adicionalmente, el problema puede verse agravado por **la desatención de los dispositivos a la hora de recibir las actualizaciones** necesarias.

Por último y como se ha visto en los últimos 4 o 5 años los dispositivos de IoT mal protegidos o desactualizados **pueden ser utilizados maliciosamente por terceros para realizar ciberataques**, principalmente del tipo de denegación de servicio hacia la disponibilidad de un sistema o red, como la botnet Mirai , por ejemplo.

¿Cuáles son los retos futuros del INCIBE?

Desde INCIBE nos planteamos tres objetivos ambiciosos y muy claros: El primero es la protección del ciudadano y el sector privado. Tenemos un papel fundamental para concienciar a ciudadanos y empresas. **La ciberseguridad no es un aspecto reservado a organismos o a países muy especializados, sino que afecta a toda aquella persona que utiliza tecnología.**

Además, debemos acercar la ciberseguridad de una forma **amigable y sencilla**. Prácticamente toda la sociedad española sabe que la ciberseguridad ya es algo que les puede afectar, pero **quizá no saben de qué forma pueden protegerse.** Tenemos que tener la capacidad de detectar lo antes posible todos los ciberataques o incidentes que puedan afectar a ciudadanos y empresas; analizarlo, ponerlo en conocimiento y ayudar en la protección. Debemos seguir cooperando con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE), ya que unir el conocimiento de un investigador con el conocimiento de un técnico está generando muy buenos resultados en la lucha contra el ciberdelito.

Por último, la ciberseguridad es **una oportunidad real para general puestos de trabajo**; para desarrollar las empresas de ciberseguridad actuales; para ayudar a convertir empresas hacia este nuevo sector y para desarrollar nuevas empresas, generar 'start ups' etc. Con los datos que hemos desarrollado desde INCIBE estamos viendo que muchas de ellas siguen siendo viables y algunas están exportando sus servicios en mercados internacionales, por lo que, de esta forma, **también se crea riqueza en nuestro país.**

and our environment, so if these data are not well protected or adequate measures are not taken, this may cause serious risks for our privacy. It is common **to use weak or default passwords, to transfer data without encryption, to insufficiently protect systems** and data being managed, etc. Additionally, the problem may get worse by **devices not receiving proper maintenance in the form of updates.**

Finally, as the last four or five years have shown, badly protected or out-dated IoT devices **can be used maliciously by third parties to carry out cyberattacks**, mainly denial-of-service attacks that make a system or network unavailable, as was the case of the Mirai botnet, to name but one example.

What are INCIBE's challenges for the future?

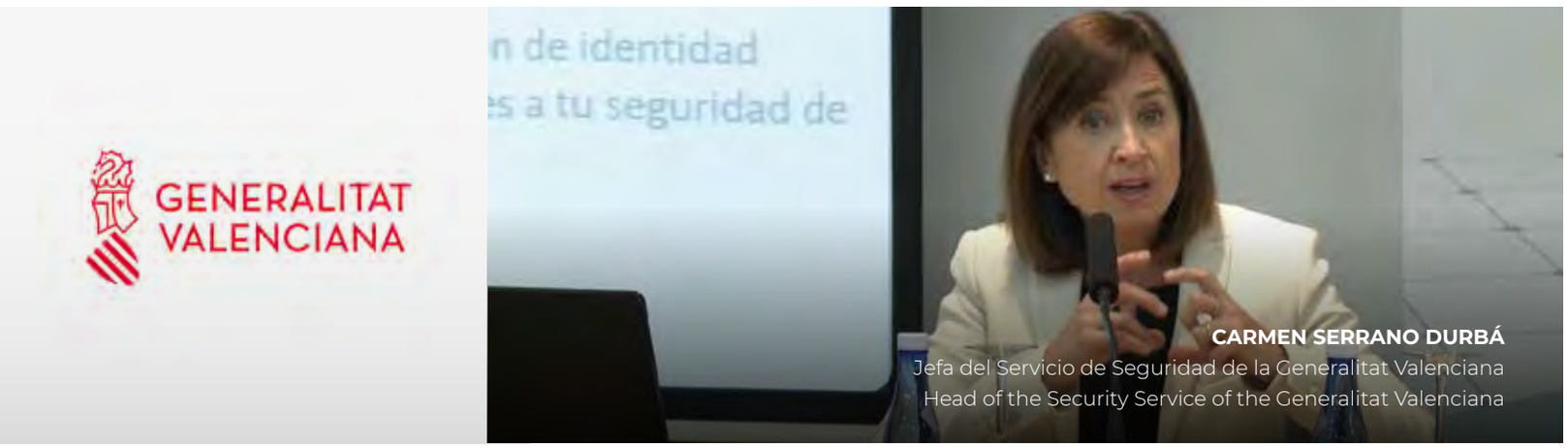
INCIBE has taken on three very clear, ambitious challenges: The first one is to protect citizens and the private sector. We have an essential role to play in raising awareness among citizens and companies. **Cybersecurity is not something reserved for official entities and very specialized countries, but something affecting every person using technology.**

Secondly, we have to present cybersecurity in an **easy, friendly way**. Practically all of Spanish society knows that cybersecurity is something that can affect them, but **maybe they don't know how to protect themselves**. We have to be able to detect as quickly as possible any cyberattacks or incidents that may affect citizens and companies, analyse them, inform about them, and help to protect against them. We have to continue cooperating with the State security forces and law enforcement agencies, because we have found that bringing together the knowledge of researchers and technicians leads to very good results in the fight against cybercrime.

Finally, cybersecurity is **a real opportunity to create jobs**, develop the cybersecurity companies that already exist, help convert companies to this new sector, and develop new companies, generate start-ups, etc. The data we have gathered at INCIBE show that many of them remain viable and some are exporting their services to international markets, so this is also a way of creating wealth in our country.

“No solo nuestros datos corren peligro, sino nuestra privacidad, nuestra intimidad y nuestra vida”

“Not only is our data at risk, but also our privacy, our intimacy, and our lives”



¿Cuáles son las principales áreas que se trabajan desde la Generalitat Valenciana en el área de ciberseguridad?

En la Generalitat Valenciana trabajamos en todas las áreas de ciberseguridad que afectan a los sistemas de información y a las tecnologías implantadas en la Generalitat así como la seguridad de dispositivos IoT, equipos de electro-medicina y sistemas industriales. También trabajamos los aspectos de gobierno y gestión de la seguridad y cumplimiento normativo.

Los elementos de seguridad de la Generalitat están formados por:

- El marco normativo que establece la **Política de Seguridad.**
- Una **Estrategia de Ciberseguridad** que demuestra el compromiso de este gobierno.
- **Instrumentos y tecnologías** de seguridad.
- **Centro de Seguridad TIC** (CSIRT-CV), con equipo humano especializado que trabaja en la prevención y detección temprana y la respuesta ante incidentes.

¿Qué tipo de actuaciones lleva a cabo la Generalitat Valenciana en materia de ciberseguridad?¿Cómo luchan contra el cibercrimen?

Las actuaciones se pueden clasificar en tres grupos: **actividades de prevención**, encaminadas a evitar la materialización de amenazas; **actividades de detección,** orientadas a detectar e identificar la ocurrencia de

What are the main areas that the Generalitat Valenciana (Valencian regional government) works on in the field of cybersecurity?

At the Generalitat Valenciana, we work on all areas of cybersecurity that affect information systems and the technologies we use, as well as the security of IoT devices, electromedical devices and industrial systems. We also handle security governance and management, and legal compliance. The following comprise the Generalitat's security elements:

- The regulatory framework established by the **Security Policy**;
- A **Cybersecurity Strategy** that proves the administration's commitment;
- Security **tools and technologies**;
- **An ICT Security Centre** (CSIRT-CV), with a specialized human team working on prevention, early detection, and incident response.

What action does the Generalitat Valenciana take in the field of cybersecurity? How do you fight cybercrime?

We take three types of action: **prevention**, aimed at preventing threats from materializing; **detection**, meant to detect and identify possible security incidents; and **response**, which includes containment and eradication, recovery, learning, and subsequent feedback. When we detect an incident and suspect it may be of a criminal nature, we get some proof and

posibles incidentes de seguridad y **las actividades de respuesta ante los incidentes** que incluyen la contención y erradicación, recuperación y el aprendizaje y retroalimentación posterior. En caso de que en algún incidente tratado detectemos sospechas de un posible delito, tomamos muestras de las evidencias y trasladamos el caso a las fuerzas y cuerpos de seguridad del estado con los que mantenemos una estrecha relación.

¿Cuáles son los principales retos a los que se ha tenido que enfrentar como jefa del Servicio de Seguridad en la Generalitat Valenciana?

El reto más importante, sin duda, fue hace poco más de un año, **la crisis del WannaCry.** Evitar que ningún equipo se viera afectado en una organización tan grande, suponía implantar unas medidas de contención restrictivas que evidentemente iban a afectar al trabajo de la administración y había que llegar a un equilibrio en el que debíamos **proteger nuestros sistemas sin que dejasen de funcionar los servicios esenciales**, sobre todo en lo que respecta a los servicios sanitarios. Fueron unos días muy intensos en los que llevaba encima una gran responsabilidad.

¿Qué tipo de incidentes en materia de seguridad de la información suele encontrarse más a menudo?

Los incidentes más frecuentes, aunque no los más críticos, son los de **intento de intrusiones desde el exterior**, seguidos de los de código malicioso y los relacionados con el correo electrónico (intentos de phishing).

¿Cuál es exactamente su papel como CISO en ese "conjunto de instituciones de autogobierno" que conforman la Generalitat Valenciana?

Como jefa del Servicio de Seguridad y Responsable de Seguridad en la Generalitat Valenciana mi papel es la **definición de políticas y estrategias de seguridad, la definición de medidas para conseguir los niveles de seguridad requeridos en los distintos sistemas de información y en general la gestión integral de la seguridad TI.**

En el caso de la Administración Pública, existe legislación específica para instar a la Administración a promover, en beneficio de los ciudadanos, el uso de las nuevas tecnologías y está obligada a ofrecer sus servicios a través de medios telemáticos. ¿Cree necesario disponer de un código de buenas prácticas para minimizar los riesgos asociados a su utilización por parte de la ciudadanía?

En mi opinión, lo necesario es generar una **cultura de**

contact State security forces and law enforcement agencies, with whom we work closely together.

What are the main challenges you have faced as head of the Security Service of the Generalitat Valenciana?

The most important challenge was, without a doubt, a little over a year ago, **the WannaCry crisis**. To ensure that no terminals were affected in such a large organization involved applying restrictive containment measures that evidently would affect the administration's functioning, and we had to reach a balance where, on the one hand, **we protected our systems** and, on the other hand, **basic services could still keep functioning,** especially health services. Those were some very intense days in which I carried a heavy responsibility.

What type of incidents involving information security do you encounter most often?

The most frequent incidents, even if not the most critical, are **intrusion attempts from outside**, followed by malicious code and those related with email (phishing).

What is exactly your role as CISO in this "group of self-governing institutions" that make up the Generalitat Valenciana or Valencian regional government?

As head of the Security Service and person in charge of security in the Generalitat Valenciana, my tasks include **the definition of security policies and strategies, the definition of measures to attain the required levels of security in the different information systems, and in general, the overall management of IT security.**

In the case of the civil service, there is specific legislation calling on the administration to promote the use of new technologies in the benefit of citizens. The administration is also obliged to offer its services by telematic means. Do you think a code of good

ciberseguridad en la ciudadanía, no sólo para sus relaciones electrónicas con la Administración sino para poder disfrutar de todas las ventajas de las TIC sin sobresaltos ni malos tragos. Las tecnologías nos arrollan, su crecimiento acelerado en todos los ámbitos, la aparición de tecnologías y soluciones para todo y su capacidad de transformar la sociedad cambiando la forma de hacer las cosas, de relacionarnos, de informarnos, de trabajar, en general de vivir de una forma distinta, nos llega a tal velocidad que las adoptamos sin tener en cuenta los riesgos a los que nos enfrentamos. **Son las personas, las que deben identificar los riesgos y adquirir unas buenas prácticas en el uso de la tecnología.**

Dedicándose al mundo de la seguridad de la información, ¿cómo sentirse seguro en Internet?

Cuando conoces los riesgos y estás al día de las grandes amenazas es imposible sentirse seguro. Bajo la premisa de que la seguridad total no existe la solución es **controlar los riesgos a los que uno se expone**. Con unas buenas prácticas y ciertas precauciones se puede vivir en la red reduciendo los riesgos. Yo, personalmente como usuaria, intento no caer en la paranoia, pero sí que es verdad que me lo pienso bastante antes de hacer el "click". Leo las condiciones de uso que nadie lee, reviso los permisos que piden las aplicaciones, tomo precauciones y compruebo bien a qué redes me conecto, en qué páginas pongo mis datos, qué datos publico, en qué ocasiones debo navegar de forma anónima, etc. A pesar de esto, hago un uso intensivo de las tecnologías y las redes sociales.

¿Está cambiando el papel del CISO en el sector público?

Lo que está cambiando es la concepción de la necesidad de la figura del CISO en la Administración. Cada vez está viéndose más la necesidad de que alguien **gestione la seguridad de forma global en las organizaciones** y que esa figura tenga un puesto de cierto reconocimiento, que se haga oír en la dirección.

practices is necessary to minimize the risks associated with the use of telematic means by the general public?

In my opinion, we need to promote a **culture of cybersecurity** among people, and not only regarding their electronic relations with the administration, but also so they can enjoy all the advantages of ICT without any scares or bad experiences. Technologies overwhelm us. Their rapid growth in all fields, the emergence of technologies and solutions for everything, and their ability to transform society by changing our way of doing things, of relating, of informing ourselves, of working, and in general, of living differently, these are all happening so fast that we adopt them without taking into account the risks we face. **It is up to us, individuals, to identify the risks and to acquire good practices in the use of technology.**

As an expert in information security, can you tell us how to feel safe on the Internet?

When you are aware of the risks and you know all about the latest big threats, it is impossible to feel safe. Once you assume that total security does not exist, the solution is **to control the risks one is exposed to**. Good practices and certain precautions can reduce the risks of living on the Internet. Personally, as a user, I try not to fall into paranoia, but I do think twice before I click. I read the terms of use nobody reads, I review the permissions that apps request, I take precautions, and I check the networks I connect to, what pages I enter my data into, what data I publish, on what occasions I should surf anonymously, etc. In spite of this, I do use technologies and social networks intensively.

Is the role of the CISO in the public sector changing?

What is changing is the concept of the need for a CISO in public administration. It is becoming increasingly clear that organizations need someone **who manages security in a global way** and that this person needs to be recognized, they need to have a say in management.

What are the strengths and opportunities of the Valencian autonomous region in matters of information security?

The Valencian autonomous region is gaining importance in the field of cybersecurity. There are local companies dedicated to this field that enjoy national and international recognition and prestige and, why not to mention it, the CSIRT-CV (ICT Security Centre) was the first CERT at the autonomic level and, as such, a pioneer in its field. After more than ten years, it has attained an important level of maturity and recognition. All of this has generated an important

¿Cuáles son las fortalezas y oportunidades de la Comunitat Valenciana en materia de seguridad de la información?

La Comunidad Valenciana está adquiriendo relevancia en el campo de la Ciberseguridad. Hay empresas dedicadas a esta materia con reconocimiento y prestigio a nivel nacional e internacional y, porqué no decirlo, CSIRT-CV que fue un CERT pionero al ser el primero a nivel autonómico, con más de 10 años de evolución, ha alcanzado ya una madurez y reconocimiento importante. Todo esto ha generado una sinergia importante en el sector de la ciberseguridad. Por otro lado, nuestra comunidad cuenta con gran cantidad de empresas que necesitan apoyo de empresas especializadas para mejorar su ciberseguridad, por lo que esto ofrece **grandes oportunidades al sector.**

Dirige el CSIRT-CV, el Centro de seguridad TIC de la Comunitat Valenciana, ¿qué tipo de iniciativas lleva a cabo?

CSIRT-CV presta servicios a los ciudadanos de la Comunidad Valenciana, los profesionales y entidades privadas, especialmente las de menor tamaño y la Administración Pública, tanto local como autonómica. Principalmente esta última por la ubicación del centro por lo que las actuaciones son muy variadas. Dentro de la red corporativa de la Generalitat lleva la **monitorización de la red, detección y respuesta a incidentes.** Para el resto de colectivos, se están iniciando actuaciones específicas para cada uno de ellos encaminadas sobre todo a la **concienciación y formación** en ciberseguridad. Es prioritario que se genere una cultura de ciberseguridad en todos los ámbitos de nuestra sociedad.

¿Cómo es la relación del CSIRT-CV con las empresas? ¿En qué medida las ayuda?

CSIRT-Cv tiene a las empresas valencianas dentro de su ámbito de actuación, con **especial atención a las PYME**. Los servicios que se ofrecen a estas, además del soporte técnico cuando sufren un incidente de seguridad, son los informes de alertas y boletines, la monitorización de servicios web por la que les informamos de servicios que puedan tener comprometidos y sobre todo los de formación y concienciación. Actualmente estamos preparando campañas de sensibilización y **cursos de formación para directivos de las empresas y cursos de perfil más técnico dirigidos a los CISO.**

¿Las empresas TIC están realmente concienciadas de la importancia de salvaguardar su información corporativa?

No lo suficiente. Se oye hablar mucho de ciberseguridad, como consecuencia de los ciberincidentes de gran

synergy in the cybersecurity sector. Our region also has numerous companies that need the support of specialized companies to improve their cybersecurity, so it is also a **great source of opportunities for the sector.**

You run the CSIRT-CV, the Valencian autonomous region's ICT security centre. What type of initiatives do you implement?

The CSIRT-CV provides services to the citizens of the Valencian autonomous region; professionals and private entities, especially the smaller ones; and the public administration, both at the local and autonomic levels. The latter mainly because of the centre's location, so there is great variety in its actions. Within the corporate network of the regional government, the CSIRT-CV **monitors the network and detects and responds to incidents**. For the rest of collectives it carries out customized actions mainly aimed at awareness-raising and training in cybersecurity. Creating a culture of cybersecurity in all areas of our society is a priority.

How is the CSIRT-CV's relationship with companies? To what extent do you help them?

The CSIRT-CV's scope of action includes Valencian companies, **especially SMEs**. In addition to technical support for security incidents, it offers them security alerts, newsletters, web-service monitoring where we tell them what services may be compromised, and especially, training and awareness-raising. We are currently preparing awareness-raising campaigns and **training courses aimed at business executives as well as more technical courses for CISOs.**

Are ICT companies really aware of how important it is to safeguard their corporate information?

Not sufficiently. There is a lot of talk about cybersecurity

impacto que han tenido mucha repercusión mediática y por la entrada en vigor del RGPD. De todos modos no se lo toman tan en serio como deberían. Las empresas TIC deberían preocuparse de que **todos los productos que desarrollan sean seguros por diseño.** Es el **"security by design"** que referencia el RGPD así como de integrar la seguridad en sus procesos de negocio.

¿Qué consejo imprescindible de ciberseguridad le daría a una empresa?

El primer consejo es que hagan lo que hagan, sea cual sea su actividad, que **incluyan en los objetivos de la empresa la ciberseguridad.** Las empresas que no hayan pensado en la seguridad tendrán poco futuro. La seguridad va a ser un **factor de excelencia** de las empresas y tiene que tener un carácter horizontal. Esta seguridad tiene que guiarse por principios de **racionalidad y proporcionalidad**, es decir, que hay que analizar los riesgos, identificarlos y hacer un Plan de Mejora de la Seguridad que priorice las acciones y los presupuestos. Igual que se dedican recursos a la seguridad física hay que dedicarlos a la ciberseguridad. También es una buena medida contar con servicios profesionales de ciberseguridad y cuando sea necesario contratar servicios operación de Ciberseguridad (SOC) que monitoricen y detecten posibles incidentes. Aquí, en la Comunidad Valenciana contamos con buenas empresas que prestan este tipo de servicios.

Las empresas seguras serán las más competitivas y las que produzcan soluciones seguras serán las que destacarán en el mercado. Próximamente, el mercado será el que regule las necesidades de seguridad. La demanda de seguridad hará que las empresas se pongan las pilas.

El CSIRT-CV es una iniciativa pionera, al tratarse del primer centro de estas características que se crea en España para un ámbito autonómico. Dado que Valencia quiere importar el modelo de Silicon Valley ¿Cómo puede

now as a consequence of the recent high-impact, high-profile cyberincidents and because of the new GDPR. Still, ICT companies do not take it as seriously as they should. They should concern themselves with ensuring **all their products include security by design, by which** I mean the **"security by design"** referred to by the GDPR, and the integration of security in their business processes.

Is there any crucial advice you would give companies?

My first piece of advice is that whatever they do, whatever their activity is, they should **include cybersecurity in their corporate objectives**. There is little future for companies that have not considered cybersecurity. Security is going to be a **factor of excellence** for businesses. And it has to be horizontal in nature. This security must be guided by principles of **rationality and proportionality**, i.e., risks have to be analysed, identified, and a Security Improvement Plan has to be designed to prioritize actions and funding. In the same way that resources are dedicated to physical security, they have to be dedicated to cybersecurity, too. It is also a good idea to hire the services of cybersecurity professionals and, when necessary, to contract SOC services that monitor and detect possible incidents. The Valencian autonomous region has good companies that provide these types of services.

Secure companies will be the most competitive ones and those that produce secure solutions will stand out in the marketplace. Soon it will be the market that regulates security needs. The demand for security will force companies to get their act together.

The CSIRT-CV is a groundbreaking initiative. It is the first such centre to have been created in Spain for an autonomic level. Since Valencia wants to import the Silicon Valley model, what benefits does it derive from having a centre of reference in information security and new technologies like the CSIRT-CV?

The maturity attained by the CSIRT-CV since it started ten years ago makes it a centre of reference that can serve as a model for many companies. Its position in specialized forums and in national and international CERT groups also helps other CERTs that are looking to consolidate and to enter these groups where collaboration takes place and information is exchanged on threats, defence strategies, techniques, tools and procedures, and the response to global incidents is coordinated in a joint, procedural way. This year, CSIRT-CV is leading the CSIRT.es group, the CSIRT/CERT forum whose actions cover Spain.

Do you believe people in general know enough about the

beneficiarle el contar con un centro de referencia en seguridad de la información y las nuevas tecnologías como CSIRT-CV?

La madurez que ha adquirido CSIRT-CV en los más de diez años de trayectoria convierten al centro en un referente que puede servir de modelo para muchas empresas.

Por otro lado, su posicionamiento en foros especializados y en los grupos de CERT nacionales e internacionales sirve de apoyo a aquellos CERT que tengan como objetivo consolidarse como tales y entrar a formar parte en los grupos, que es donde se colabora y comparte información de amenazas, estrategias de defensa, técnicas, herramientas y procedimientos, y se coordina la respuesta ante incidentes globales de forma común y procedimentada. Este año CSIRT-Cv está liderando el grupo CSIRT.es, foro de CSIRT/CERT cuyo ámbito de actuación es el territorio español.

¿Cree que los ciudadanos tienen un conocimiento adecuado sobre la importancia de velar por la seguridad de su información? ¿De qué forma se les apoya desde CSIRT-CV?

No, la inconsciencia de los riesgos está bastante generalizada. Como parte de su catálogo de servicios, a principios de 2017 CSIRT-CV empezó a dar forma al llamado **"Plan Valenciano de Capacitación en Ciberseguridad"**, proyecto con el objetivo de aumentar el nivel de madurez en ciberseguridad y la confianza en el uso de la tecnología de ciudadanos, empresas y personal de las diferentes administraciones públicas. El Plan Valenciano de Capacitación en Ciberseguridad, que establece acciones dirigidas a distintos colectivos, en especial a **aquellos más desprotegidos, amenazados o con riesgo de exclusión**. Este plan está dirigido a fomentar prácticas seguras en el uso de Internet y las tecnologías entre ciudadanos, empresas y Administraciones, incluida la Generalitat en su conjunto, y a crear **una cultura de ciberseguridad en todos los valencianos**. Dicho plan cuenta con un plan de comunicación del cual se han empezado a difundir campañas en los medios. También se ha lanzado un nuevo portal de concienciación (https://concienciat.gva.es/), que concentra todos los recursos de formación y concienciación: cursos, infografías, consejos de seguridad, guías, etc.

¿Qué tipología de protocolos tiene establecido el CSIRT-CV para actuar rápida y eficazmente ante un incidente de seguridad en sistemas de información?

CSIRT-CV tiene implantado y certificado un modelo de gestión **basado en la norma ISO 27001.** Además, la base del funcionamiento de un CSIRT/CERT son los procedimientos. Es un centro procedimentado y preparado para actuar en la respuesta ante incidentes y para la gestión de crisis.

importance of ensuring their information is secure? How do you support them at the CSIRT-CV?

No. There is a fairly general lack of awareness of the risks. As part of its range of services, at the beginning of 2017 the CSIRT-CV started defining the **"Valencian Cybersecurity Training Plan"**, a project aiming to make citizens, companies and government workers more competent in cybersecurity as well as more confident in the use of technologies. The Plan establishes actions designed to help different collectives, especially **those that are most vulnerable, threatened, or at risk of exclusion**. It promotes safe practices in the Internet and technology use among citizens, companies and public administration, including the entire Generalitat Valenciana, and it creates **a culture of cybersecurity in all Valencians**.
As part of its communications plan, several media campaigns have been initiated. A new awareness-raising website has been set up (https://concienciat.gva.es/) that groups together under one roof all the training and awareness-raising resources: courses, infographics, safety tips, guides, etc.

What types of protocols has the CSIRT-CV established to ensure swift and efficient action against security incidents in information systems?

The CSIRT-CV uses a certified management model **based on the ISO 27001 norm**. CSIRT/CERT centres operate based on procedures. Ours is a procedural centre prepared to act in response to incidents and to manage crises. WannaCry was a real-life test for that.

The concept of the Internet of Things is becoming ever more deeply embedded in our society. Is our data at risk? What will our lives be like when everything is connected to the Internet?

This is actually closer than would appear. Without realizing it, we connect more and more things to the Internet: cell phones, surveillance cameras, television

Esto se puso a prueba en real en el momento del WannaCry.

El concepto Internet of Things está cada vez más latente en la sociedad. ¿Nuestros datos corren peligro?, ¿cómo será nuestra vida cuando todo esté conectado a Internet?

Esto está más cerca de lo que parece, sin darnos cuenta vamos conectando cosas a Internet: los móviles, las cámaras de vigilancia, las televisiones, los coches, los contadores de la luz, los electrodomésticos, etc. Parece tan obvio que aprovechemos la accesibilidad que ofrece conectar todo a Internet que **el proceso de hiperconectividad se acelera.**

No solo nuestros datos corren peligro, sino nuestra **privacidad, nuestra intimidad y nuestra vida**. El riesgo de interconexión de cosas físicas va más allá de la información que nos puedan robar. Cuando conectamos ordenadores a Internet, nos pueden romper la confidencialidad de la información o como mucho tomar control de la cámara y tomar imágenes, usar nuestro equipo para atacar a otros o dañarlo. Sin embargo cuando son las cosas las que se conectan a internet, un acceso no deseado puede parar el dispositivo, o alterar su funcionamiento. Las cosas que se conectan a internet son sensores y actuadores. Estos, siendo comprometidos, **pueden detener el funcionamiento de una instalación o generar un mal funcionamiento,** que puede ser una infraestructura crítica, un aparato de electro medicina, una planta de generación de energía, una red de distribución de agua, un edificio inteligente, etc.

Nuestra vida con todo conectado a Internet será maravillosa si todos, usuarios, profesionales TIC, educadores, familias, universidades, empresas, administraciones, etc, nos concienciamos, nos ponemos como objetivo la ciberseguridad, valoramos la seguridad de las soluciones tecnológicas que elegimos y aprendemos a gestionar los riesgos.

Las tecnologías nos traen un mundo lleno de oportunidades que debemos aprender a usar de forma segura para poder aprovechar. Será necesario que los gobiernos tomen acuerdos para **la lucha contra el cibercrimen y la búsqueda de soluciones globales** a un problema que es global. Hará falta que suframos varios ataques a gran escala como el WannaCry para que estas necesidades vayan calando y que seamos conscientes de que **no podemos avanzar tecnológicamente siendo tan vulnerables.**

sets, cars, electricity meters, household appliances. It seems so obvious to take advantage of the accessibility of connecting everything to the Internet that **it accelerates the process of hyperconnectivity.**

Not only is our data at risk, but also our **privacy, our intimacy, and our lives.** The risks involved with connecting physical things go beyond the possible theft of information. When we connect computers to the Internet, our information privacy may be breached, or at the most, our webcams may be taken over and pictures taken without our consent, and even our computer itself can be used to attack or damage other computers. Now, when what is connected is not just a computer but a device, unauthorized access can stop that device or alter its functioning. The things that are connected to the Internet are devices such as sensors and actuators. When these are compromised, it **can bring an installation to a stop or cause it to malfunction**, and when that installation is a critical infrastructure, a piece of electromedical equipment, a power plant, a water supply network, an intelligent building, etc.

Our lives with full Internet connectivity will be wonderful if all of us - users, ICT professionals, educators, families, universities, companies, administration, etc - realize the importance of cybersecurity, make it our goal, value the security of the technological solutions we choose, and learn to manage risk.

Technologies bring us a world full of opportunities we must learn to use safely in order to take advantage of them. Governments will have to reach agreements **to fight against cybercrime and to look for solutions** to a problem that is global in scope. It may take several large-scale attacks like WannaCry for these needs to really sink in and for us to realize **we cannot advance technologically if we are so vulnerable.**

CTV COMPONENTES DE TRÁFICO VERTICAL

INGENIERÍA PARA ESPECIALISTAS DEL ASCENSOR

ENGINEERING FOR ELEVATOR SPECIALISTS

www.ctvlifts.com

20 AÑOS DE EXPERIENCIA
YEARS OF TRAVEL

DISEÑO Y FABRICACIÓN
DE ESTÁNDARES Y ESPECIALES
DESIGN AND MANUFACTURING
FOR STANDARD AND SPECIAL SOLUTIONS

SERVICIO DE POSTVENTA PROPIO
AFTER-SALES SERVICE

GESTIÓN INTEGRAL
ALL IN SERVICE

ASESORAMIENTO TÉCNICO
TECHNICAL APPRAISAL

EN SU PROPIO IDIOMA
COMMUNICATION IN YOUR OWN LANGUAGE

BÚSQUEDA DE MATERIAL
MATERIAL PROCUREMENT

Pol. Ind. La Huertecilla. C/Generación nº 44 29004 Málaga (España) T +34 952 20 71 66 F +34 952 20 32 91 e-mail ctv@ctvlifts.com

Nayar Systems Garaje, donde la innovación empieza jugando

Nayar Systems Garage, where innovation starts by playing

Como si de una habitación con multitud de bloques de construcción se tratara. Como si en lugar de tener asignadas solo unas pocas piezas, te dieran la oportunidad de tenerlas todas a tu disposición. Una habitación llena de ideas, de herramientas, de tiempo para crear, para jugar, para innovar. Porque **la innovación se basa en jugar con las tecnologías**, en experimentar y en verlo todo desde otras perspectivas diferentes a las cotidianas.

Nayar Systems Garaje es esa habitación llena de piezas donde jugar e innovar. Un departamento de la compañía Nayar Systems **dedicado exclusivamente a investigar**, a probar y a desarrollar, sin los marcados deadlines que exigen las tareas diarias y los proyectos destinados a satisfacer las necesidades de los clientes.

“La innovación se basa en jugar con las tecnologías, en experimentar y en verlo todo desde otras perspectivas”

Por lo tanto, **¿cuál es el objetivo principal de Nayar Systems Garaje?** No es otro que **aprender jugando.** Adquirir conocimientos que beneficien a toda la empresa. Se convierte en un spin-off de la marca matriz, erigiéndose como un departamento que se sale de la estructura más rígida de una empresa, dándole mayor libertad a un número determinado de trabajadores –máximo cuatro personas por proyecto– con ganas de innovar. Valga decir que, posiblemente,

As if it was a room with plenty of building blocks. As if instead of having just a few pieces, you were given the opportunity to have them all. A room full of ideas, of tools, of time to create, to play, to innovate. Because **innovation is based on playing with technologies**, on testing and watching things from other perspectives, different from the daily ones.

Nayar Systems Garage is that room full of pieces where one can play and innovate. It is a department in Nayar Systems Company **dedicated exclusively to researching**, to testing and developing, and without fixed deadlines required by daily routines and projects aimed at satisfying clients’ needs.

“Innovation is based on playing with technologies, on testing and watching things from other perspectivess”

Therefore, **what is the main objective of Nayar Systems Garage?** It is not other but **to learn by playing**. To acquire knowledge that will benefit the whole company. It becomes a spin-off of the original brand, a department out of the most rigid structure of a company, which gives more freedom to a certain number of employees –maximum four people per project- with interest for innovating. Probably, the fruit of continuous research will result in the birth of a new product that will get commercialised. However, it is an indirect and secondary objective that comes

el fruto de la continua investigación se traduzca en el nacimiento de un nuevo producto que pasará a ser comercializado, sin embargo, se trata de un objetivo indirecto y secundario, derivado intrínsecamente de la actividad natural del Garaje.

¿Cómo se trabaja en Nayar Systems Garaje? Pepe Aracil, CTO de la compañía y líder del departamento, cuenta que lo principal es tener un objetivo claro y una problemática que abordar. En base a ello, el siguiente paso es determinar con qué elementos o piezas hacer realidad ese objetivo y ahí ya entra el campo de investigación. Pepe asevera que cuando un trabajador tiene asignado un rol definido en una empresa, con plazos estipulados y una carga de trabajo importante, queda poco tiempo para jugar con la tecnología e innovar. **Y una empresa tecnológica, nunca puede perder la capacidad de innovar.**

“Lo principal es tener un objetivo claro y una problemática que abordar”

Por ello, Nayar Systems Garaje se compone por un grupo de personas motivadas y aisladas de atender al negocio de una forma directa. Personas con un amplio abanico de conocimientos, capaces de abordar todas las áreas del desarrollo. En una era donde el ser humano suele ser el eslabón más débil de la cadena cuando hablamos de seguridad y ciberseguridad, la compañía invierte sus recursos en fortalecer todos los canales de su sistema de información. Por ello, la seguridad en la nube de Nayar Systems está garantizada, porque la empresa pone todo **su know-how y experiencia de más de una década** en avalarla.

Los conocimientos que se adquieren gracias a la actividad del Garaje se transfieren a otros proyectos más veteranos, así como a la propia compañía. De este modo, **Nayar Systems se nutre transversalmente de ese departamento** dedicado exclusivamente a investigar y a innovar, para aplicar continuos desarrollos tecnológicos a los proyectos que componen sus firmas comerciales actuales. Cuando la actividad de un Garaje da comienzo, la compañía sabe que muchos proyectos no saldrán. Comercialmente, no son aplicables a corto plazo y muchos de ellos se quedan a las puertas de un lanzamiento comercial, pero aquel que sale, tiene las garantías suficientes para alcanzar el éxito. Una vez se inicia la comercialización del proyecto, este deja de depender del Garaje y el departamento se centra en otro producto que resuelva una nueva problemática.

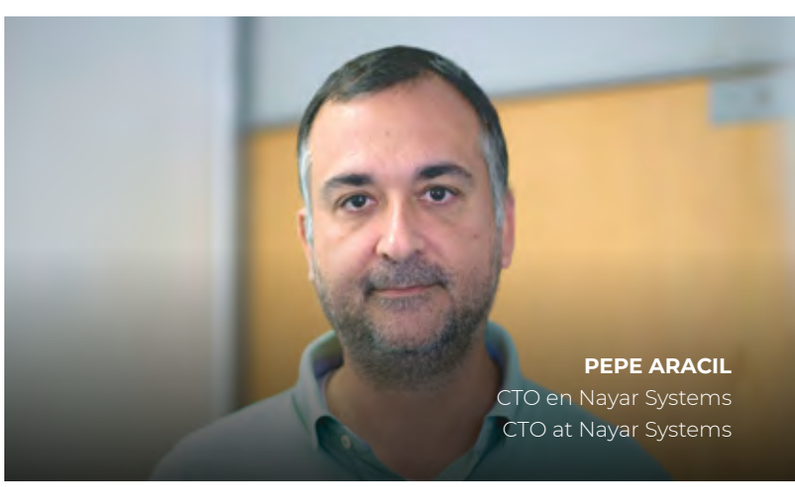
En el caso de Nayar Systems Garaje, se detectó una necesidad en las puertas que se abren con un mando, tanto a nivel de seguridad como de comodidad para el usuario. Por ello, todo el equipo ha investigado y desarrollado durante meses una solución

inherently from the natural activity of the Garage.

How do people work at Nayar Systems Garage? Pepe Aracil, the company’s CTO and the department’s leader, says that the main thing is having a clear objective and a problem to solve. Based on this, the next step is to determine which elements or pieces are needed to achieve that objective and here comes the research field. Pepe claims that when an employee has a clear role at the company, with stipulated deadlines and an important workload, there is little time to play with technology and innovate. **And a technological company can never lose its capacity to innovate.**

“The main thing is having a clear objective and a problem to solve”

For this reason, Nayar Systems Garage is composed of a group of motivated people who are cut off from taking direct care of the business. People with a wide range of knowledge, able to deal with all development areas. In an era when human beings are the weakest link in the chain regarding security and cybersecurity, the company invests its resources in strengthening all the channels of its information system. Thus, security in Nayar System’s cloud is guaranteed, because the company puts all **its know-how and more than ten-year experience** to guarantee it.



PEPE ARACIL
CTO en Nayar Systems
CTO at Nayar Systems

The knowledge acquired thanks to the Garage’s activity is transferred to older projects, as well as to the company itself. That way, **Nayar Systems is nourished crosswise from that department** dedicated exclusively to research and innovate in order to apply continuous technological developments to the projects that form their current commercial firms. When the activity of a Garage starts, the company knows that lots of projects will not turn out. They are not commercially applicable in the short term and many of them are left just before their commercial launch. But the project that gets launched has sufficient guarantee to be successful. Once the project

de apertura de puertas con el teléfono móvil, utilizando su tecnología bluetooth, dado que se trata de un dispositivo que siempre llevamos encima. De ahí nace **Virkey**. Un proyecto en el que se toca hardware, el chip ESP32 y donde se desarrolla una App que funciona con la misma base de código para IOS, Android y cualquier otro sistema operativo.

“Los conocimientos que se adquieren gracias a la actividad del Garaje se transfieren a otros proyectos más veteranos, así como a la propia compañía”

Pero Virkey también avanza a pasos agigantados hacia el sector del ascensor, donde Nayar Systems ha desarrollado su know-how durante sus más de diez años de trayectoria empresarial. Gracias a Virkey, las funcionalidades de una llave electrónica se incrementarán, permitiendo un acceso controlado para llegar al sótano, eliminando la llave física. Asimismo, se podrán restringir horarios determinados y cualquier movimiento quedará registrado en el teléfono móvil, disminuyendo a todos los niveles las posibilidades de acceso de individuos no conocidos mediante copias de llaves.

En una compañía como Nayar Systems, en la que el 80% de los beneficios se invierten en investigación y desarrollo, se evidencia la fuerte apuesta de la empresa por innovar en una red de comunicación segura que responda a las exigencias de sus públicos, y que se aplica continuamente en el desarrollo de su actividad empresarial. Nayar Systems invierte sus recursos en **hacer de lo ordinario algo extraordinario**, liderando la innovación y el conocimiento en soluciones de comunicación y conectividad tecnológica, con compromiso y transparencia.

commercialization is started, it stops depending on the Garage, and the department focuses on another product which solves another problem.

In the case of Nayar Systems Garage, a necessity was detected on the doors that get opened with a remote control, both at security level, as for the user’s convenience. Thus, during months the whole team has researched and developed a solution to open the doors with the mobile phone, using its Bluetooth technology, since it is something we always take along. This is where **Virkey** was born. It is a project where they worked with hardware and the chip ESP32 and developed an app that works with the same code base for IOS, Android and any other operating system.

“The knowledge acquired thanks to the Garage’s activity is transferred to older projects, as well as to the company itself”

But Virkey also moves by leaps and bounds towards the elevation sector, where Nayar Systems has developed its know-how during its more than ten years of business development. Thanks to Virkey, the functionalities of an electronic key will grow, thus letting a controlled access to the basement by getting rid of the physical key. Additionally, certain hours could be restricted and any movement would be registered in the mobile phone, what would reduce at all levels the possibility that unknown people get access with a copy of the keys.

In a company like Nayar Systems, in which 80% of the earnings are invested in research and development, it is clear the big bet of the company on innovating in a safe communication network that meets their audience’s requirements and that is continually applied to the development of its business activity. Nayar Systems invests its resources in **making the ordinary extraordinary**, being a leader in innovation and the knowledge of communication and technological connectivity solutions, with compromise and transparency.

SMART LIFTS

SMART LIFES

Primer dispositivo inteligente diseñado y fabricado íntegramente por Nayar Systems

First smart device
designed and manufactured entirely
by Nayar Systems

MAKE THE ORDINARY
EXTRAORDINARY

GSR

GSM SMART ROUTER

NAYARSYSTEMS | 72 horas M2M TECHNOLOGIES | ADVERTISIM | net4machines

info@nayarsystems.com · www.nayarsystems.com

El papel de la operadora móvil proporcionando seguridad en un ecosistema de IoT

The role of the mobile operator in providing security to the IoT ecosystem

SINOPSIS

Cuando pensamos en **"Internet de las cosas"** (IoT, por sus siglas en inglés), nos viene a la mente un conjunto interminable de servicios que tienen la capacidad de proporcionar importantes mejoras en nuestro día a día. El espíritu y la motivación impulsan el progreso, pero también es fundamental incluir la seguridad en las fases de diseño e implementación desde el principio, para evitar resultados inesperados y no deseados.

En Telefónica hemos lanzado una iniciativa centrada en la seguridad IoT, con el objetivo de **integrar la seguridad en nuestras propuestas de IoT**, y de esta manera, definir y construir una propuesta de valor de seguridad en IoT.

En este documento, explicamos cuál es el papel de una empresa de telecomunicaciones en el ecosistema del Internet of Things, centrándonos en las capacidades de seguridad que se pueden proporcionar y que se complementan con una solución innovadora que Telefónica ha desarrollado con la colaboración reciente de Amazon e Ikerlan.

MODELO DE SEGURIDAD DE IOT Y EL ROL DE MNO

Aunque las diferentes áreas involucradas en IoT tienen sus propias características particulares que deben analizarse específicamente, todas comparten

ABSTRACT

When we think about the **“Internet of Things”** we all bring to our minds an endless set of services that have the potential to make radical improvements in our life. It is the spirit and motivation that moves progress forward, but security must also be considered in its design and implementation from the very beginning to avoid unexpected and undesired outcomes.

In Telefónica we have launched an initiative focused on IoT Security aimed at **embedding security in our IoT proposals** and defining and building an IoT Security value proposition.

In this paper, we explain what is the role of a telco in the IoT ecosystem focusing on the security capabilities that can be provided and complemented with an innovative solution that Telefónica has developed in a recent collaboration with Amazon and Ikerlan.

IOT SECURITY MODEL AND THE ROLE OF A MNO

Although the different areas involved in IoT have its own particular features that need to be specifically analysed, they all share the need to provide network connectivity to these devices. For that, IoT platforms can help in processing the information the devices send and applying the needed actions.

la necesidad de proporcionar conectividad de red a los dispositivos. Para eso, las plataformas de IoT pueden ayudar a procesar la información que envían los dispositivos y aplicar las acciones necesarias.

En general, se acepta que el análisis de seguridad en profundidad requiera considerar cada Vertical específica, sin embargo, también es posible definir un modelo horizontal para establecer el marco común en el paradigma de IoT. La figura 1 representa el modelo de seguridad IoT basado en la propuesta de la GSMA, compuesto por tres elementos: puntos finales, redes y plataformas. Cada uno de estos elementos se analiza con más detalle en las siguientes secciones.

Hence, although it is generally accepted that an in-depth security analysis requires to consider each specific Vertical, it is possible to define a horizontal model to set the common framework for the IoT paradigm. Figure 1 represents an IoT security model based on the one proposed by the GSMA, composed by three elements: endpoints, networks and platforms. Each one of these elements are analysed with more detail in the next sections.

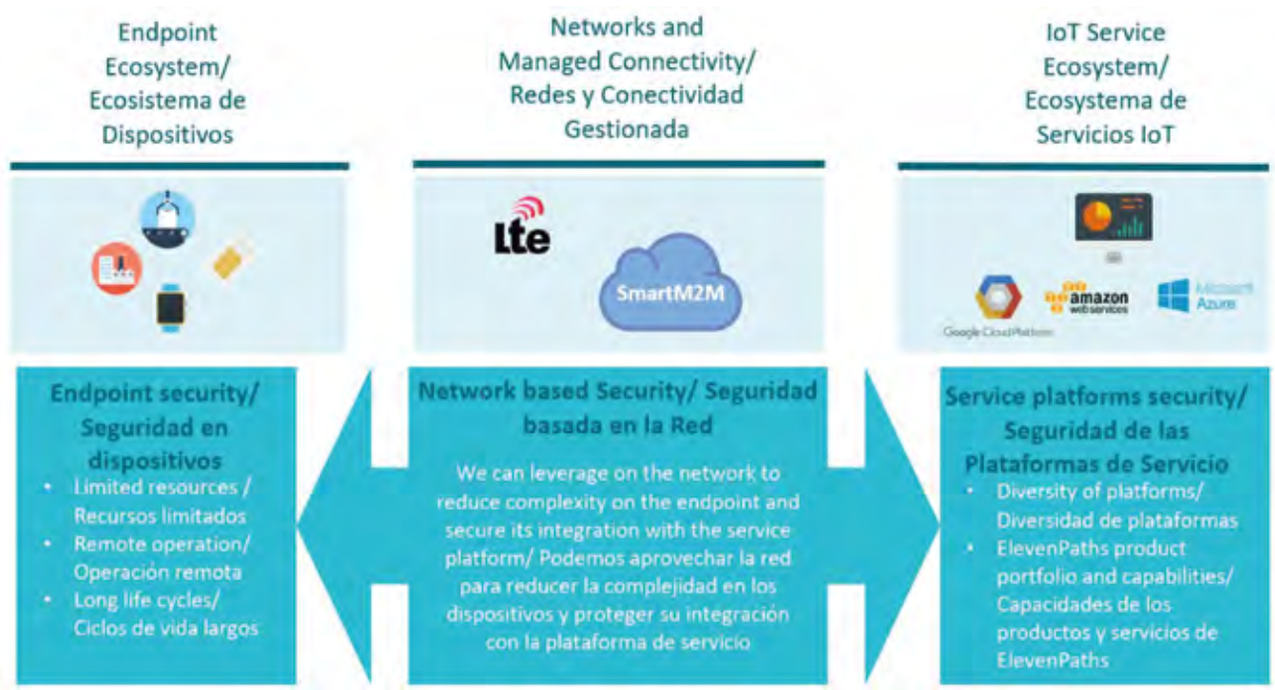


Figura 1. Modelo de Seguridad / Figure 1. Security Model

Dispositivos

En el ecosistema de IoT, uno de los extremos lo conforman los dispositivos IoT, que normalmente están geográficamente dispersos y envían información desde los sensores a la plataforma en el otro extremo, la cual ejecuta las acciones solicitadas. Desde una perspectiva de seguridad, los dispositivos tienen tres características de limitación clave que deben considerarse:

- Tienen **recursos de procesamiento y batería limitados**, lo que hace que agregar capacidades de seguridad (como cifrado de datos) sea más difícil.
- En la mayoría de los casos, **deben ser operados de forma remota**, lo que hace necesarios los

Endpoints

In the IoT ecosystem endpoints are IoT devices, which are normally geographically dispersed and usually send information from the sensors to the platform, that enforces its requested actions. From a security perspective, the endpoints have three key limiting features that must be considered:

- They have **limited processing and battery resources,** which makes adding security capabilities (such as data encryption) harder.
- In most of the cases **they must be remotely operated**, what makes necessary secure mechanisms for remote monitoring and management. In addition, most devices are physically accessible by an attacker which requires safe designs that harden the devices and protects them from physical manipulation.
- **Devices have long life cycles**, that could extend up to 10 years. This requires designing security mechanisms and procedures that can ensure the resiliency of the IoT infrastructure.

mecanismos seguros para la monitorización y la administración remota. Además, la mayoría de los dispositivos son accesibles físicamente por un atacante que requiere diseños seguros que fortalecen los dispositivos y los protegen de la manipulación física.
- **Los dispositivos tienen ciclos de vida largos**, que podrían extenderse hasta 10 años. Esto requiere diseñar mecanismos y procedimientos de seguridad que puedan garantizar la flexibilidad de la infraestructura de IoT.

Una ventaja desde el punto de vista de la seguridad es que los dispositivos IoT tienden a centrarse en aplicaciones muy específicas, a diferencia de lo que sucede con dispositivos multipropósito como teléfonos inteligentes o computadoras, lo que simplifica el perfilado de los dispositivos IoT y, por lo tanto, la detección de anomalías.

"Es fundamental incluir la seguridad en las fases de diseño e implementación desde el principio, para evitar resultados inesperados y no deseados."

Plataformas de servicio

En el otro extremo del modelo, tenemos las plataformas en la nube, las cuales han agregado muchas características y capacidades para **facilitar la interacción con dispositivos de IoT y el desarrollo de servicios**. Actualmente, existe una gran diversidad de plataformas, cuyos principales representantes son Amazon Web Services (AWS), Google Cloud Platforms, IBM Bluemix, Microsoft Azure y Telefónica Open Cloud.

Además de la diversidad entre ellos, que obliga a los desarrolladores e ingenieros a definir diferentes mecanismos de seguridad, existen pocos mecanismos de seguridad que se apoyen en las capacidades de red para las infraestructuras de IoT. Fortalecerlas podría simplificar y mejorar su implementación y configuración. De hecho, estas tareas se pueden hacer desde la red.

Red

La red es la pieza que está el medio de este esquema y **hace posible la comunicación entre los dispositivos y los servicios de IoT**. Es un elemento clave ya que podemos aprovecharlo para reducir la complejidad en el dispositivo y proteger su integración con la plataforma de servicio.

Es allí donde los operadores de red móvil (MNO)

An advantage from the security point of view is that IoT devices tend to focus on very specific applications, multipurpose devices such as smartphones or computers, which simplifies the profiling of the device and, hence, the detection of anomalous activity.

"Security must also be considered in its design and implementation from the very beginning to avoid unexpected and undesired outcomes."

Service platforms

On the other side of the model we have the cloud platforms that have added many features and capabilities **to facilitate the interaction with IoT devices and the development of services**. Currently, there is a great diversity of platforms, whose main representatives are Amazon Web Services (AWS), Google Cloud Platforms, IBM Bluemix, Microsoft Azure and Telefónica Open Cloud.

Apart from the diversity among them, which forces developers and engineers to define different security mechanisms, there are few security mechanisms leveraged on network-capabilities for IoT infrastructures. Reinforcing them could simplify and enhance its implementation and configuration. These tasks could be done from the network.

Network

The network is the piece in the middle of this scheme and **it makes possible the communication between endpoints and IoT services**. It is a key element since we can leverage on it to reduce complexity on the endpoint and secure its integration with the service platform.

There is where Mobile Network Operators (MNOs) can provide a key differential value. Communication network components are inherent to IoT, furthermore, they are built over standards (e.g. LTE), where 'security by design' has been one of its key principles. Both facts set a strong foundation for enabling **MNOs as providers of compelling e2e security propositions** that extend their core security capabilities.

Some of the **key security features** required for IoT are:

- **Identification and authentication** of the devices involved in the IoT Service.
- **Access control** for the different devices that need to be connected to create the IoT Service.

pueden proporcionar un valor diferencial clave. Los componentes de la red de comunicación son inherentes a IoT, además, están construidos sobre estándares (por ejemplo, LTE), donde la "seguridad por diseño" ha sido uno de sus principios clave. Ambos hechos establecen una base sólida para situar a los **MNO como proveedores de soluciones de seguridad end-to-end** convincentes que amplían sus capacidades de seguridad básicas.

Algunas de las **características clave de seguridad** requeridas para IoT son:

- **Identificación y autenticación** de los dispositivos involucrados en el servicio IoT.
- **Control de acceso** para los diferentes dispositivos que deben conectarse para crear el servicio IoT.
- **Protección de datos** para garantizar la seguridad (confidencialidad, integridad, disponibilidad, autenticidad) y la privacidad de la información transmitida por la red del Servicio IoT.
- **Procesos y mecanismos para garantizar la disponibilidad** de los recursos de la red y protegerlos contra los ataques.
- **Monitorización y análisis** de comunicaciones para detectar actividad anómala.

En cuanto a la identificación y autenticación, Telefónica ha desarrollado una solución innovadora que permite identificar de forma segura dispositivos IoT que se conectan con plataformas en la nube. Esta solución se describe en la siguiente sección.

PROTECCIÓN DE LA CONEXIÓN A LOS SERVICIOS EN LA NUBE CON LA TARJETA SIM

En una red móvil, los dispositivos se identifican usando el IMSI (identificador del suscriptor) y / o IMEI (identificador del dispositivo). Actualmente se utiliza para administrar esos dispositivos con fines de conectividad gestionada, pero también se puede proporcionar administración de identidades del dispositivo desde el acceso a la plataforma (por ejemplo, usando certificados digitales), lo cual simplifica la administración del dispositivo, no solo en un nivel de conectividad de red, sino también en un IoT nivel de servicio.

De hecho, en Telefónica hemos desarrollado una solución que proporciona de forma segura un certificado digital en la tarjeta SIM de un dispositivo IoT. El dispositivo usa el certificado para autenticarse en una plataforma en la nube. En la implementación actual esta plataforma es AWS IoT.

Aunque el provisionamiento de un certificado por dispositivo es una buena solución para la autenticación de dispositivos, la mayoría de las empresas no

- **Data protection,** in order to guarantee the security (confidentiality, integrity, availability, authenticity) and privacy of the information carried by the network for the IoT Service.
- **Processes and mechanisms to guarantee availability** of network resources and protect them against attack.
- **Communications monitoring** and analytics for detecting anomalous activity.

SECURING THE CONNECTION TO CLOUD SERVICES WITH THE SIM CARD

In a mobile network, endpoints are identified using IMSI (identifier of the subscriber) and/or IMEI (identifier of the device). That is currently used for managing those devices for managed connectivity purposes, but leveraged on that, device identity management from platform access can also be provided (e.g. using digital certificates), simplifying device management not just at a network connectivity level but also at an IoT service level.

In fact, in Telefónica we have developed a solution that securely provisions over the air a digital certificate in the SIM card of an IoT device. The device uses the certificate to authenticate in a cloud platform which in the current implementation is AWS IoT.

Although provisioning one certificate per device is a good solution for device authentication, most companies do not have the capabilities to do it securely in scale and sometimes implement insecure and manual credential bootstrapping processes. Using the SIM card as a secure hardware for storing the credentials can help in overcoming those difficulties. In addition, the X.509 certificate can be securely delivered using an OTA (Over-The-Air) provisioning platform.

Those two key elements (SIM card as a secure hardware and OTA platform for certificate delivery) are the basis of the recently implemented solution, which provides significant improvements to current credential provisioning mechanisms as it can massively deliver X.509 certificates to end devices in a cost-effective way.

These are the steps of the whole process that are also represented in the dashboard showed in Figure 2 :

- **Step 1: Device starts bootstrapping**. Before this step the device has no credentials and it is powered off. When it starts bootstrapping, it detects that there is no credentials and requests them to the Telefónica bootstrapping server.
- **Step 2: Smart m2m performs network identification**.

cuentan con las capacidades para hacerlo de forma segura en escala y, a veces, implementan procesos de arranque con credenciales inseguros y manuales. Usar la tarjeta SIM como un hardware seguro para almacenar las credenciales, puede ayudar a superar esas dificultades. Además, el certificado X.509 se puede entregar de forma segura utilizando una plataforma de provisionamiento OTA (Over-The-Air).

Esos dos elementos clave (tarjeta SIM como hardware seguro y plataforma OTA para la entrega de certificados) son la base de la solución implementada recientemente, que proporciona mejoras significativas a los mecanismos de provisionamiento de credenciales actuales, ya que puede entregar certificados X.509 a dispositivos finales de manera rentable.

Estos son los pasos de todo el proceso que también están representados en la interfax que se muestra en la Figura 2:

- **Paso 1: el dispositivo inicia el arranque.** Antes de este paso, el dispositivo no tiene credenciales y está apagado. Cuando se inicia el arranque, se detecta que no hay credenciales y las solicita al servidor de arranque de Telefónica.
- **Paso 2: la plataforma Smart m2m realiza la identificación de la red**. El dispositivo se identifica por su IP y, a partir de ella, se solicitan los detalles de la SIM y del dispositivo a la plataforma de conectividad gestionada Smart m2m de Telefónica.

The device is identified by its IP and based on it, SIM and device details are requested to the Telefónica Smart m2m managed connectivity platform.

- **Step 3: Device is registered at AWS IoT.** The SIM details are used to register the device on AWS IoT and create its credentials (X.509 certificate), that will provide access to the device only to its AWS Thing Shadow.
- **Step 4: Digital certificate is sent to the SIM.** The credentials are sent to the SIM card through a secure data channel and stored in the SIM file system. The digital certificate provides access to the device only to its AWS Thing Shadow. The device reports data every 2 seconds.

In particular, this process has been implemented in a scenario with the following elements:

- **An energy meter** that measures the power consumption of a lamp.
- **The energy meter** is connected to a device that provides 3G M2M connectivity and that has the SIM card where credentials are received.

This solution, among others, is part of the proposal that Telefónica has in relation to IoT Security. One of its innovative features is that it requires no proprietary capabilities on the SIM card (they just need to be Release 6), therefore it is suitable for any IoT SIM card from Telefónica. Additionally, the SIM does not need to implement encryption. This solution is based on standard 3GPP technology and it works on any device that supports standard AT commands.

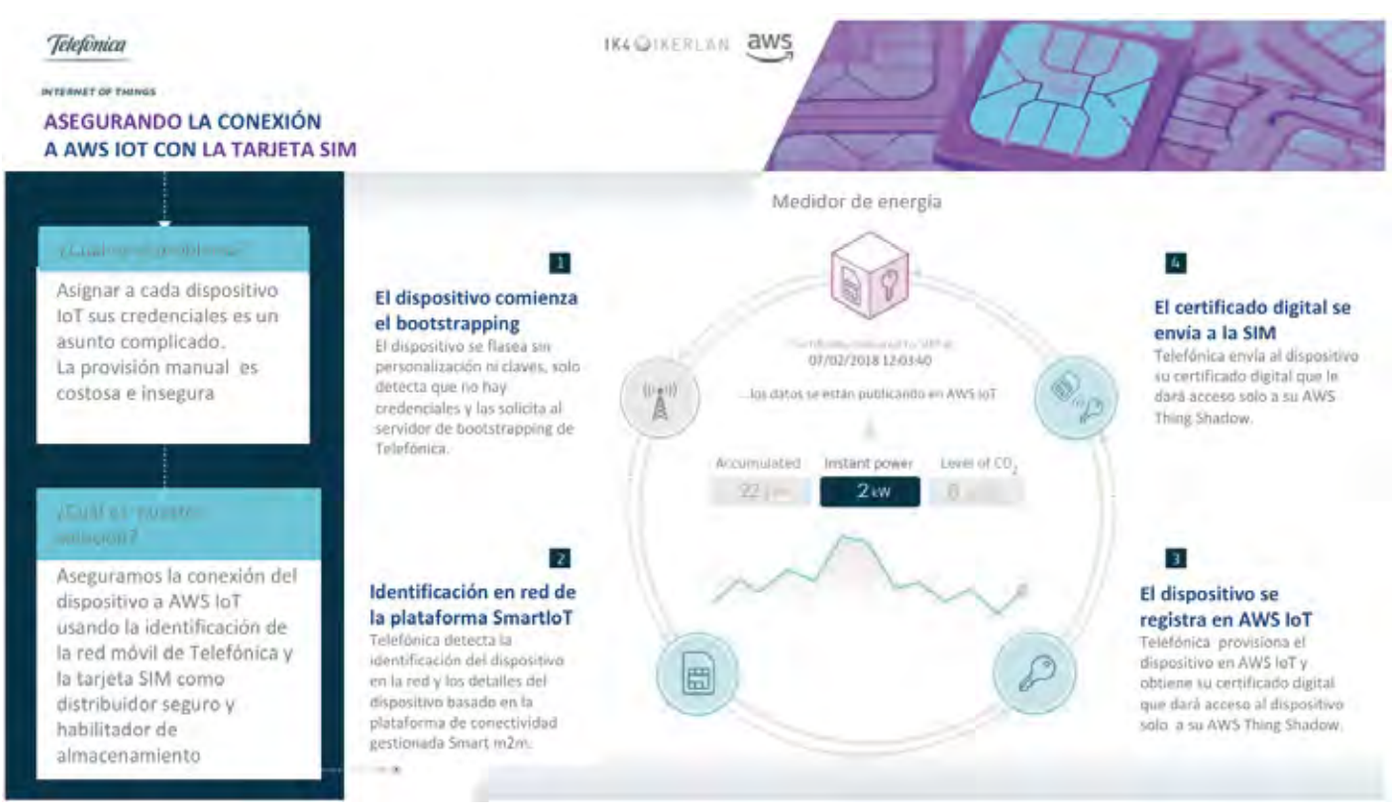


Figura 2 Interfaz con los pasos del proceso para provisionar el certificado en la tarjeta SIM.

Figure 2 .Dashboard with steps of the process for provisioning the certificate in the SIM

- **Paso 3: el dispositivo está registrado en AWS IoT**. Los detalles de la SIM se utilizan para registrar el dispositivo en AWS IoT y crear sus credenciales (certificado X.509), que proporcionará el acceso al dispositivo solo al Shadow del dispositivo en AWS.
- **Paso 4: el certificado digital se envía a la tarjeta SIM.** Las credenciales se envían a la tarjeta SIM a través de un canal de datos seguro y se almacenan en el sistema de archivos SIM. El certificado digital proporciona acceso al dispositivo solo al Shadow del dispositivo de AWS. El dispositivo envía datos cada 2 segundos.

En particular, este proceso se ha implementado en un escenario con los siguientes elementos:

- **Un medidor de energía** que mide el consumo de energía de una lámpara.
- **El medidor de energía** está conectado a un dispositivo que proporciona conectividad 3G M2M y que tiene la tarjeta SIM donde se reciben las credenciales. La Figura 3 muestra la consola que contiene estos elementos.

Esta solución, entre otras, es parte de la propuesta que tiene Telefónica en relación con seguridad en IoT. Una de sus características innovadoras es que no requiere elementos propietarios en la tarjeta SIM (solo necesitan ser versión 6), por lo tanto, puede utilizarse con cualquier tarjeta SIM IoT de Telefónica. Además, la tarjeta SIM no necesita tener capacidades criptográficas. Esta solución se basa en la tecnología 3GPP estándar y funciona en cualquier dispositivo que admita comandos AT estándar.

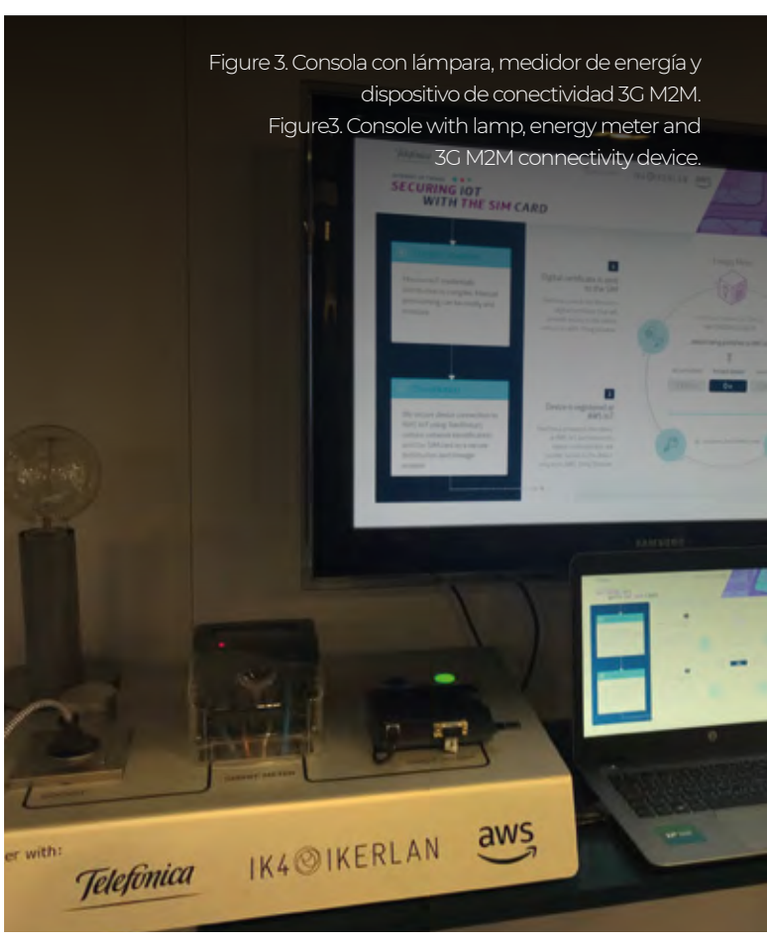


Figure 3. Consola con lámpara, medidor de energía y dispositivo de conectividad 3G M2M.
Figure3. Console with lamp, energy meter and 3G M2M connectivity device.

Entrevista a Darío Vicario: “Pantallas multimedia: un paso más hacia la digitalización de la industria de la elevación”

Interview with Darío Vicario: “Multimedia screens: one more step topwards the digitalisation of the elevator industry”

En 2016 thyssenkrupp presentó MAX, la solución para el Internet de las Cosas diseñada con Microsoft Azure, que **combina big data, la nube e inteligencia artificial para predecir posibles fallos del ascensor**. Con MAX, cerca de 24.000 técnicos irán teniendo en sus manos toda la información necesaria para poder realizar su trabajo de la forma más eficiente. En thyssenkrupp se siguen dando pasos en pro de renovar e innovar el sector y propiciar que las nuevas tecnologías sean una realidad para sus clientes, ahora, con las Pantallas Multimedia para ascensores.

In 2016, thyssenkrupp presented MAX, the solution for the Internet of Things designed with Microsoft Azure, **combining big data, cloud and artificial intelligence for predicting potential elevator faults**. With MAX, around 24,000 technicians will have all the information they need at their fingertips to ensure that tasks are carried out as efficiently as possible. At thyssenkrupp, progress is still being made with the aim of upgrading and innovating the sector and ensuring new technologies are a reality for its customers, now, with the Multimedia Screens for elevators.

MAX como sistema de mantenimiento predictivo, ha sido una de las grandes revoluciones en el sector de elevación, pero ¿se trata de una solución de hoy?

MAX es el primer sistema de mantenimiento predictivo en tiempo real de ascensores y escaleras mecánicas en el mundo, que efectivamente ya es una solución de hoy. Este nuevo servicio que hemos puesto en marcha supone un salto cualitativo en la seguridad y disponibilidad de los ascensores. Con MAX hemos conectado más de **110.000 ascensores en todo el mundo a la nube**, para transmitir y almacenar la información que estos producen. Analizando todos estos datos podremos adelantarnos a las averías, hacer un mantenimiento optimizado y dar un mejor servicio a nuestros clientes.

MAX, as a predictive maintenance system, has been one of the great revolutions in the elevator sector, but, is it a system for today's world?

MAX is the first real-time, predictive maintenance system for elevators and escalators in the world and it is indeed already a solution today. This new service we have launched represents a quantum leap in terms of elevator safety and availability. With MAX we have **connected over 110,000 elevators worldwide to the cloud**, to transmit and store information generated by these. By analysing all these data, we can predict faults, provide an optimised maintenance service and offer our customers a better service.

A través del "Internet de las Cosas", nuestra solución **reduce el tiempo de inactividad** del ascensor con diagnósticos a tiempo real, y es capaz de **predecir problemas de mantenimiento antes de que ocurran**, avisando de la necesidad de sustituir componentes antes del final de su ciclo de vida.

Through the Internet of Things, our solution **reduces the inactivity time** of the elevator, delivering real-time diagnostics, and capable of **predicting maintenance problems before they occur**, by indicating the need to replace components before the end of their lifecycle.

Es un gran avance ¿Cuáles son los beneficios para sus clientes y los usuarios de los ascensores que están dotados de MAX?

El consumo de energía urbana no para de aumentar y lo seguirá haciendo en los próximos años. El ascensor mismo, supone hasta un 10% del consumo energético total de un edificio. Con el lanzamiento en España de la tecnología MAX uno de los beneficios que perciben nuestros clientes, es una aportación de eficiencia, porque mejora su disponibilidad y **ayuda a economizar el consumo energético de los edificios y reduce la huella de CO2.** Para nosotros es una gran satisfacción poder aportar un plus por la sostenibilidad, con la que estamos muy comprometidos.

It is a huge step forward, what are the benefits for your customers and for users of elevators equipped with MAX?

There is a growing trend in urban energy consumption and this will continue be the case in the years to come. The same occurs with elevators, it accounts for up to 10% of a building's total energy consumption. With the launch of the MAX technology in Spain, one of the benefits our customers can enjoy is greater efficiency since it delivers maximum elevator availability and **helps control the energy consumption of buildings and reduces carbon emissions**. We are extremely proud to be able to contribute towards greater sustainability, to which we are strongly committed.

Hemos visto que recientemente han lanzado un nuevo producto, relacionado con la digitalización, las Pantallas Multimedia para ascensores.

Efectivamente, hemos lanzado esta nueva solución para modernizar y llevar el parque actual de ascensores al siglo XXI y ofrecer una plataforma de contenidos personalizables por los propietarios. Esta iniciativa, que se suma a MAX, refuerza el objetivo de llevar a los ascensores a nueva era, más acorde con las ciudades del mañana.Hemos presentado recientemente en el mercado español las nuevas **Pantallas Multimedia conectadas**. Con ellas, los propietarios de los ascensores, podrán mostrar y difundir contenidos e información a tiempo real en las cabinas de los ascensores, permitiendo a los usuarios visualizarlos, mientras viajan en el ascensor.

Pantalla Multimedia de Thyssenkrupp
Multimedia screen by Thyssenkrupp

We saw recently that you launched a new product related to digitalisation, Multimedia Screen for elevators.

That's right, we launched this new solution to modernise and bring the current fleet of elevators into the 21st century and offer a platform of customisable contents for owners. This initiative, together with MAX, strengthens the aim of propelling elevators into the new era, in accordance with the cities of tomorrow. We recently presented the new **connected Multimedia Screen** in the Spanish market. With these, elevator owners will be able to display and disseminate contents and information in real time in the elevator cars, enabling users to view them while travelling in the elevator.

¿A quién se dirigen las Pantallas Multimedia?

Al parque de ascensores existente, pero nuestros nuevos ascensores también contarán con las Pantallas Multimedia, como opción a elegir por el cliente. De los más de 880.000 ascensores instalados en España, un 50% de ellos tiene una antigüedad superior a 20 años, siendo en muchos casos objeto de remodelaciones parciales que permiten alargar la vida del ascensor y modernizar sus funciones, seguridad y diseño. A través de esta nueva iniciativa, thyssenkrupp quiere modernizar el parque actual de ascensores en España para llevarlo a una era más digital, ya que esta solución es apta de instalarse en ascensores ya existentes, conectándolos a través de una red wifi o por tarjeta 3G. A través de un gestor de contenidos, el **propietario o administrador del edificio puede personalizar toda la información**

Who are the Multimedia Screens aimed at?

Pantalla Multimedia de Thyssenkrupp
Multimedia screen by Thyssenkrupp

en base a sus necesidades, permitiéndole también publicar sus propios contenidos, tanto multimedia como noticias, avisos, promociones, etc., El sistema permite su actualización en cualquier momento a través de un Smartphone o una Tablet.

Los mayores beneficiarios de las pantallas serán sin duda los usuarios de los ascensores, pero creemos que clientes como: hoteles, centros comerciales, aeropuertos, metros, edificios de oficinas y comunidades de propietarios, encontrarán en nuestras Pantallas Multimedia, un nuevo canal de comunicación muy interesante, con sus propios clientes.

¿Qué es lo que espera thyssenkrupp de esta nueva aportación a la digitalización?

España es el **quinto mercado mundial en la industria del ascensor**, por lo que es un escenario idóneo para introducir las novedades que hacen que thyssenkrupp lleve el ascensor del futuro un paso por delante. Con esta nueva innovación, sumada a las posibilidades que ofrece MAX, estamos un paso más cerca de digitalizar nuestra industria y ser los primeros en dotar a nuestros clientes, de sistemas adaptados a las nuevas tecnologías.

www.thyssenkrupp-elevator.com/es
@thyssenkruppES

The existing fleet of elevators, but our new elevators will also be equipped with Multimedia Screens, as an option for clients.

Of the 880,000+ elevators installed in Spain, 50% of them are over 20 years old and many have very often undergone refurbishment works to extend the lifecycle of the elevator and modernise their functions, safety and design. With this new initiative, thyssenkrupp wants to update the existing fleet of elevators in Spain to bring it into a more digital era, since this solution can be installed in existing elevators, by connecting them to a Wi-Fi network or via a 3G card.

Through a content manager, **the owner or administrator of the building can customise all the information according to their needs** and also publish their own contents, including multimedia and news, notifications, promotions, etc. The system can be updated at any point via a Smartphone or Tablet.

The main beneficiaries of the screens will without doubt be the elevator users, but we think other customers such as: Hotels, Shopping Centres, Airports, Undergrounds, Office Buildings and communities of owners, will find that our Multimedia Screens offer them a very interesting new communication channel with their own customers.

What does thyssenkrupp expect from this new contribution to digitalisation?

Spain is the **fifth market worldwide in the elevator industry**, therefore it is the ideal setting to introduce innovations that enable thyssenkrupp to be at th forefront of the development of the elevator of the future. With this innovation, together with the possibilities offered by MAX, we will be one step closer to digitalising our industry and being the first to provide our customers with systems adapted to new technologies.

www.thyssenkrupp-elevator.com
@thyssenkruppES

Tecnología para tus sentidos.

Pantalla multimedia

La pantalla multimedia para ascensores es un canal de comunicación que aporta un valor añadido a usuarios y clientes de hoteles, centros comerciales, edificios residenciales, centros de salud o empresas, ofreciendo información en tiempo real.

T: 901020909 · servicliente@thyssenkrupp.com
www.thyssenkrupp-elevator.com/es
@thyssenkruppES

engineering.tomorrow.together.

thyssenkrupp

Ciberseguridad en el mundo IoT

Cybersecurity in the world of IoT

El internet de las cosas forma ya parte de la vida cotidiana de las personas: Hogares inteligentes, wearables, coches que se comunican con la nube, ascensores conectados, etc. Cada vez más dispositivos hacen uso de esta tecnología, formando parte de una **transformación digital sin precedentes**, que nos convertirá en una sociedad digital hiperconectada.

Los beneficios de esta revolución del IoT son innumerables: desde la mejora de la experiencia de los usuarios con los productos conectados, hasta la reducción de los costes de los procesos industriales y de mantenimiento.

Pero esta nueva realidad de equipos interconectados **también plantea nuevos retos**, que deben tenerse en cuenta a la hora de adoptar esta tecnología como parte de un producto. El mayor de todos ellos, para todos estos dispositivos y sistemas en la nube, es la **ciberseguridad.**

“Esta nueva realidad de equipos interconectados también plantea nuevos retos, que deben tenerse en cuenta a la hora de adoptar esta tecnología”

Según datos del informe “Risk or reward: What lurks within your IoT?” de KPMG, en el año 2020 se estima que habrá 20 billones de dispositivos conectados. Cada uno de estos dispositivos conectados, supone un punto de vulnerabilidad para una empresa, pudiendo exponer, en algunos casos, datos de usuarios o del propio negocio que supondrían un impacto muy negativo para la propia empresa.

The Internet of Things today forms part of our everyday lives: smart homes, wearables, cars communicating with the cloud, connected lifts, etc. More and more devices are using this technology, forming part of an **unprecedented digital transformation** that will turn us into a hyper-connected digital society.

There are numerous benefits to this IoT revolution, from the improvement of the user experience with connected products to the reduction of costs in industrial and maintenance processes.

But this new reality of interconnected equipment **also brings new challenges** which must be borne in mind when embracing this technology as part of a product. And for all these cloud-based systems and devices, the greatest challenge of all is **cybersecurity**.

“This new reality of interconnected equipment also brings new challenges which must be borne in mind when embracing this technology”

According to the report by KPMG, “Risk or reward: What lurks within your IoT?”, by the year 2020, there will be 20 billion devices connected. Each one of these connected devices represents a vulnerability in a company, which in some cases could expose user data or the business itself, causing a very negative impact on the company.

Algunas de las prácticas más habituales que llevan a acentuar los riesgos de la tecnología IoT, se pueden resumir en los siguientes puntos:

1. **Equipos con recursos limitados o bajo coste.** Dispositivos con capacidad de procesamiento baja, y que por tanto no son capaces de implementar los mecanismos habituales de seguridad avanzada para conexión a internet. En muchos casos los fabricantes de los dispositivos conectados priman la eficiencia y el coste frente a la seguridad.

2. **Diseños de red complejos e inseguros**: Cada vez resulta más sencillo conectar cualquier dispositivo a la nube. Este hecho hace que cada vez más empresas emprendan este camino sin contar con el asesoramiento adecuado, y que llevan a diseños de soluciones potencialmente inseguros.

3. **Fallos de seguridad en el diseño de los dispositivos y en su explotación:** Primar el "time to market" de los equipos a la seguridad. Acceso de terceros a los datos a través de portales de internet no seguros, o políticas de gestión de claves de usuario inadecuadas.

Todos estos puntos, y muchos más, son ampliamente conocidos en el sector del internet de las cosas y pueden solventarse de forma adecuada acudiendo a un principio fundamental: "Secure by Design".

Para MP, ese principio fundamental ha estado presente en todas las etapas del diseño de su plataforma **"MP Connected Lifts**" y de su nueva maniobra de ascensor MP ecoGO, diseñada para proporcionar un **alto nivel de conectividad y un tele-mantenimiento avanzado.**

Desde el equipo de comunicaciones que se coloca en el ascensor, hasta el diseño de la red de comunicaciones, MP ha contado con el asesoramiento y la colaboración de empresas o instituciones expertas en el sector de las comunicaciones, tales como Telefónica o la Escuela superior de Ingenieros de Sevilla, entre otras.

MP pone a disposición de sus clientes el acceso al mundo IoT a través de su plataforma **"MP Connected Lift" con una solución potente, segura y en continua evolución**, que permitirá adentrarse en este mundo obteniendo todas las ventajas y sin estar expuestos a ninguno de los riesgos.

Some of the habitual practices which could exacerbate the risks of IoT technology are:

1. **Low-cost or low-capacity equipment:** devices with a low processing capacity and which, therefore, cannot implement the usual advanced security measures for Internet connection. In many cases, the manufacturers of connected devices prioritise efficiency and cost over security.

2. **Complex, insecure network design:** it is ever simpler to connect any device to the cloud. This means that companies increasingly take this option without seeking the necessary advice, which leads to solutions with potentially insecure designs.

3. **Security defects in the design of devices and in their use:** prioritising the "time to market" of security equipment. Access by third parties to data through insecure Internet portals or inadequate user password management policies.

All of these points, and many more, are widely recognised in the Internet of Things sector and can be adequately resolved by applying a fundamental principle: "Secure by Design".

For MP, this fundamental principle has been present in every stage of the design of our "**MP Connected Lift"** platform and our new lift controller, the MP ecoGO, desgined to provide a **high level of connectivity and an advanced remote maintenance.**

In everything, from the communications equipment installed in the lift, to the design of the communications network, MP has sought the advice and collaboration of expert companies and institutions from the communications sector, including Telefónica and the University of Seville, among others.

At MP, we bring access to the world of IoT to all of our clients through our "**MP Connected Lifts" platform, with a powerful, secure solution which is in constant evolution**, and which will bring all of the benefits of this world, without being exposed to any of the risks.

La seguridad en el IoT: “Protege lo importante porque no vas a poder proteger todo”

Security in IoT: “Protect what is important because you will not be able to protect everything”

JAVIER ANAYA | Actualmente, el término **Internet de las cosas**, IOT (Internet Of Things) se usa para definir un modelo de conexión avanzada de dispositivos, sistemas y servicios que va más allá del tradicional M2M (máquina a máquina), cubriendo una amplia variedad de protocolos de comunicaciones.

Según fuentes de la **CNMC** de hace escasamente unas semanas, hay **5,5 millones de dispositivos M2M conectados en la actualidad en España.** Este sector crece a un ritmo superior al 10% anual y se espera que alcance un volumen de unos 8 millones de conexiones en 2021. No obstante, la eclosión de la tecnología IoT está haciendo que estos números se queden pequeños. La gran cantidad de sensores, medidores, señalizaciones y demás dispositivos que se plantean a día de hoy conectados con nuestros sistemas de gestión son innumerables y hacen muy difícil la previsión de “número de conexiones” al respecto.

La aparición de **tecnologías “baratas”** que facilitan conexiones y comunicaciones está haciendo que se produzca un aluvión de empresas dedicadas a favorecer la gestión de este tipo de dispositivos. Dispositivos económicamente muy accesibles, sobre comunicaciones económicamente bajas y con tiempos de fabricación, puesta en marcha y despliegue muy bajos.

El **binomio riego-beneficio** que está presente siempre en todas las decisiones de inversión, debe cambiar inevitablemente, en este nuevo escenario donde tecnología y comunicaciones tienen un papel tan

JAVIER ANAYA | The term **Internet of Things** (IoT) is currently used to define an advanced connection model for devices, systems and services that goes beyond the traditional M2M (machine to machine), and it covers a wide range of communication protocols.

According to the **National Commission on Markets and Competition**, there are at present **5.5 million M2M devices connected in Spain**. This sector is growing more than a 10% yearly and it is expected to reach 8 million connections in 2021. However, the blooming of IoT technology is making these numbers small. The great amount of sensors, metres, indicators and other devices thought to be connected nowadays with our management systems are countless, and make very difficult to predict the number of connections.

The appearance of **“cheap” technologies** that facilitate connections and communications is generating a deluge of companies dedicated to favour the management of this kind of devices. Devices that are very accessible economically, over economically low communications and with very short production, implementation and display times.

The **pairing *risk-benefit***, which is always present in every investment decision, must change inevitably, in this new scenario where technology and communications play so important a role, for that of ***security-price.***

When deploying IoT services, **the security system associated to these devices and communications is**

importante, por el de **seguridad-precio.**

A la hora de desplegar servicios IoT **no se está teniendo en cuenta el sistema de seguridad asociado a estos dispositivos** y a estas comunicaciones. Se está dando más importancia al precio de los dispositivos y la facilidad de puesta en marcha que a su seguridad y, sí, hay muchos dispositivos, a priori, poco "atacables", poco hackeables... vamos, con muy poco interés, en acceder a ellos: La temperatura de tu frigorífico, los dispositivos de riego de tu jardín, etc.

"El binomio riego-beneficio, que está presente siempre en todas las decisiones de inversión, debe cambiar inevitablemente [...] por el de seguridad-precio"

El propio ascensor de una comunidad de vecinos parece un objetivo poco atractivo para "los malos", no obstante... **desactivar 150 ascensores y pedir un "rescate" a cambio de devolverlos a la vida** ya no parece tan "raro". La imagen de la empresa ante los clientes que les deja sin ascensor durante un tiempo, la potencial pérdida de esos clientes, aparte del propio pago de ese rescate, es decir, la propia violencia que genera un soborno de este estilo, son un problema verdadero para cualquier firma de asistencia de ascensores. Por no hablar de ascensores en instalaciones sensibles a acciones de más repercusión (centros comerciales, edificios públicos, instalaciones críticas, etc) donde **hasta el terrorismo tiene cabida.**

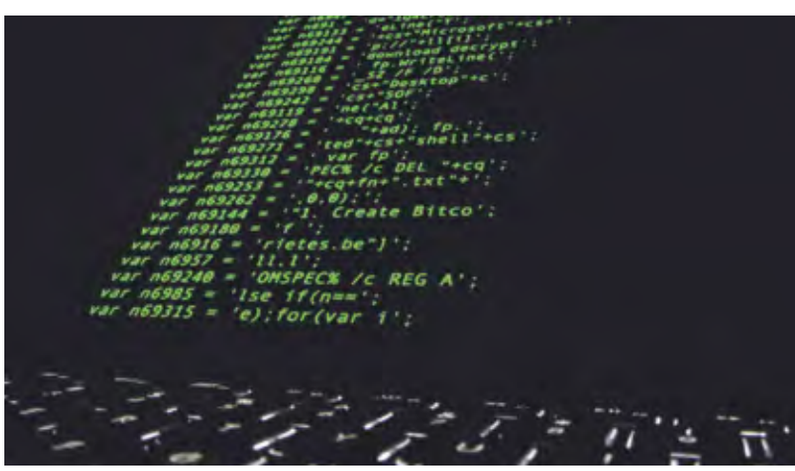
El **Ransomeware** es la técnica de cibercrimen más extendida a lo largo de todo el planeta. Sólo en España se detectaron **unos 20.000 casos en 2017**. En cuanto al **ciberterrorismo,** parece evidente que tiene un objetivo claro en este tipo de sistemas dentro de instalaciones críticas o de gran repercusión. De esta clase de ciberdelincuencia **no hay ni siquiera datos publicados**, aunque sí muchas referencias y mucha rumorología.

La propuesta de los operadores de telecomunicaciones debe ir en consonancia no sólo con el despliegue de sistemas sino también con la seguridad de esas redes. La vulnerabilidad de los sistemas se está asociando siempre a malas prácticas o falta de ellas respecto de los empleados, o a la falta de actualizaciones del sistema operativo o de los dispositivos firewall de las empresas. **Perdemos de vista, a su vez, que hay cientos de miles de rastreadores buscando por Internet dispositivos abiertos o con bajo nivel de seguridad** para ver qué pueden hacer con ellos... Recordemos el ataque que sufrieron las principales páginas web del mundo en octubre de 2016 con el ataque "MIRAI" que provocó mediante un ataque de denegación de servicio que millones de dispositivos conectados empezaran a obedecer órdenes para atacar estos sistemas.

not being taken into account. The price of the devices and the ease of its implementation are getting more importance than its security and, yes, there are a lot of devices that can be, a priori, little attackable, little "hackable", that is, of very little interest to access to them, such as the temperature of your fridge, the watering devices of your garden, etc.

"The pairing *risk-benefit*, which is always present in every investment decision, must change inevitably [...] for that of *security-price*"

The lift of a residential building seems a little appealing objective for "the bad ones". However, **disabling 150 lifts and asking for a ransom to reactivate them** does not seem so strange. The company's image with regard to clients left with no service for some time, the possible loss of those clients, apart from the payment of the ransom, that is, the violence generated by this kind of bribery, are a real problem for any lift assistance company. Not to mention lifts in buildings sensitive to actions with bigger consequences (shopping centres, government buildings, critical facilities, etc) where **there is place even for terrorism.**



Ransomware is the most widespread cybercrime technique in the world. **20,000 cases were detected in 2017** only in Spain. Regarding **cyberterrorism**, it seems obvious that it has a clear objective in this kind of systems inside critical facilities or those having great impact. **There is no published data** about this type of cyberdelinquency, but there are many references and rumours.

The proposal of telecommunications operators must go in line with the systems deployment but also with the security of those networks. The systems vulnerability is being always associated to bad practices or the lack of these ones by the employees, or to not updating the operating systems or the firewalls of the companies. **At the same time we overlook the fact that there are hundreds of thousands of trackers searching the**

Cuando una empresa de fabricación de cartón ve secuestrados sus ordenadores, su servidor y, por consiguiente, sus datos, no podían creerse objetivo de nadie y sin embargo se veía obligada a pagar **10.000 euros en menos de 12 horas** para poder recuperar "su vida". Un solo dispositivo remoto conectado a un proceso de fabricación mediante una **"cheap network"** facilitó la entrada a su sistema de gestión de alarmas y a su sistema de gestión. A partir de ahí, el resto fue muy sencillo. Estos cientos de miles de rastreadores encuentran puertas abiertas a través de dispositivos conectados a internet sin la suficiente seguridad y **no sólo porque los empleados no cumplan las normas o los sistemas no se actualicen adecuadamente.**

Los operadores somos responsables de que todos los dispositivos estén, **no sólo conectados y facilitando despliegues, sino conectados con la suficiente seguridad.** El sistema GPRS/GSM lleva 25 años demostrando que es el sistema que más seguridad ofrece y por ello debe ser prioritario en función de la seguridad requerida. El resto de comunicaciones: cheap network, banda libre, etc, por supuesto, son operativas, **pero no para comunicaciones que requieran un cierto nivel de seguridad.**

"El Ransomeware es la técnica de cibercrimen más extendida a lo largo de todo el planeta"

Algunos operadores de telecomunicaciones no tiramos la toalla y seguimos pensando en **fórmulas para evitar y contrarrestar este tipo de ataques:** securizando las comunicaciones -a través de VPN- entre el ascensor y la central, y entre el ascensor y el técnico de mantenimiento desplazado, garantizando el 0% de hiperactividad, protegiendo las comunicaciones frente a ataques de denegación de servicio, controlando y gestionando los enrutamientos de las direcciones IP, etc. **Todas las medidas son pocas**. Debemos exigirle a nuestro Operador de Telecomunicaciones que nos ofrezca siempre el mayor nivel de seguridad en cada momento para garantizar la Seguridad de nuestras comunicaciones. Ya sea para proteger un automóvil en movimiento como un ascensor de una comunidad de vecinos sencilla.

A finales de 2015 se reunió un panel de expertos relacionados con la Sociedad de la Información, Ingenieros, empresarios, Fuerzas de Seguridad, institutos de Seguridad informática de varios países, catedráticos universitarios, sociólogos, políticos, etc, se dieron cita para hablar de seguridad. Los resultados se presentaron en un informe bajo un título que resumía todas las conclusiones en una: **"Protege lo importante, porque no vas a poder proteger todo..."**

Internet for open devices or devices with a low level of security to see what they can do with them. We must remember the attack suffered by the world's main web pages in October 2016 with "MIRAI" that caused, by way of a denial-of-service attack, millions of connected devices to start taking orders to attack these systems.

When a company that produces cardboards has its computers and server and, as a result, also its data hijacked, it could not believe to be the objective of anybody. Nevertheless, it was forced to pay **10,000 euros in less than 12 hours** to recover its "life". One single device remotely connected to a production process through **a cheap network** facilitated the entrance to its alarm and management systems. From there, the rest was very simple. These hundreds of thousands of trackers find open doors through devices connected to the Internet without the sufficient security and **not only because the employees do not comply with the rules or because the systems are not adequately updated.**

The operators are responsible of getting all the devices **connected and facilitating deployment, especially of having them connected with sufficient** security. The GPRS/GSM system has been 25 years demonstrating it is the system that offers the greatest security and thus it must be preferential based on the required security. The rest of communications (cheap network, unlicensed band, etc) are operational, of course, **but not for communications that require certain security level.**

"Ransomware is the most widespread cybercrime technique in the world"

Some telecoms operators do not throw in the towel and we keep thinking of **methods to avoid and counteract this kind of attacks**: by making communications secure –through VPN- between the lift and the head office, and between the lift and the maintenance technician; ensuring a 0% hyperactivity; protecting communications against denial-of-service attacks; controlling and managing the routing of IP addresses, etc. **All possible measures are too few**. We must demand our telecommunications operator to always offer us the highest security level at every moment to ensure the security of our communications. Be it for protecting a moving car or an easy building lift.

At the end of 2015 a board of experts related to information society met. Engineers, businessmen, security forces, computer security institutes from different countries, university professors, sociologists, politicians... met up to talk about security. The results were presented in a report under a title that summarized all the conclusions in one: **"Protect what is important because you will not be able to protect everything".**

Alai Secure, primer operador Triple-play en Seguridad Telco

M2M

Red Inteligente

ADSL Segura

"Ofrezca a su red de ascensores la oferta de comunicaciones convergente ***más segura del mercado"***

- Llamadas 100% garantizadas y seguras
- Sistema anti-hiperactividad
- Sistema anti-hacking
- Detección de incidencias
- Servicio de IP Fija independiente
- **SIM Alto rendimiento, especial para comunicaciones M2M**

alaisecure.com

Alai Secure

Operador triple-play en Seguridad Telco

La seguridad en el sector de la elevación

Security in the elevation sector

La seguridad en los ascensores ha sido desde el inicio de este invento un factor clave en su desarrollo y popularidad. El invento del ascensor de 1852 que se atribuye a Elisha Graves Otis no es más que la invención de un sistema de seguridad para evitar la caída en caso de rotura del cable.

Todas las empresas del sector de los ascensores **consideran la seguridad un factor primordial** y las PYMES no se quedan atrás en este aspecto. No solo se cumple con los requisitos establecidos por la normativa vigente EN 81-20/50 sino que también, desde las pequeñas empresas, miramos al futuro y estamos en constante formación y desarrollo, con departamentos de innovación tecnológica que desarrollan nuevas fórmulas de registro de datos y mantenimiento de los ascensores a partir del control remoto.

La seguridad no consiste solamente en sistemas que eviten los accidentes cuando un elemento se estropea o falla. Nuestro objetivo va mucho más allá de este concepto: **prevenir cualquier problema y solucionarlo antes de que tenga consecuencias**; que el ascensor nunca se estropee porque toda reparación se pueda prevenir y planificar es lo que se espera conseguir en las pequeñas y medianas empresas del sector de los ascensores.

Gracias al Internet de las Cosas y al Machine Learning, estas aspiraciones son posibles y cada vez están más presentes en la industria de la elevación. La digitalización de las empresas está al alcance de todos y las economías de escala no suponen una desventaja frente a las grandes multinacionales en este campo.

Ascensors Ebyp goza desde hace ya 5 años de **un**

Security surrounding lift installations has been since the beginning of this invention a key point in its development and popularity. The invention of the lift in 1852 by Elisha Graves Otis was just the addition of an innovative security system to avoid the downfall for break of the cable.

All the companies from elevation and lift sector consider security an imperative and SMEs aren't falling behind in this field. Not only the requirements stablished by the current law EN 81-20/50 are fulfilled, but also from the small companies we think ahead and are in constant training and development owning I+D+i departments focused on technologic innovation that develop new ways of data record and lift's maintenance through remote control.

Security not only consist on systems which avoid accidents when an element breaks down. Our goal goes further away from this concept: **we aim to prevent any problem and solve it before it can cause any damage**; that the elevator never breaks down because all repairs can be prevented and planned is what is expected to be achieved in small and medium-sized companies in the elevator sector.

Thanks to Internet of Things and Machine Learning, the named hopes are possible, and they have more and more presence within the elevation industry. Digitalization of companies is within range of everybody and economies of scale do not represent a disadvantage in front of large multinational companies.

Ascensors Ebyp has enjoyed its **own lift monitoring system** thanks to the implementation of **bidirectional communication** devices for 5 years right now. Across this developed system, we have been able to stablish three telecommunication's operations that have became key

sistema propio de monitorización del ascensor gracias a la implementación de **dispositivos de comunicación bidireccional**. A través de este sistema desarrollado, hemos establecido tres actividades de telecomunicación que han devenido claves para nuestra actividad. Con la telemetría de la maniobra el propio ascensor nos reporta sus fallos y problemas a tiempo real a través de los sensores y contactores que lo constituyen. Este sistema nos permite atender las averías más rápidamente y reducir el tiempo de parada de la instalación. Con la telemetría del teléfono este se revisa automáticamente cada 72 horas para asegurar su correcto funcionamiento en caso de emergencia. Por último, a partir del telecontrol podemos supervisar el funcionamiento de un ascensor en tiempo real y cambiar la configuración de la maniobra a distancia.

“A partir del telecontrol podemos supervisar el funcionamiento de un ascensor en tiempo real”

Por supuesto para poder utilizar estos sistemas sin ningún riesgo, la ciberseguridad es indispensable. Es por esto por lo que el sistema ha sido diseñado por un consultor especializado quien lo revisa constantemente para mantenerlo actualizado y evitar cualquier riesgo de intrusión.

Aprovechar las nuevas tecnologías para mejorar la **experiencia de nuestros clientes** y lograr la **máxima seguridad** en nuestras instalaciones no es solo un reto, es una necesidad. Desde Ascensors Ebyp, consideramos indispensable explotar este objetivo para mantenernos competitivos en un mercado de cambio continuo.

activities of our service. Through telemetry of handling the lift itself reports shortcomings and problems detected from its own sensors and contactors in real time. This system allows us to attend the system failures faster and to reduce the time the lift remains out of service. Through telemetry of phone, the system performs an automatic checking of the communication every 72 hours to guarantee its proper functioning in case of emergency. Finally, through tele-control we can supervise the functioning of any lift in real time and change the working configurations of the system remotely.

“Through tele-control we can supervise the functioning of any lift in real time ”

Of course, to use all these systems properly and without any risk, cybersecurity is essential. For that reason, the system has been designed by a specialized consultant who is in charge of the continuous supervision of it in order to keep it update and to avoid any intrusion risk.

Take advantage of new technologies to improve **customer’s experience** and reach the **most secure systems** ever is not only a challenge, but also a necessity. From Ascensors Ebyp, we consider essential to achieve this goal, so that we could maintain ourselves competitive in a continuous-changing market.

Ciberseguridad, la palabra de moda

Cybersecurity, Today's Buzzword

DAVID MORENO DEL CERRO | En los últimos meses, hemos podido comprobar de qué manera términos como hacker, ciberdelincuencia, robo de información, ransomware o incluso Wannacry están presentes en nuestro día a día. El uso extensivo de las tecnologías de la información, junto con la omnipresencia de Internet, ha expuesto a nuestras empresas y nuestra información a una serie de amenazas que hace cinco o seis años eran casi anecdóticas. Hoy en día **no hay ninguna compañía que esté libre de riesgo** y podemos dividirlas en dos tipos: las que han sido atacadas y las que todavía no lo han sido (o, al menos, no son conscientes de ello).

La labor más importante de un CISO (Chief Information Security Officer) o responsable de seguridad en una empresa es velar porque **se sigan unos procesos en la protección de la información,** asegurar que tecnológicamente **se dispone de los medios para afrontar una crisis de ciberseguridad** y, lo más importante, **que se puede recuperar el negocio** y la situación previa. Además de eso, debe trabajar junto a la dirección de la compañía para alinear todas sus acciones con los objetivos de negocio; tiene que desarrollar una **cultura de protección** y diseñar **planes de formación y concienciación** a todos los niveles; estar alineado con las áreas legales de la empresa para darles el apoyo técnico que necesiten para asegurar el cumplimiento normativo (por ejemplo, en la aplicación del recién estrenado Reglamento General de Protección de Datos). Como se puede comprobar, se trata de una figura que **afecta transversalmente a todos los procesos de negocio** y debe estar presente en todos ellos, de una u otra manera.

En mi caso, como CISO de Tendam (anteriormente Grupo Cortefiel), tengo la responsabilidad de proteger

DAVID MORENO DEL CERRO | These last few months have shown how terms such as hacker, cybercrime, information theft, ransomware and even Wannacry have become a part of our daily lives. The extensive use of information technologies, coupled with the omnipresence of the Internet, has exposed our companies and our information to a series of threats that five or six years ago would have been merely anecdotal. Today, however, **all companies are exposed to risk**, and we can divide them into two groups: those that have suffered attacks and those that have not yet been attacked (at least, as far as they know).

The most important task of a company's CISO (Chief Information Security Officer) or person in charge of security is **to ensure that certain information-protection procedures are followed**, that the **technological means are available to face a cybersecurity crisis**, and most importantly, that both the company's business and previous situation can be restored. They also have to work together with management to align all these actions with the company's business objectives; they have to develop a **security culture** and design **training and awareness-raising plans** at all levels; they have to work closely with the company's legal departments to provide the technical support needed to ensure compliance with regulations (for example, applying the recently introduced General Data Protection Regulation). Clearly, the CISO is a figure that **impacts all business processes** and must be present in all of them in some form or another.

In my case, as CISO of Tendam (previously Grupo Cortefiel), I am responsible for protecting the information of a group of five fashion brands (Cortefiel, Pedro del Hierro, Springfield, Women'secret, and Fifty), all of them

la información de un grupo formado por cinco marcas del sector moda (Cortefiel, Pedro del Hierro, Springfield, women'secret y Fifty), líderes en sus segmentos, con presencia internacional y clubes de fidelidad formados por millones de clientes. No es una tarea sencilla, que requiere disponer de **un equipo humano y técnico preparado**, pero, sobre todo, estar al cabo de la calle de cualquier iniciativa que el negocio ponga en marcha, para poder a**decuar de la mejor manera posible nuestras acciones y reaccionar llegado el caso**.

Como indicaba anteriormente, nuestra empresa tiene presencia en todos los continentes, lo que presenta un plus de complejidad añadido. Nuestra infraestructura está operando permanentemente, desde México hasta Rusia, pasando por Hong Kong o India. Nuestros más de 9.000 empleados tienen **diferentes culturas y distintas aproximaciones a temas relacionados con la seguridad y la privacidad**, lo que, añadido a las dificultades culturales propias, exigen un esfuerzo adicional a la hora de formar e informar sobre cualquier tema relacionado. En nuestro caso, diseñamos planes formativos trabajando juntamente con personal local, conocedor de la idiosincrasia particular de cada uno de los países, pero siempre alineándonos con las directrices marcadas desde la central en España.

Cabe destacar que, como cualquier otra empresa, manejamos ingentes cantidades de datos, **tanto de negocio como de carácter personal** (de clientes, proveedores o empleados). Es esta última información en la que ponemos mayor foco; para nosotros, lo más importante es **asegurar la privacidad y un uso correcto de la información personal**. Desde el año 1992, año en el que apareció la primera ley española en materia de protección de datos (la LORTAD) existe una sensibilización especial, que viene originada por la concepción que tenemos de nuestro negocio, donde **el cliente y no el producto es el centro de nuestra estrategia**. Ya con la LOPD, que está a punto de ser renovada, se desarrollaron programas de revisión y adecuación que iban más allá de lo que imponía el reglamento en vigor. Es por eso por lo que el salto hacia el RGPD, no sin esfuerzo, está resultándonos menos traumático de lo que sería normal.

"Para nosotros, lo más importante es asegurar la privacidad y un uso correcto de la información personal"

Aunque no seamos una empresa tecnológica y nuestro foco sea la distribución de moda, ponemos gran esfuerzo en conocer **las últimas tendencias existentes en el mercado en materia de seguridad informática.** Trabajamos con proveedores y colaboradores expertos en diferentes ámbitos de la disciplina, desde compañías puramente técnicas que nos proporcionan soluciones

leaders in their sectors, with an international presence and fidelity clubs comprised of millions of clients. It is not an easy task, and one that requires a **team well prepared in both human and technical terms** and, especially, possessing up-to-date knowledge of all of the group's initiatives **in order to act and, if need be, react optimally.**

As I mentioned earlier, our group is present on all continents, which adds extra complexity. Our infrastructure is permanently active, from Mexico to Russia, through Hong Kong and India. Our more than 9,000 employees **come from different cultures and have different ways of approaching security- and privacy-related issues**. This, added to the typical cultural difficulties, demands extra care when training in and informing about any related topic. In our case, we design training programmes in conjunction with local staff who are familiar with each individual country's particular idiosyncrasies, while simultaneously adhering to the guidelines established by the headquarters in Spain.

It is important to note that, just like any other enterprise, we handle huge volumes of data, b**oth business-related and personal** (concerning clients, suppliers and employees). Most of our efforts focus on personal data because we consider **privacy protection and the proper use of personal information** to be all-important. Since 1992 and the introduction of the first Spanish law on data protection (the LORTAD), this subject has been of special concern to us because of our business concept, which puts **our clients and not our products at the centre of our strategy.** In response to the LOPD law on data protection, a new version of which is about to enter into effect, we developed programmes to review and adapt our data handling that went beyond the requirements of said law. This is why the transition to the GDPR, while not effortless, is being much less traumatic for us than would normally be the case.

"We consider privacy protection and the proper use of personal information to be all-important"

Although our company is not into technology but into fashion distribution, we do invest a lot of effort into keeping abreast of **the latest market trends in matters of IT security**. Our suppliers and partners are experts in different aspects of this field, from companies that provide purely technical market solutions to consultants and specialists in ethical hacking, cybervigilance or computer forensics. All of them work together in an integrated manner and in alignment with our policies in matters of security and protection.

I believe it is very important for companies to rely on

de mercado, pasando por consultoras y especialistas en hacking ético, cibervigilancia o informática forense, todos ellos dirigidos de forma integrada y alineados con nuestras políticas de seguridad y protección.

Creo que es muy importante que las empresas se apoyen en especialistas, por dos motivos fundamentales: en la actualidad, **hay muy poco talento en el mercado de la ciberseguridad,** no hay profesionales con experiencia y cuesta mucho contratar personal capacitado. Si a esto añadimos que nuestro foco de negocio es la moda, preferimos centrarnos en dar el máximo valor a la compañía en ese área, dejando a las compañías expertas ayudarnos en la otra materia. El segundo motivo consiste en que **la disciplina de la seguridad informática es tremendamente dinámica** y exige un nivel de formación muy alto y puesta al día constante, cosa que en nuestro caso es complicado de conseguir por el mismo motivo que antes, no es nuestro "core" de negocio.

He dejado para el final una reseña a las acciones que para mí son las más importantes que hay que realizar para mitigar el creciente número de amenazas y que he comentado de forma escueta al principio del texto: **la concienciación**. La frase está ya muy manida, pero sigue siendo válida: **el usuario es el eslabón más débil**. Efectivamente, casi el 100% de los incidentes de seguridad son provocados por fallos humanos, bien sean intencionados o no, lo que demuestra que la tecnología no da respuesta a todos los problemas. Disponer de unos empleados que conozcan los riesgos asociados a las tecnologías (especialmente al uso de Internet) y que sepan cómo reaccionar ante una incidencia de seguridad es un plus que nos va a ayudar a reducir el riesgo. Por ejemplo, la diferencia entre identificar adecuadamente un intento de fraude por correo electrónico o no puede suponer un impacto económico directo de varios cientos de miles de euros**. Los usuarios deben convertirse en nuestro primer nivel de defensa** y para ello debemos darle la formación e instrucción pertinente, siempre adecuadas a su cometido y funciones dentro de la empresa.

"Los usuarios deben convertirse en nuestro primer nivel de defensa"

Finalizo esta exposición resumiendo las principales funciones de la posición que ocupo: **gestionar los riesgos tecnológicos, alinear cualquier acción con la estrategia de negocio, concienciar al personal y dar apoyo a la compañía en materia de seguridad informática.** Esas son, en mi opinión, las tareas más importantes de cualquier CISO.

specialists, for two basic reasons. Firstly, **there is currently very little talent in the cybersecurity market,** there are no experienced professionals, and it takes a lot of effort to hire qualified personnel. Add to this that our main business focus is fashion, and it becomes clear that we are better served by focusing as much as possible on this area and leave security matters in the hands of specialised companies. Secondly, **the field of IT security is incredibly dynamic** and requires a very high and constantly updated level of expertise, something difficult to achieve in our case for the previously mentioned reason, which is that it is not the core of our business.

I have left for the end an overview of the actions that I consider to be the most important to mitigate the effects of the growing number of cyberthreats and that I have briefly mentioned at the beginning of this text: **awareness-raising**. It may be a hackneyed phrase by now but it remains true: **users are the weakest link**. Indeed, almost 100% of security incidents are the result of human mistakes, either deliberate or not, which proves that technology alone cannot solve all problems. Having employees that are aware of the risks associated with technologies (especially the use of the Internet) and who know how to react when a security incident takes place is very helpful in reducing risk. For example, failure to correctly identify an email fraud attempt can cause a direct economic impact of hundreds of thousands of euros. **Users must become our first line of defence**, and to this end we must provide them with proper training and instructions adapted to their tasks and functions in the company.

"Users must become our first line of defence"

To conclude, I am going to summarise the main functions of the post I hold: **managing technological risks, aligning all actions with business strategy, raising employee awareness, and providing the company with computer-security support**. These are, in my opinion, the most important tasks of any CISO.

ADVERTISIM

ADVERTISIM MANAGER

Diseña y gestiona los contenidos de tus dispositivos Advertisim en tiempo real y de forma remota, independientemente del país en el que se encuentren.

Design and manage contents for your Advertisim displays in real time and remote control, regardless of its geographical location.

www.advertisim.com

NAVARSYSTEMS | 72 horas | ADVERTISIM | net4machines

La ciberseguridad en las carreteras del futuro

Cybersecurity on the roads of the future

RETOS EN LAS CARRETERAS DEL FUTURO

Avances tecnológicos y similitud con entornos industriales

La carretera no es ajena a la transformación digital, desde hace ya tiempo se está desplegando multitud de dispositivos del ámbito IoT de distinta naturaleza: cámaras de vigilancia, semáforos, sensores de monitorización de la infraestructura (tempreratura, luz, detectores de humo, etc), paneles de señalización, controles de acceso, etc.

El incremento de uso de tecnología se evidencia cuando se observa la **evolución del ratio de direcciones IP,** visibles dentro de nuestra red, por kilómetro gestionado. Prácticamente se ha duplicado en los dos últimos años y mantiene una tendencia similar a futuro. Por cierto, en entornos IoT/industriales no todos los dispositivos interactúan a través de TCPIP, **el radioespectro es otro ámbito que también debe ser vigilado.**

La gestión tecnológica de la carretera plantea retos similares a los entornos industriales, donde los dispositivos han sido construidos y desplegados siguiendo patrones de resistencia a condiciones ambientales adversas, poco consumo energético y alta perdurabilidad. Dispositivos que son telecomandados a distancia por sistemas SCADA.

El coche, un superdispositivo IoT

CHALLENGES ON THE ROADS OF THE FUTURE

Technological advances and similarity with industrial environments

Roads are also experiencing the effects of digital transformation. Many IoT devices of different kinds have been deployed on them for quite some time: Surveillance cameras, traffic lights, sensors monitoring infrastructure (temperature, light, smoke detectors, etc), traffic signs, access controls, etc.

The increase in the use of technology is made evident in the **evolution of the ratio of IP addresses** visible in our network per kilometre managed. It has practically doubled over the past two years and is maintaining a similar trend for the future. Incidentally, in IoT/industrial environments not all devices interact through TCP/IP; **the radio spectrum should also be monitored.**

Technological road management presents challenges similar to industrial environments, where the construction and deployment of devices is determined by factors such as resistance to adverse weather conditions, low energy consumption, and high durability. Devices that are remotely controlled by SCADA systems.

The car, an IoT superdevice

The leading actor on the road is the vehicle. **For now, it is the Connected Vehicle, but its performance is progressing toward that of the Autonomous Vehicle.**

El gran protagonista en la carretera es el vehículo, **actualmente Vehículo Conectado pero que va desplegando prestaciones de Vehículo Autónomo progresivamente**. La Sociedad de Ingenieros Automotrices (SAE) ha establecido un esquema de 5 niveles que determina el nivel de autonomía de los vehículos. Esta escala es la de referencia para el sector:

- **Nivel 1 - Asistente de conducción:** El sistema algunas veces realiza alguna parte de la tarea. Un ejemplo es el sistema de control de crucero.
- **Nivel 2 - Autonomía parcial:** El sistema realiza alguna tarea de conducción. El conductor continúa monitorizando todo y haciendo todas las tareas básicas. Un ejemplo es el sistema que previene riesgo de salida carretera sin basarse en las líneas pintadas en el pavimento.
- **Nivel 3 - Autonomía condicional:** El sistema puede realizar algunas tareas y monitorizar el entorno en algunos casos. El conductor debe estar disponible para tomar el control cuando el sistema lo requiere. El sistema Autopilot de Tesla se encuentra en este segmento.
- **Nivel 4 - Alta autonomía:** En casos definidos (por ejemplo un carril segregado de autopista), no se precisa conductor, el sistema toma todas las decisiones, pudiendo conducir y monitorizar el entorno.
- **Nivel 5 - Plena autonomía:** El sistema lo hace todo, ha desaparecido el volante.

Tal y como hemos mencionado anteriormente creemos que las primeras experiencias reales de autonomía Nivel 4 tendrán lugar en las vías de alta capacidad.

“El incremento de uso de tecnología se evidencia cuando se observa la evolución del ratio de direcciones IP por kilómetro gestionado”

Riesgos

Nuestras prioridades frente a los riesgos que se derivan son claras, se trata de prevenir riesgos que puedan:

- **Poner en peligro a la persona física**, en este capítulo encontramos riesgos del tipo:
  - Alteración de señales de tráfico, bien sea en el punto origen o en la interpretación que realiza el sistema receptor que lo interpreta.
  - Compromiso de los sistemas de guiado y seguridad del vehículo autónomo.
- **Poner en peligro a la persona virtual**, en todo aquello que tiene que ver con el derecho fundamental a la privacidad, tanto a nivel de identificación de datos personales como a la generación de perfiles de comportamiento.
- **Comprometer activos de la compañía**, siendo algunos ejemplos:

The Society of Automotive Engineers (SAE) has established a five-level scale for classifying vehicle autonomy that is the reference for the sector:

- **Level 1 - Driving assistance:** The system occasionally performs a part of the task of driving. An example would be the cruise control.
- **Level 2 - Partial autonomy:** The system performs some driving tasks. The driver continues to monitor everything and to perform all the basic tasks. An example would be the system that keeps a car in its lane without using the lines painted on the pavement.
- **Level 3 - Conditional autonomy:** The system can perform some tasks and monitor the environment in some cases. The driver must be ready to take control when required to by the system. Tesla's Autopilot is an example of such a system.
- **Level 4 - High autonomy:** Under well-defined circumstances (for example, a segregated lane in a motorway), no driver is necessary. The system takes all decisions and is able to drive and monitor the environment.
- **Level 5 - Full autonomy:** The system does everything; the steering wheel has disappeared.

As mentioned before, we believe that the first real experiences of level 4 autonomy will take place on high-capacity roads.

“The increase in the use of technology is made evident in the evolution of the ratio of IP addresses per kilometre managed”

Risks

Our priorities regarding the ensuing risks are clear: we need to prevent risks that can:

- **Endanger the physical person**. Such risks occur when:
  - Traffic signals are altered, either at the point of origin or in their interpretation by the receiving system that interprets them.
  - The autonomous vehicle's guidance and security systems are compromised.
- **Endanger the virtual person** in all aspects related to the basic right to privacy, from the identification of personal data to behavioural profiling.
- **Compromise company assets**. Examples could be:
  - The destruction or disabling of surveillance cameras.
  - The disabling of security measures.

Leaving aside incidents involving vehicles (of which there have been several and they are known), there are several precedents of road-traffic incidents, including:

- Destrucción o inhabilitación de cámaras de vigilancia.
- Inhabilitación de controles de seguridad.

Sin entrar en incidentes con vehículos (que hay varios y son conocidos) hay varios precedentes de incidentes en el tráfico por carretera, entre ellos:

- **2005 - Dispositivos de inhabilitación de tráfico usados en USA para cambiar semáforos de rojo a verde.** En este caso los atacantes eran conductores sin escrúpulos que buscaban eludir sanciones.
- **2008 - Sabotaje a la regulación semafórica de la ciudad de Los Ángeles.** En este caso los atacantes eran empleados que tenían una disputa laboral.
- **2013 - Túnel en Israel que queda inoperativo por un ataque DDoS** (Denegación de servicio) generado por una botnet desde las cámaras de vigilancia. En este caso el ataque tenía un nivel superior de sofisticación y se clasificó entre ataque de ciberterrorismo o ciberguerra (conocido como cyberwarfare). Este último incidente conllevó la revisión de la estrategia nacional de ciberseguridad de Israel.

Perfiles de atacantes

En los casos expuestos anteriormente ya se observa que los atacantes son de distinto tipo:

- **2005 - Traffic-disabling devices were used in the US to change traffic lights from red to green**. In this case the attackers were unscrupulous drivers aiming to avoid traffic fines.
- **2008 - Sabotage of the computer system controlling Los Angeles's traffic lights**. In this case the culprits were city employees who were having a labour dispute.
- **2013 - A tunnel in Israel was shut down by a DDoS** (Distributed Denial-of-service) attack conducted from the surveillance cameras by a botnet. The attack was highly sophisticated and was classified as an act of cyberterrorism or cyberwarfare. This attack led to a revision of Israel's national cybersecurity strategy.

Attacker profiles

The examples mentioned earlier show that there are different types of attackers:

1. **Unethical hackers:** the initial profile, experts wanting to show off within their community by creating security incidents without being fully aware of the damage they cause out in the real world.
2. **Hacktivists:** collectives who protest for political or social reasons and use the cyberattacks to publicise their cause.
3. **Cyberterrorists:** an evolution of hacktivism with more serious consequences. Their aim is to cause real damage to people and organizations, sometimes actually compromising human lives.
4. **Cybercriminals:** cybercrime currently generates more profit than drug trafficking. Ransomware attacks are one of their main extortion tools.
5. **Cyberwarfare:** several countries have been developing offensive and defensive capabilities in cyberspace for a long time.

The effects of incidents

Let's imagine an extreme case in which the level of autonomy of a specific range of vehicles has been sabotaged, causing them to behave erratically in traffic. **Who would the incident affect?**

- Without a doubt, **the occupants of the compromised vehicles.**
- But also the **manufacturers of the vehicle**, because they would have to deploy the first response measures.
- **Security forces and bodies**, because there is a real threat to people's physical integrity.
- **The operator of the infrastructure**, because traffic management in its entirety would be affected.

This brief reflection highlights the need to design and deploy comprehensive **plans to respond to future incidents**. In the future, we will have to deploy incident-response mechanisms capable of detecting, alerting about, and reacting to very serious incidents, and all of this in a matter of milliseconds.

1. **Hackers no éticos:** es el perfil inicial, personas expertas que buscan exhibirse dentro de la comunidad a la que pertenecen, generando incidentes de seguridad sin ser plenamente conscientes del daño real que producen.
2. **Hacktivistas**: colectivos que protestan por cuestiones políticas o sociales y que, a través de ciberataques buscan visibilidad para su causa.
3. **Ciberterroristas**: Es una evolución del hacktivimo en nivel de gravedad de las consecuencias. Buscan hacer daño real en personas y organizaciones, en ocasiones llegando a comprometer vidas humanas.
4. **Cibercriminales**: El cibercrimen genera hoy en día más ingresos que el tráfico de drogas. Los ataques de ransomware son hoy en día una de sus principales herramientas de extorsión.
5. **Cyber warfare:** Varios países llevan ya tiempo desarrollando capacidades defensivas y ofensivas en el ciberespacio.

Afectaciones frente a incidentes

Supongamos un caso extremo en el que el nivel de autonomía de una gama concreta de vehículos autónomos ha sido saboteado y genera un comportamiento errático en la vía. **¿A quién afectará el incidente?**:

- **A los ocupantes de los vehículos comprometidos**, sin duda.
- También **al fabricante del vehículo**, pues es quien deberá desplegar las primeras medidas de respuesta.
- **A las fuerzas y cuerpos de seguridad**, dado que se estará provocando un riesgo real a la integridad de las personas.
- **Al operador de la infraestructura**, porque afectará a toda la gestión viaria.

Esta breve reflexión introduce la necesidad de definir y desplegar **planes de respuesta integrales a futuros incidentes**. En el futuro deberemos desplegar mecanismos de respuesta a incidentes que, en milisegundos, sean capaces de detectar y generar alertas y desplegar primeras acciones de respuesta frente a compromisos de especial gravedad.

“Actualmente el Vehículo Conectado va desplegando prestaciones de Vehículo Autónomo progresivamente”

RIESGOS DE CIBERSEGURIDAD ESPECÍFICOS DE LOS DISPOSITIVOS IOT

Enumerados algunos aspectos muy específicos del sector carretera, introducimos ahora nuestra reflexión sobre seguridad en dispositivos IoT. Los dispositivos IoT tienen muchos aspectos positivos: son de bajo coste, sencillos de instalar, permiten la telegestión,

“For now, it is the Connected Vehicle, but its performance is progressing toward that of the Autonomous Vehicle”

SPECIFIC CYBERSECURITY RISKS IN IOT DEVICES

Having enumerated some very specific aspects of the road sector, we are now going to reflect on security in IoT devices. IoT devices have many positive aspects: they are low cost, easy to install, allow remote management, facilitate real-time monitoring, reduce maintenance costs, etc.

We live surrounded by IoT. It **is estimated that by 2020 there will be between 20 and 50 billion connected devices**, for areas as diverse as factories, buildings, cities, vehicles, medicine, the environment...

Being connected to the Internet, these devices are within the reach of any individual interested in exploiting any security gaps the device might have in order to obtain personal or financial gain. **They may even completely take over the devices and pursue illegal objectives**. There have been takeovers in the past: vehicles of different brands, water-treatment plants, hotel key cards, surveillance cameras, toys, pacemakers, and drones.

facilitan la monitorización en tiempo real, reducen costes de mantenimiento, etc.

Vivimos rodeados de IoT, para 2020 **se prevé que existan entre 20.000 millones y 50.000 millones de dispositivos conectados**, para áreas dispares como fábricas, edificios, ciudades, vehículos, medicina, medio ambiente, etc.

Estos dispositivos, al estar conectados a Internet, se encuentran al alcance de cualquier individuo que pueda tener interés en obtener un beneficio personal o económico de los fallos de seguridad que puedan tener. **Incluso podrían llegar a obtener el control total de estos dispositivos** para conseguir objetivos ilícitos. A modo de ejemplo, se ha obtenido el control de vehículos de diferentes marcas, de los sistemas de plantas de tratamiento de agua, de las "tarjetas llave" de hoteles, de cámaras de videovigilancia, de juguetes, de marcapasos y de drones.

"En el futuro deberemos desplegar mecanismos de respuesta a incidentes que, en milisegundos, sean capaces de detectar y generar alertas"

El caso con mayor relevancia, en este ámbito, es la **botnet Mirai.** Una botnet es un **grupo de dispositivos informáticos infectados y controlados de forma remota por un atacante.** En el caso de Mirai se considera que centenares de miles de dispositivos IoT (principalmente routers y cámaras de videovigilancia) se encuentran infectados y han sido utilizados por quienes tienen el control de esta botnet para ocasionar diferentes ciberincidentes. El mayor ataque de esta botnet se produjo en octubre de 2016 cuando se ordenó a los dispositivos de esta botnet que atacaran de forma conjunta a la empresa Dyn que gestiona el servicio de resolución de nombres en Internet (DNS) para grandes corporaciones americanas. Este ataque causó la caída durante varias horas de servicios como: Airbnb, Amazon, CNN, HBO, Netflix, Paypal, Spotify y Twitter.

"Para 2020 se prevé que existan entre 20.000 millones y 50.000 millones de dispositivos conectados"

¿Cómo reducir estos riesgos?

Los riesgos son intrínsecos a la tecnología IoT, por lo que nunca los podremos eliminar totalmente. Sin embargo, **deberíamos reducirlos a un nivel que pueda ser asumido por el usuario final** (ya sea una empresa o un particular) de forma que el nivel de riesgo sea razonable.

"In the future, we will have to deploy incident-response mechanisms capable of detecting, and alerting in a matter of milliseconds"

The most relevant example in this field is that of the Mirai botnet. A botnet is **a group of IT devices infected and remotely controlled by an attacker**. In the case of Mirai, it is thought that hundreds of thousands of IoT devices (mainly routers and surveillance cameras) are infected and have been used by those controlling this botnet to cause different cyberincidents. The biggest attack took place in October 2016, when the devices of this botnet were ordered to carry out a joint attack on Dyn, the company that manages internet domains for large American corporations. The attack took down major Internet services such as Airbnb, Amazon, CNN, HBO, Netflix, Paypal, Spotify, and Twitter.

"It is estimated that by 2020 there will be between 20 and 50 billion connected devices"

Nos encontramos en una época de despliegue masivo de dispositivos IoT. **El mercado requiere que estos sean baratos y sencillos.** Los fabricantes desean obtener ventajas competitivas y presentar sus productos antes que la competencia. Tanto fabricantes como usuarios **suelen priorizar la funcionalidad respecto a la seguridad**. Los ciberincidentes están cambiando esta priorización tanto por parte de los afectados directamente por los incidentes, como a nivel de legislación: Protección de infraestructuras críticas, Directiva NIS, GDPR.

Para proteger los dispositivos IoT existen una serie de **recomendaciones** que deberían ser seguidas por los fabricantes y exigidas por los usuarios finales. A continuación, se muestran las principales buenas prácticas definidas en la **"Marca de Garantía de confianza en ciberseguridad para entornos IoT"** definida por el Centro de Estudios en Movilidad e IoT de ISMS Forum Spain:

- **Designar un responsable de seguridad del producto** en la empresa fabricante.
- Desarrollar las aplicaciones **basándose en estándares de desarrollo seguro.**
- **Realizar un análisis de riesgos de ciberseguridad del dispositivo.**
- **Realizar una evaluación de impacto en la privacidad.**
- **Disponer de un Seguro de Responsabilidad Civil** que cubra los riesgos de ciberseguridad y privacidad.
- **Incluir aspectos de ciberseguridad en la garantía.**
- **Monitorizar la seguridad del dispositivo** y ofrecer parches y actualizaciones durante todo el periodo de vida del producto.
- **Permitir la eliminación de forma segura de la información del producto** una vez finalizada su vida útil.
- **Deshabilitar cualquier puerto de comunicación o interfaz que no sea imprescindible.**
- **Utilizar protocolos seguros de comunicación** que cifren la información y autentiquen a los dispositivos.
- **Disponer de métodos seguros de autenticación** con contraseñas gestionadas por el usuario.
- **Políticas de caducidad y complejidad de las contraseñas.**
- **Almacenamiento seguro de las contraseñas.**
- **Mantener registros de las conexiones realizadas.**
- **Protecciones anti-DoS y antimalware.**
- **Cumplimiento de la legislación** en materia de protección de datos personales.

How to reduce these risks?

Risks are intrinsic to IoT technology, so we will never be able to completely eliminate them. However, **we should reduce them to reasonable levels that can be assumed by end users** (be they companies or private individuals).

This is the era of the massive deployment of IoT devices. **The market requires them to be cheap and simple**. Manufacturers want to obtain competitive advantages and to present their products ahead of the competition. Both manufacturers and users **tend to give priority to functionality over security**. Cyberincidents are changing this priority, both among those directly affected by the incidents and at the legislative level with the protection of critical infrastructures, NIS Directive, GDPR.

IoT devices can be protected using a series of **recommendations** that manufacturers should follow and end users should demand. Below are the main good practices described in the "Guarantee Mark of trust in cybersecurity for IoT environments" created by the Mobility and IoT Think-tank of ISMS Forum Spain:

- **Designating a person in charge of the product's security** at the manufacturer.
- Developing applications **following safe development standards.**
- **Analysing the device's cybersecurity risks.**
- **Performing an assessment of the impact on privacy.**
- **Having civil liability insurance** covering cybersecurity and privacy risks.
- **Including cybersecurity aspects in the warranty.**
- **Monitoring device security** and offering patches and updates during the product's whole lifespan.
- **Allowing the safe elimination of a product's information** once it has reached the end of its life cycle.
- **Disabling any communications port or interface that is not strictly necessary.**
- **Using safe communications protocols** that encrypt information and authenticate devices.
- **Having secured authentication methods** with user-managed passwords.
- **Having policies governing password expiry and complexity.**
- **Safe password storage.**
- **Maintaining records of connections established.**
- **Anti-DoS and antimalware protection.**
- **Complying with legislation** on personal data protection.

El nuevo mundo hiperconectado ¿seguro?

The new hyperconnected world: is it safe?

FIRAS ATASSI | El Internet de las cosas (IoT) ha supuesto una última revolución que supone una **mayor integración entre el mundo real y el mundo tecnológico**, cambiando radicalmente el modo en que accedemos y utilizamos la tecnología en nuestro día a día. Pero este nuevo ecosistema conlleva, inevitablemente, nuevos riesgos.

Cada vez tenemos más aparatos conectados, tanto en casa como en la empresa. Si bien es cierto que toda esta tecnología surge para facilitarnos más la vida y nos permite estar conectados y tomar el control de la información de nuestras empresas y nuestros hogares en cualquier lugar del mundo, **cada vez están surgiendo más dispositivos que se deberían regularizar**. Y más aún si están fabricados en base a incluir la privacidad, la seguridad y la confidencialidad desde la fase de diseño, ya que en caso contrario lo que tenemos son puertas por las que un hacker podría entrar.

“El Internet de las cosas ha supuesto una última revolución que supone una mayor integración entre el mundo real y el mundo tecnológico”

Imaginemos que alguien pueda acceder al sistema de control de nuestro vehículo mientras circula o que alguien puede acceder a los datos de salud de tu reloj o a sensores que controlan nuestras infraestructuras críticas. ¿No es lo ideal verdad?

Los riesgos asociados a la seguridad y privacidad que se derivan de este nuevo ecosistema hiperconectado

FIRAS ATASSI | The internet of Things (IoT) has been a revolution that involves a **greater integration between the real and technological world**, changing radically the way we access and use technology in our daily life. But this new ecosystem inevitably involves new risks.

We have an increase in connected devices, both at home and at the office. Although this technology arises to make life easier and allows us to be connected and having control of the information of our companies and homes from any place of the world, **there are many devices that should be regularized**. Furthermore if they are manufactured based on the inclusion of privacy, security and confidentiality from the design phase, otherwise we have a door opened to hackers.

“The internet of Things has been a revolution that involves a greater integration between the real and technological world”

Imagine that someone can access the control system of our vehicle while driving or access our health data stored in our smartwatch, or even sensors that control our main infrastructures. It is not an ideal situation, right?

The everyday risk associated to security and privacy that comes from this new hyper connected ecosystem is one of the main challenges we face in IoT concerning companies. And sometimes **we don’t even know the real issues that arises from**

es uno de los principales retos que afrontamos en el IoT dentro de las empresas. Y es que, en ocasiones, **desconocemos los riesgos reales de la convergencia de conectar a personas con objetos, objetos con sensores y sensores con datos**, que a su vez van a cambiar nuestros procesos y van a transformar los negocios y la vida de las personas en su día a día.

En este sentido, el mayor reto para una compañía es poder controlar o saber qué información sale de nuestras redes o qué datos están siendo capturados por dispositivos que a priori no son sospechosos, y tenemos que establecer procedimientos para garantizar que los requerimientos de seguridad de estos dispositivos no han sido ignorados.

No en vano, según el **Informe Anual sobre Ciberseguridad 2017 elaborado por Cisco**, en el que han participado unos 3.000 responsables de seguridad de empresas de 13 países del mundo, la ciberseguridad es uno de los objetivos estratégicos de máxima prioridad para los directivos de la mayor parte de las empresas participantes. El informe también revela que, si bien, el 60% de los encuestados considera que los sistemas de seguridad de su empresa son efectivos o altamente efectivos, cerca de un tercio han tenido alguna brecha de seguridad durante el último año con un impacto sobre sus cliente o ingresos.

“La ciberseguridad es uno de los objetivos estratégicos de máxima prioridad para los directivos de la mayor parte de las empresas”

A mi entender se debe trabajar en estándares unificados para la fabricación de sensores y dispositivos, teniendo como prioridad la **privacidad, seguridad y protección de datos**. En este sentido, en SEUR implementamos políticas de privacidad estrictas con el objetivo de asegurar que los datos que se están recogiendo están protegidos y son realmente necesarios para los servicios que ofrecemos.

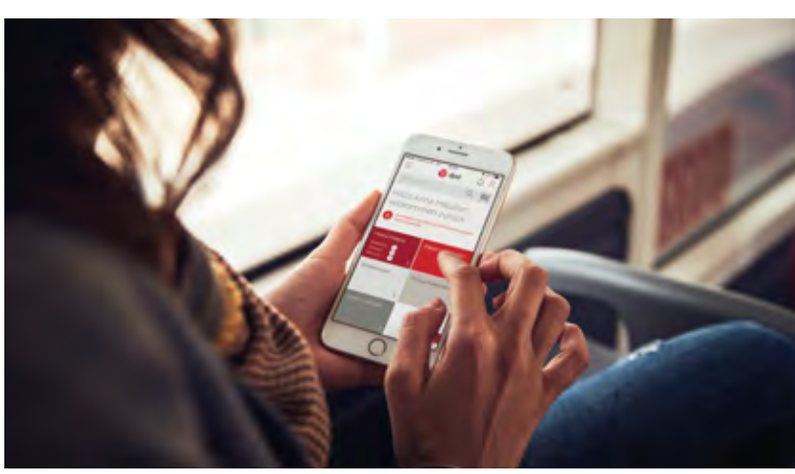
Y es que, sin lugar a dudas, esta nueva economía hiperconectada introduce grandes ventajas y facilidades para empresas e individuos, pero también entraña importantes riesgos que debemos ser capaces de neutralizar.

connection between people and devices, devices with sensors and sensors with data, which will change our processes and will transform the day-to-day life of people and businesses.

Thus, the biggest challenge for a company is to have knowledge or control of the information that comes out of our networks, or which data is being captured by unsuspected devices. We need to establish procedures to ensure that the security requirements of these devices have not been ignored.

Not surprisingly, according to **Cisco's Annual Report on Cyber Security 2017**, which involved some 3,000 Corporate Security Officers from 13 countries around the world, cybersecurity is one of the strategic objectives of the highest priority for senior executives of the participating companies. The report also reveals that while 60% of respondents believe that their company's security systems are effective or highly effective, about one-third have had some security breach over the last year with an impact on their customers or incomes.

“Cybersecurity is one of the strategic objectives of the highest priority for senior executives of the participating companies”



To my mind, we must work on unified standards for the manufacture of sensors and devices, with a focus on **privacy, security and data protection**. To this point, we implement in SEUR a strict privacy policy, aiming to ensure the data that is being collected are protected and necessary for the services we offer.

This new hyper connected economy has undoubtedly great advantages and facilities for companies and individuals, but it also entails important risks and we must have the ability to neutralize them.

Ciberseguridad en la industria interconectada

Cybersecurity in the interconnected industry

MIRIAM GARCÍA ❙ El ya presente de la industria está ligado a la **interconexión de las máquinas** y a su **intercambio de información** a través de Internet. Es evidente que esta situación conlleva numerosas ventajas, pero también algunos riesgos derivados de la conexión a Internet, en muchas ocasiones, por la falta de seguridad en el **diseño del sistema** (o security by design), y en otras, por la rápida evolución de la técnica que deja obsoletas las tecnologías y las medidas de seguridad adoptadas en ellas.

Se vaticina que tras la conexión de las máquinas, algo que ya ocurre en el sector de la elevación para monitorizar el mantenimiento del ascensor o alargar la vida de sus componentes, el siguiente paso es **la conexión de estas con el usuario.** En este sentido, la conexión de los ascensores con los usuarios a través de aplicaciones móviles, y el **reconocimiento facial y de voz** en el control de accesos serán algunas de las novedades que podremos ver en un futuro cercano. La interconexión con los usuarios supondrá la generación de una ingente cantidad de datos de alto valor, que podrá motivar ciberataques dirigidos.

Este panorama amplía el campo de ataque, que podría verse dirigido tanto a hacerse con el control de la máquina, como con los datos de los usuarios, impactando, por tanto, no solo en el negocio, sino también **afectando a la vida y a los derechos de los usuarios.** Así por ejemplo, el ciberataque podría ir dirigido a **hacerse con el control remoto de las funciones de un ascensor** y afectar a su disponibilidad, a **modificar los datos de su funcionamiento** o a **enviar datos erróneos a los técnicos** sobre la necesidad de mantenimiento

MIRIAM GARCÍA ❙ In today's industry, **machines are interconnected** and **exchange information** through the Internet. This situation obviously entails many advantages, but also some risks deriving from the connection to the Internet, on many occasions because of a lack of **security by design**, and on others, because technical advances occur so quickly that technologies and their accompanying security measures become obsolete.

Now that machines have been connected among themselves, like in the elevator sector for monitoring elevator maintenance and extending component service life, the next step is predicted to be **their connection with users**. Thus, in the near future we can expect to see elevators being connected with users through cell-phone applications, and **facial and voice recognition** being used to control access. These connections with users will generate a huge volume of high-value data that may give rise to targeted cyberattacks.

This outlook widens the scope for possible attacks to include those directed at gaining control of machines and those aiming to obtain user data. Attacks, then, will not only affect business itself, but also **the lives and rights of users.** For example, cyberattacks could attempt **to remotely control an elevator's operation** and affect its availability, **modify its operating data**, or **send erroneous information to technicians** regarding its need for maintenance. In the second of these cases, the theft of data, and especially sensitive data such as biometrics, puts users' privacy at risk.

"Not just technical but also legal cybersecurity. In the era of Digital Transformation, **digital environments**

del mismo. En el segundo de los casos, la obtención de datos de usuarios máxime cuando se trata de datos sensibles como los biométricos, pone en riesgo la privacidad del usuario.

«No solo ciberseguridad técnica, también jurídica. En la era de la Transformación Digital, **se precisa seguridad jurídica también en los entornos digitales**, ya que los ciberincidentes no solo afectan la seguridad de la información sino que pueden tener un fuerte impacto en los derechos y libertades de los ciudadanos y de las empresas»

Uno de los principales riesgos son l**as brechas de seguridad** con la fuga de información y entre ella, datos personales. Si ello ocurriera, **la responsabilidad por la fuga de información recaería sobre la empresa** quien tendría que demostrar que adoptó las medidas de seguridad jurídicas, técnicas y organizativas suficientes conforme al estado de la técnica para evitarla. Además, en caso de brecha de seguridad con fuga de datos personales, **la empresa deberá notificar el incidente a la autoridad de control pertinente**, en este caso, la Agencia Española de Protección de datos, en el plazo de 72 horas, incluyendo información sobre la naturaleza de la brecha, las consecuencias para los derechos de los usuarios, así como las medidas adoptadas para mitigar el incidente.

“En la era de la Transformación Digital, se precisa seguridad jurídica también en los entornos digitales”

Este incidente no solo podría tener consecuencias a nivel de responsabilidad de la empresa, sino que también lo tendrá en su **buena imagen o reputación.** Pero no solo eso, sino que, además, podrá tener un **fuerte impacto en la vida de los usuarios** al infringir sus derechos y libertades fundamentales. Para evitar estas situaciones, las empresas pueden y deben apoyarse en **programas de compliance** que de una manera proactiva mitigan los riesgos. Para ello, las empresas deben haber identificado y analizado previamente los riesgos a los que están expuestas, y tras ello, proceder a gestionarlos anticipándose al incidente. En materia de seguridad, además, es posible apoyarse en una gran cantidad de buenas prácticas, como por ejemplo, la adopción de los principios **security by design** y **security by default** en los sistemas y redes informáticas; y en **estándares internacionales,** como por ejemplo, la serie de normas ISO/IEC 27000 sobre seguridad de la información o la serie de normas ISO 31000 sobre gestión del riesgo.

also require legal security because not only do cyberincidents affect information security, they can also have a strong impact on the rights and freedoms of citizens and companies."

One of the main risks is **security breaches** involving information leaks and, among those, leaks involving personal data. Should this happen, **responsibility for the information leak would fall on the company,** which would have to prove that it took adequate technologically up-to-date legal, technical, and organizational measures to prevent the incident from taking place. Furthermore, if the security breach involves the leaking of personal data, **the company must inform the relevant authorities**—in this case, the Spanish Data Protection Agency (AEPD)—within seventy-two hours, sending them information on the nature of the breach, its consequences for the rights of users and the measures adopted to mitigate the effects of the breach.

“In the era of Digital Transformation, digital environments also require legal security”

MIRIAM GARCÍA
Abogada especialista en Ciberderecho & Compliance en Ecix Group
Lawyer specialized in Cyberlaw and Compliance at Ecix Group

Such an incident could have consequences not only regarding the company's responsibility, but it could also damage its **image or reputation**. Not only this, but it could even have a **strong impact on users** because of its infringement of their basic rights and freedoms. To avoid these situations, companies can and must rely on **compliance programs** that proactively mitigate risks. To this end, companies must first identify and analyse the risks they are exposed to, and then manage these by anticipating incidents. Furthermore, in m atters of security, companies can resort to a wide range of good practices that include applying the principles of **security by design** and **security by default** to computer systems and networks, and adopting international standards, such as the ISO/IEC 27000 series on information security or the ISO 31000 series on risk management.

Ciberseguridad, ¿moda o necesidad?

Cybersecurity, fashion or need?

LA HUMANIDAD EN EL ALBOR DE UNA NUEVA ERA DIGITAL

La sociedad del siglo XXI está expuesta en la actualidad a una serie de cambios que bien se pueden parecer a los que anticipaban algunos libros y películas futuristas de los años 60 (coches autónomos, video conferencia, robots, etc). Lo cierto es que **nadie conoce con certeza el futuro**, ni lo que nos deparará, aunque sí que es posible intuir que la humanidad se encuentra muy cerca de un posible cambio de época o de era.

Las nuevas tecnologías han irrumpido en el panorama global, de una forma diferente a como se han introducido otros avances tecnológicos, en otras épocas. La diferencia de la situación actual de otros avances radica en que principalmente **los avances están llegando primero a las personas y son las empresas las que tienen que adaptar sus procesos internos** con objeto a introducir esas tecnologías, cuando en el pasado era el ciudadano de a pie quien tenía que adaptar sus hábitos a los nuevos avances que las empresas proponían.

LA PALANCA DE LA TRANSFORMACIÓN DIGITAL

Las empresas y otras organizaciones (organismos públicos, ONGs, etc) están acostumbradas al dinamismo, raro es que nos encontremos una empresa que no haya cambiado su modelo operativo en los últimos cincuenta años. Estos cambios, salvo agotamiento de ciclos de modelo de negocio, se llevan a cabo mediante leves adaptaciones continuas que permiten

HUMANITY IN THE DAWN OF A NEW DIGITAL ERA

The society of the 21st century is currently exposed to a series of changes that may well resemble those anticipated by some futuristic books and films of the 60s (autonomous cars, video conferences, robots, etc). The truth is that no o**ne really knows about the future**, although it is possible looking a little bit forward about humanity and realize how close we are to a possible change of era.

New technologies have emerged onto the global scene, in a different way how other technological advances have emerged in the past. The difference between the current situation from other past technological advances is in **how are reaching people first. The companies have to adapt their internal processes** in order to introduce these technologies. While in other past situations the consumers were the ones who had to adapt their habits to the new technological advances.

THE LEVER OF THE DIGITAL TRANSFORMATION

Companies and other organizations (public bodies, NGOs, etc.) are used to dynamic environment, it is rare to find a company that has not changed its operating model in the last fifty years. These changes, except for exhaustion of business model cycles, are carried out by slight continuous adaptations that allow gradually to change the approach of the organizations to the new consumer 's needs. **Consumers do not change significantly but they have an adaptation period associated by both parties.**

ir virando de forma gradual la aproximación de las organizaciones a las nuevas necesidades que puede tener el consumidor, principalmente porque estas nuevas necesidades o **hábitos del consumidor no cambian de forma abrupta sino que llevan asociado un periodo de adaptación por ambas partes.**

Las nuevas tecnologías tienen una característica principal que lo diferencian de otros avances, primero que **son baratas** (o se abaratan con el tiempo) y segundo que **no entienden de fronteras**, por lo que permite su difusión entre todos los consumidores en periodos de tiempo cortos. Esta característica principal afecta significativamente a los modelos de negocio de diferentes maneras:

"Los hábitos del consumidor no cambian de forma abrupta sino que llevan asociado un periodo de adaptación"

1. Puede cambiar **la cadena de valor e incluso transformarla**. Las nuevas tecnologías pueden cambiar los hábitos de los consumidores cambiando el modo en como consumen los bienes y servicios, como por ejemplo en la industria hostelera de reparto de comida a domicilio, con empresas que se dedicaban casi en exclusiva a ello (Telepizza, PizzaHut, Domino's, etc) que se han visto en muy poco tiempo a competir con gran parte de la oferta hostelera de una ciudad (Just Eat, La nevera roja, Uber Eats, etc). Pero también incluso a transformarla por completo como ocurrió con la industria musical en la que se ha pasado de comprar un medio como un CD/DVD (Sony, Virgin, etc) a comprar un servicio de pago por uso (Spotify, Apple Music, etc).

2. Posibilita **crear oportunidades de negocio**, muchas veces incluso sobre ideas o conceptos que ya existían, pero sobre los que no había medios. Un caso muy claro de nuevas oportunidades de negocio

New technologies have a quite characteristics that differentiate it from other advances, first **they are cheap** (or become cheap along time) and second new technologies do **not understand about borders**, so spreading among all consumers in short periods of time is feasible. These main characteristics affects significantly the business models in different ways:

"Consumers do not change significantly but they have an adaptation period associated "

1. Changes **in value chain or even transform it**. New technologies can change the habits of consumers by changing the way they consume goods and services, such as in the industry of food delivery. Specific companies were almost exclusively dedicated to it (Telepizza, PizzaHut, Domino's, etc) They have been placed in a very short time competing with the majority part of the city restaurant offer (Just Eat, The red fridge, Uber Eats, etc). But also the chain value could be transformed completely as it happened with the music industry. Consumer in the past were used to buying items as a CD / DVD (Sony, Virgin, etc) to buy a pay-per-use service (Spotify, Apple Music, etc).

2. It is possible **to create new business opportunities**, mainly on ideas or concepts that already existed, but on which there were no way of making business. A very clear case of new business opportunities can be found in the transport industry with the irruption of vehicles for micro renting in cities (emov, Zity, car2go, etc), which would not be possible due to lack of agility without the use of the new technologies.

3. Encourages **the appearance of new players** to the extent that they can use new technologies to target specific groups of consumers who are willing to use only new technologies, defining adhoc operating models for these consumers.

The existing companies have two important challenges in trying to adapt to this new scenario. On one hand, it has to c**ontinue providing service to its current clients**, with traditional approaches, on the other hand they have **to incorporate new technologies into their processes**; in order to allow them to relate to the digital client of today and the future (the digital natives). This process is usually known as digital transformation in organizations and have as a fundamental element the incorporation of new digital trends in the processes of the company.

This process of introducing new technologies in organizations, will cause a greater **technological**

lo podemos encontrar en la industria del transporte con la irrupción del microalquiler de vehículos en ciudades (emov, Zity, car2go, etc), que no sería posible por falta de agilidad sin la utilización de las nuevas tecnologías.

3. Favorece la **aparición de nuevos jugadores** en la medida de que estos pueden utilizar las nuevas tecnologías para dirigirse a colectivos específicos de consumidores que estén dispuestos a utilizar únicamente las nuevas tecnologías, definiendo modelos operativos adhoc para estos consumidores.

Las empresas ya existentes tienen dos hándicaps importantes a la hora de poder adaptarse a este nuevo escenario. Por una parte tienen que **seguir prestando servicio a sus actuales clientes**, con medios más tradicionales; por otra parte tienen que **incorporar las nuevas tecnologías a sus procesos**, que le permitirán relacionarse con el cliente digital de la actualidad y con el del futuro (los nativos digitales). Este proceso se suele conocer como transformación digital en las organizaciones y tienen como un elemento fundamental la incorporación de las nuevas tendencias digitales en los procesos de la empresa.

Este proceso de introducción de nuevas tecnologías en las organizaciones va a provocar un mayor **apalancamiento tecnológico** (o dependencia de las tecnologías) de las empresas, en la medida que cada vez los procesos internos necesarios para funcionar serán más digitales y requerirán de la tecnología para funcionar. Según hemos visto anteriormente, la transformación digital plantea una serie de ventajas y de retos evidentes a todas las empresas, pero hay otro aspecto que es común a todas las organizaciones que está ligado al apalancamiento tecnológico y que emerge como necesario en este nuevo entorno, este es el de la Ciberseguridad como **elemento que preserve la tecnología de los riesgos asociadas a esta.**

EFECTO ESTABILIZADOR DE LA CIBERSEGURIDAD

De la misma forma que hoy en día no podríamos entender la sociedad sin la energía eléctrica, **la nueva era digital no podrá entenderse sin la Ciberseguridad**, entendiendo la Ciberseguridad como un elemento necesario que aportará confianza y estabilidad a todo el entorno digital, y en consecuencia a empresas, gobiernos y ciudadanos como parte de la sociedad.

La introducción de la Ciberseguridad en el ecosistema tecnológico probablemente no se haga de forma gradual, a pesar de que se están realizando esfuerzos en la actualidad, sino que como ha ocurrido en ocasiones anteriores en la historia de la humanidad el grado de importancia que tome sufra un aumento

leverage in companies (or technology dependence), to the extent that each time the internal processes necessary to operate will be more digital and will require technology to function. As we have seen before, digital transformation offer some advantages and obviously also some challenges for all companies, but there is another common aspect to every organizations that is linked to this technological leverage and emerges as necessary in this new environment. This topic is realizing that Cybersecurity is a necessary **element that preserves the technology from the risks associated**.

THE STABILIZING EFFECT OF CYBERSECURITY

In the same way that today we could not understand society without electricity, **the new digital era can not be understood without Cybersecurity**. Cybersecurity should be also understand as a necessary element that will bring confidence and stability to the entire digital environment, and therefore to companies, governments and citizens as part of the overall society.

The introduction of Cybersecurity in the technological ecosystem will not be probably implemented gradually (even though some current efforts are in plance). As in other previous occasions in the history of humanity, the Cybersecurity relevance will suffer a

DANIEL LAGARCHA LAMELA
Director del Centro de Ciberseguridad en ISMS
Director of the Cybersecurity Center at ISMS

importante una vez se hayan los efectos devastadores de una ausencia o aplicación inadecuada.

La Ciberseguridad es una disciplina relativamente joven, que aún es necesario desarrollar y que además **siempre tendrá una dependencia directa con la tecnología** (que es recíproca). La evolución de la Ciberseguridad en los próximos años se pivotará en tres factores principales. El primero es el de la propia tecnología, la Ciberseguridad requiere de herramientas tecnológicas que deberán adaptarse a los nuevos entornos digitales, esta adaptación está llegando aunque a una velocidad inferior a la del resto de la tecnología, por ahora. El segundo factor, es el de la regulación, la nueva economía digital no entiende de fronteras ni de aranceles y además es capaz de sortear las leyes de los países para establecerse en ámbitos no regulados que le permiten mayor libertad para operar. Con la aparición de las leyes NIS y GDPR en la UE o la ley de Ciberseguridad China, se percibe la importancia que está tomando la Ciberseguridad y la privacidad en los países, que tratan de poner coto de alguna mediante una serie de reglas fundamentales a la nueva economía digital.

“La nueva era digital no podrá entenderse sin la Ciberseguridad”

El tercer factor y más importante es **el de las personas,** no solo porque la Ciberseguridad va a requerir de profesionales adecuadamente formados (se espera que para el 2020 la demanda de profesionales de seguridad se incremente en un 50%), sino porque independientemente de que trabajemos en el sector de la Ciberseguridad, la cultura de Ciberseguridad en toda la sociedad va a jugar un papel de mayor peso. El hecho de que cada uno de nosotros tenga una adecuada cultura de Ciberseguridad será un aspecto fundamental ya sea en nuestro ámbito profesional cualquiera que sea, como ciudadanos de esta sociedad actual (como votantes, padres, contribuyentes, consumidores de productos/ servicios, etc).

La cultura de Ciberseguridad deberá ser el factor más importante sobre el que se debe construir la nueva economía digital, cuanto antes empecemos a construir menor esfuerzo nos costará cambiar lo que ya hay construido. Aunque ya sabemos que el ser humano tiene cierta tendencia a tropezar primero para después levantarse.

significant increase once the devastating effects of its absence or inadequate implementation.

Cybersecurity is a relatively young discipline, which still needs to be developed Cybersecurity **will always also have a direct dependence on technology** (which is reciprocal). The evolution of Cybersecurity in the upcoming years will be based on three main factors. First is the technology itself, Cybersecurity requires technological tools that must adapt to the new digital environments. This adaptation is currently in place nevertheless at a speed lower than the rest of the technology yet. The second factor is about regulation, the new digital economy does not understand borders or international taxes, and is also able to elude the country laws in order to look for unregulated areas that allow them more freedom to operate. With the appearance of the NIS and GDPR laws in the EU or the Chinese Cybersecurity law, the countries have perceived the importance around Cybersecurity and Privacy. Countries are trying to put in place some fundamental rules to the new digital economy.

“The new digital era can not be understood without Cybersecurity”

The third and most important factor **is about people.** Is not just because its importance about Cybersecurity sector that will require well trained professionals (it is expected that by 2020 the demand for security professionals will increase by 50%), but also because the culture around Cybersecurity in all of society will play a more significant role. The fact that everyone has an adequate Cybersecurity culture will be a fundamental issue no matter what is our professional field, because it would be more important as citizens of current society (as voters, parents, taxpayers, consumers of products / services, etc).

The culture of Cybersecurity should be the most important factor on which to build the new digital economy, the sooner we start to build the less effort will cost to change what is already built. Although we already know that the human being has a tendency to stumble first and then get up.

¿Preparado para el Ciber Riesgo? El Seguro Ciber Protección

Are You Ready for Cyber-risk? The Cyber Protection Insurance.

FERNANDO MONTERO | El entorno que nos rodea ha cambiado, especialmente en materia de tecnología. Estamos viviendo una **transformación digital**, tanto en nuestra vida privada como en la profesional, siendo cada vez más dependientes del entorno digital. Pasamos de un entorno Off Line a un entorno On Line.

La tecnología nos facilita mucho la vida pero también nos expone a nuevos riesgos, muchos de ellos aún desconocidos. Igualmente en el mundo de las empresas (y de la industria), todas las estrategias pasan en mayor o menor medida por:

- **Automatización y optimización** de procesos.
- Transformación digital, buscando **omni-canalidad** y el mayor conocimiento del cliente.
- Uso inteligente del **"Data"** y **"Big Data"**.

Estamos viviendo una invasión de la tecnología de la recogida de datos hasta el punto que estamos en la democratización de la producción informativa, almacenar el dato es hoy mucho más barato.

Todo esto nos lleva a la situación que, una empresa cuanto más digital sea, más automatización tenga implementada y más transacciones y datos guardados tenga (o quiera tener), más vulnerable será.

Por tanto, el uso masivo de la tecnología hace necesario que las empresas mantengan una actitud proactiva frente a los riesgos que conlleva.

FERNANDO MONTERO | Our environment has changed, especially in terms of technology. We are experiencing a **digital transformation**, both in our private life as in our professional one, becoming every time more dependent on the digital environment. We pass from an offline environment to an online environment.

Technology makes our life a lot easier, but it also exposes us to new risks, many of them still unknown. The same happens with companies (and industries), every strategy, to a greater or lesser extent, goes through:

- **Automation and optimization** of the processes.
- Digital transformation, searching for **omnichannel** and a better knowledge of the client.
- Smart use of **data** and **big data.**

We are experiencing a data gathering technology invasion to the point of being in the democratization of informative production; today it is cheaper to store data.

This prompts us to a situation in which the more digital a company is, the more automation it has implemented and the more data and transactions it has kept (or wants to keep); the more vulnerable it will be.

Therefore, the massive use of technology makes it necessary for companies to maintain a proactive attitude to face the risks it involves.

Esta tendencia se confirma con los siguientes datos:

- EL 89 % de las empresas competirán en base de la **“Experiencia Cliente”**.
- El 90% de las empresas tienen como prioridad la **“Transformación digital**”.
- En 20 años, **el 75 % de la masa laboral habrá “nacido digital”**
- El 77 % de las empresas **ven el “Mobile” como una prioridad.**

En el mundo de las empresas y los profesionales, los datos y su conocimiento marcan las estrategias y en muchas ocasiones la seguridad de la información es la clave para garantizar la continuidad del negocio.

“El uso masivo de la tecnología hace necesario que las empresas mantengan una actitud proactiva frente a los riesgos que conlleva”

Todas las empresas son susceptibles de sufrir ataques ciber, por tanto la concienciación en la inversión en seguridad/prevención es fundamental.

Estar protegido ante un ataque ciber no es solo una cuestión de seguridad, va más allá, **afecta directamente a la competitividad de un negocio**. Estos ataques se están incrementando de forma exponencial y se dan en todos los sectores de actividad.

Las pymes y profesionales son los que más vulnerabilidades presentan:

- Por **desconocimiento** de las amenazas.
- Solo el 40 % disponen de **infraestructuras digitales correctamente garantizadas**.
- Tienen **acceso a grandes corporaciones** a través de sus webs.
- Un 70 % de ataques ciber se producen a compañías **de menos de 100 empleados**.
- Se disponen de niveles de protección adecuados en PC´s pero **no se protegen los dispositivos móviles**.

España es **el primer país de Europa en utilización de servicios “Cloud” en estrategias de negocio**. Somos el tercer país en sufrir ataques ciber después de EEUU y UK.

La ciber-seguridad consiste en disponer de un conjunto de herramientas y protocolos para salvaguardar la seguridad de la información que cualquier gestor de datos de terceros utiliza con el objetivo de proteger el patrimonio y los activos.

Dentro de este conjunto de herramientas se encuentra el **Seguro Ciber Riesgo**.

El Seguro Ciber Riesgo contiene una serie de garantías que se otorgan consecuencia de:

This is confirmed with the following data:

- 89% of companies will compete based on **“Client Experience”.**
- 90% of companies have **“Digital Transformation”** as a priority.
- In the next 20 years, **75% of workers will be “digital born”.**
- 77% of companies **see “Mobile” as a priority**.

Among companies and professionals, data and its knowledge set the strategies and, on many occasions, information security is the key to ensure business continuation.

“The massive use of technology makes it necessary for companies to maintain a proactive attitude to face the risks it involves”

Every company is open to suffer a cyberattack, thus it is fundamental to raise awareness to invest on security and prevention.

Being protected against a cyberattack is not just a security matter; **it affects directly business competitiveness**. These attacks are increasing exponentially and happen in every sector.

FERNANDO MONTERO DE ESPINOSA
Mediador de Seguros Titulado del Grupo AXA
Qualified Insurance Intermediary at Grupo AXA

- Un **ataque informático** doloso perpetrado en los sistemas informáticos del asegurado.
- Un **código maligno informático** (Malware) activo en los sistemas informáticos del asegurado.
- Un **error humano** cometido en los sistemas informáticos del asegurado.
- Una **extorsión cibernética**.

¿Por qué contratar un Seguro Ciber Riesgo?

Cualquier empresa que maneje datos está expuesta al Ciber Riesgo. Los datos almacenados en soportes electrónicos supone una amenaza para cualquier organización. Los ataques cibernéticos aumentan cada día más y ninguna empresa o profesional está seguro al 100 % de recibir estos ataques, no importa el tamaño de la compañía ni el sector.

Las estadísticas indican que el origen de las infecciones son:

- El 39 % por uso de **webs poco seguras.**
- 23 % **descarga de programas en la red.**
- 19 % malware **recibido por correo electrónico.**
- 91 % de las pymes **sufren ataques a diario.**
- Tan solo el 25 % de los dispositivos móviles (Teléfono y Tabletas) de las empresas **disponen de software de seguridad.**

“España es el primer país de Europa en utilización de servicios “Cloud” en estrategias de negocio”

¿Cuáles son las garantías y prestaciones más destacables de los seguros Ciber Riesgo?

- Gastos de **recuperación de datos borrados.**
- Gastos de **restauración de los sistemas de acceso** consecuencia de bloqueos de los mismos.
- Gastos de **descontaminación del virus** (código maligno informático).
- **Asesoramientos** de profesionales expertos en ataques informáticos.
- **Responsabilidad Civil por perjuicios patrimoniales de terceros**, con la posibilidad de contratar sumas aseguradas elevadas.
- **Responsabilidad Civil Administrativa** por el incumplimiento de la **LOPD.**
- **Servicios de Asistencia**:
  - Borrado de huella digital.
  - Asistencia Técnica (HELP DESK).
  - Asesoramiento profesional de expertos en ciber extorsión.
- **Gestión de Crisis:**
  - Gastos de notificación a afectados.
  - Gastos de recuperación de imagen y daño reputacional en redes sociales incluyendo la protección de la identidad.

SMEs and professionals are the most vulnerable segments:

- For **ignoring** the threats.
- Only 40% of them have **digital infrastructures correctly guaranteed.**
- They have **access to big corporations** through their webs.
- 70% of cyberattacks are produced to **companies with less than 100 employees.**
- They have proper protection level on PCs but **mobile devices are not protected.**

Spain is the first country in Europe to use cloud services in business strategies. We are the third country in the world suffering cyberattacks after USA and UK.

Cybersecurity consists in having a combination of tools and protocols to safeguard the information security that any manager of third party data uses in order to protect assets.

In this combination of tools we find the **Cyber Risk Insurance**.

The Cyber Risk Insurance includes a series of guaranties given as a consequence of:

- An **intentional computer attack** committed on the insured’s computer systems.
- A **malicious computer code** (malware) active in the insured’s computer systems.
- A **human mistake** made on the insured’s computer systems.
- A **cybernetic blackmail**.

Why should you contract a Cyber Risk Insurance?

Any company handling data is exposed to Cyber Risk. Data stored in electronic formats means a threat for any organization. Cybernetic attacks are increasing every day and no company or professional is 100% safe from suffering these attacks, no matter the company’s size or the sector.

Statistics show that the origins of infections are:

- 39% of them use **unsafe webs**.
- 23% **download programs from the net.**
- 19% **received malware in the mail.**
- 91% of SMEs **suffer daily attacks.**
- Only 25% of the companies’ mobile devices (phones and tablets) **have security software.**

“Spain is the first country in Europe to use cloud services in business strategies”

- **Servicio forense de peritos informáticos judiciales.**
- Pérdida de beneficios por **interrupción del negocio.**
- **Equipos de sustitución** para continuidad de negocio.

¿Cuáles son las tres claves para prevenir los ataques ciber?

- **Análisis del riesgo:** Conocer el nivel de concienciación frente al ciber riesgo, identificar los sistemas y datos de interés que pueden ser atacados y estimar el coste de recuperación.
- **Establecer un plan de seguridad:** Implementar mecanismos de detección y defensa, revisar consecuencias legales frente a un ataque, diseñar un plan estratégico frente a una brecha de seguridad.
- Disponer de un equipo humano **formado y disciplinado.**

"Los ataques cibernéticos aumentan cada día más y ninguna empresa o profesional está seguro al 100% "

Por tanto, el Seguro Ciber Riesgo se presenta como una herramienta y mecanismo de seguridad que puede llegar a ser clave en momentos complejos. Incorpora coberturas de asistencia otorgadas por especialistas, de responsabilidad civil para paliar daños a terceros y sanciones relacionadas con la LOPD, de reposición de imagen y de pérdida de explotación, todos puntos sensibles que ayudarán a mantener la competitividad consecuencia de un ataque o negligencia ciber.

What are the most remarkable guarantees and features of Cyber Risk insurances?

- Cost of **recovering erased data.**
- Cost of **restoring access systems** due to their block.
- Cost of **virus decontamination** (computer malicious code).
- **Advice** from professionals, expert on computer attacks.
- **Public liability for third party heritage damage**, with the possibility of contracting high insured sums.
- **Administrative public liability** for LOPD's unfulfilment.
- **Support services**:
  - Digital trace erasing.
  - Technical support (HELP DESK).
  - Professional advice from cyberblackmailing experts.
- **Crisis management**:
  - Cost of notification to the affected.
  - Cost of recovering the image and reputation in social networks, including identity protection.
- **Forensic service from legal computer experts**.
- Loss of profit by **business interruption**.
- **Replacement equipment** for business continuation.

Which are the three keys to prevent cyberattacks?

- **Risk analysis**: Knowing awareness-raising level when facing cyber risk, identifying systems and data of interest that could be attacked and estimating recovering cost.
- **Establishing a security plan**: Implementing detection and defence mechanisms, reviewing legal consequences against an attack, designing a strategic plan against a security breach.
- Having a **trained and disciplined** human team.

"Cybernetic attacks are increasing every day and no company or professional is 100% safe"

Thus, the Cyber Risk Insurance appears as a tool and security mechanism that may be key in difficult moments. It includes assistance coverage consented by specialists, public liability coverage to alleviate third party damage and fines related to LOPD, and it covers image recovery and operating loss. All these are sensitive points that will help maintaining competitiveness after a cyberattack or negligence.

Retos de la ciberseguridad en el actual entorno empresarial

Cybersecurity challenges in the current business environment

espaitec
Parc Científic, Tecnològic i Empresarial de la Universitat Jaume I de Castelló

La Ciberseguridad, entendida como la **protección de la información digital que "vive" en los sistemas interconectados** y un elemento de concepto más amplio de Seguridad de la Información, ha tomado una relevancia sin precedentes, tanto en el ámbito tecnológico como económico ya que el impacto que supone un ciberataque a unas instalaciones provoca unas pérdidas considerables para el afectado pero también un beneficio económico importante para el atacante. En el **I Foro Ciberseguridad en Empresas**, celebrado en Valladolid el 19 de Octubre de 2017, Alberto Hernández, director general del Instituto Nacional de Ciberseguridad de España (Incibe) apuntó a que el cibercrimen reportaba un beneficio de más de 1 Billón (con b) de euros anuales. Sólo en España, según INCIBE, se detectan **más de 100.000 ataques diarios a redes de comunicación en general.** En el caso de las PYMES se ha pasado de los 18.000 ataques recibidos en sus sistemas de información en 2015 a los 120.000 del 2017, con un incremento en el nivel de sofisticación importante, lo que nos da una idea de la envergadura del problema.

Sin embargo, es bien cierto que es un mercado de oportunidades "in-crescendo". Alberto Hernández remarcaba que la facturación mundial anual ascendía a **72.000 millones de euros** creciendo a un ritmo de entre el 11% y el 13% anual mientras que en España, esta cifra, a finales de 2017, fue de **1.200 millones** con un incremento esperado por ejercicio del 13% para los próximos cuatro años, un punto por encima de la media europea. Hernández señalaba que en nuestro

So much unmatched importance has been attached to cybersecurity, which is **how protecting the digital information "living" in interconnected systems** and an element with a much broader concept about Security of Information is known as, in both technology and economic domains because the impact that a cyberattack has on installations causes considerable loss for the affected party, but also an excellent economic profit for the attacker. During the **1 Forum on Cybersecurity in Companies** held in the Spanish city of Valladolid on 19 October 2017, Alberto Hernández, the General Director of the Spanish National Cybersecurity Institute (Incibe), pointed out that cybercrime made a profit of more than 1 billion (with b) euros every year. According to INCIBE, **more than 100,000 daily attacks on communication networks** have been generally detected in Spain alone. Attacks on SMEs' information systems have gone from 18,000 in 2015 to 120,000 in 2017, and their level of sophistication has also substantially increased. These figures allow us to understand just how big this problem has become.

However, it is also true that it represents an "in-crescendo" market of opportunities. Alberto Hernández, stressed that the world's annual turnover came to **72,000 million euros**, which grew at a rate of between 11% and 13% a year. This figure in Spain was **1,200 million euros** at the end of 2017, is expected to increase yearly by 13% over the next 4 years, which is 1 point above the European mean. Hernández indicated that, surprisingly, Spain exports some 290 million euros in cybersecurity technology and services to Germany, France, Italy or the UK. Such

país se constata una exportación de 290 millones de euros en tecnología y servicios de ciberseguridad a Alemania, Francia, Italia o Reino Unido, aunque pueda sorprender, y es una actividad que emplea directamente a 6.000 personas.

"Sólo en España, según INCIBE, se detectan más de 100.000 ataques diarios a redes de comunicación"

Así, otra derivada es **la necesidad urgente de formar adecuadamente a los profesionales del sector de la Ciberseguridad** por el incremento en la necesidad de incorporar expertos en Ciberseguridad en empresas y entidades para combatir ciberataques tanto en **entornos IT** (Information Technology – tecnologías de la información por sus siglas, formados por los ordenadores, servidores y servicios en la nube de cualquier empresa) como en los recientes, con mayor crecimiento, **entornos OT** (Operation Technology – tecnologías de la operación) o **IoT** (Internet of Things) que lo forman esos dispositivos (sensores, SCADA, PLCs) con una capacidad de computación limitada que simplemente proporcionan datos y controlan el funcionamiento de determinados procesos. Según Gartner Inc., en 2018 se estima que habrán instalados más de **11.000 millones de dispositivos conectados a internet** con un incremento de más de un 30% anualmente, donde las aplicaciones del segmento de consumidor representarán un 63% del total.

Los entornos OT/IoT poseen una complejidad mucho mayor ahora que se conectan a los IT (anteriormente se encontraban aislados y por lo tanto más protegidos de este tipo de ataques desde el exterior) sobre todo por la miríada de **protocolos de comunicación** que utilizan los dispositivos tanto a nivel de infraestructura, identificación, transporte, datos, gestión, etc, así como por el retraso tecnológico en materia de ciberseguridad, unos 15 años, respecto a lo que han evolucionado los entornos IT.

"Hasta ahora sólo las grandes empresas invertían en ciberseguridad, pero cada vez más las PYMES deberán comenzar a invertir dinero en **securizar digitalmente su negocio**. A día de hoy la gran mayoría de empresas funcionan con la información digitalizada y con herramientas tecnológicas. Si quieren poder dar continuidad a su negocio, las empresas tendrán que resolver el tema de la seguridad de esta información, puesto que sin su disponibilidad o integridad, la empresa queda parada. Hoy en día, cualquier PYME que trabaje con información, ya sea local o a la nube, está expuesta a ser atacada" indica Esteban Sardanyés, CEO de ESED, empresa especializada en Ciberseguridad e instalada en Tecnocampus (el Parc Tecnològic de Mataró-Maresme), que centra su actividad en trasladar los servicios en ciberseguridad que hasta ahora sólo utilizaban las grandes empresas a las PYMES adaptando costes y necesidades.

activity allows 6,000 people to be directly employed.

"According to INCIBE, more than 100,000 daily attacks on communication networks have been generally detected in Spain"

Another point that stems from this problem is **the urgent need to suitably train professionals in the Cybersecurity sector** given the increasing need to incorporate experts in Cybersecurity into companies and organisations to fight against cyberattacks in **IT** (Information Technology, formed by any company's computers, servers and cloud services) domains, and

JUAN ANTONIO BERTOLÍN
Director de gestión de Espaitec / Managing director of Espaitec

also in the recent, but fast-growing, **OT** (Operation Technology) or **IoT (**Internet of Things) domains that these devices form (sensors, SCADA, PLCs) with their limited computing capacity that simply provide data and control the operation of given processes. According to Gartner Inc., in 2018 it is estimated that more than **11,000 million devices will be connected to the Internet** (IoT) with an increase of more than 30% annually, where the consumer applications will represent 63% of the total.

OT/IoT domains are currently much more complex as they are connected to IT, whereas before they were isolated and, thus, more protected from such outside attacks, especially given the myriad of **communication protocols** used by devices as regards infrastructure, identification, transport, data, management, etc, as well as the delay (some 15 years) in cybersecurity-related technology compared to that developed in IT domains.

"Until the present-day, only large-sized companies invested in cybersecurity, but SMEs will increasingly have to start investing money **to digitally secure their businesses.** Nowadays, most companies work with digitalised information and technology tools. If they wish to continue their businesses, companies will have to solve the problem of securing this information because if it is not available or complete, companies

"Entre la Comunidad de Seguridad, hay una broma generalizada con respecto a la seguridad de IoT que dice 'La S de IoT es sinónimo de seguridad'. **Los dispositivos IoT suelen ser dispositivos con recursos limitados**, estos dispositivos tienen capacidades de procesamiento y batería limitadas, lo que dificulta la implementación de algoritmos complejos; por ejemplo, una rutina criptográfica que verifica si una actualización descargada es auténtica y no ha sido modificada podría agotar la batería de un dispositivo desconectado si no se implementa con cuidado. Este hecho, junto con el hecho de que los dispositivos de IoT generalmente **no están diseñados teniendo en cuenta la seguridad**, han conducido a un serio problema de seguridad. La historia se repite, el mismo problema con el diseño seguro estuvo presente con los sistemas SCADA (Supervisory Control and Data Acquisition) que ahora controlan las infraestructuras críticas a nivel nacional y son un foco para los profesionales de la seguridad de la información" advierte, Paul Santapau, CTO de Continuum Security, empresa vinculada a ESPAITEC, Parque Científico Tecnológico de la Universidad Jaume I de Castellón.

"Cada vez más las PYMES deberán comenzar a invertir dinero en securizar digitalmente su negocio"

Sin embargo, la solución no sólo pasa por implementar sistemas informáticos y aplicativos eficaces y eficientes en el combate contra ciberataques sino que **nos enfrentamos a un problema de concienciación.** Miguel Hormigo Ruiz, Director del Sector de Industria de Secure e-Solutions de GMV, empresa vinculada al Parque Tecnológico de Castilla y León, enfatiza que "desde el punto de vista doméstico es necesario que el usuario se conciencie que los dispositivos que se utilizan habitualmente (weareables, sensores domésticos, actuadores, etc.) son igualmente accesibles que inseguros. En la industria, existe un nivel de concienciación muy superior, hay que incidir en que habitualmente el equipamiento IoT no se utiliza habitualmente como elemento final sino como un elemento intermedio (gateway) que permite acceder o actuar sobre un equipamiento que en el pasado estaba o bien separado o bien accesible en una red aislada".

En resumen, el Internet de las Cosas (IoT) ha llegado para quedarse y extenderse. El hecho de tener todos los dispositivos conectados facilitarán la gestión de una gran cantidad de actividades realizadas por seres humanos e indudablemente, en muchos casos, mejorarán nuestra calidad de vida pero tenemos que ser conscientes de los peligros que conlleva la "hiperconectividad" y esto abre un escenario inimaginable de oportunidades de negocio y retos tecnológicos.

will stop. Any SME that works with information today, regardless of it being local or in the cloud, is open to attacks", says Esteban Sardanyés, the CEO of ESED, a company that specialises in Cybersecurity and is set up at Tecnocampus (the Mataró-Maresme Technology Park). ESED centres its activity on transferring cybersecurity systems that only large-sized companies have used until now to SMEs by adapting costs and requirements.

"The Security Community generally jokes about the security of the IoT, in that 'The S in the IoT is a synonym of security'. IoT devices tend to have limited resources. **These devices tend to have limited processing and battery capacities**, which makes implementing complex algorithms complicated; for instance, a cryptographic routine checks if a downloaded update is authentic and has not been amended in an attempt to exhaust the battery of a disconnected device if not carefully handled. This fact, along with the fact that IoT **devices are not generally designed bearing security in mind**, has led to a serious security problem. History is repeated: the same problem with a secure design was present with SCADA (Supervisory Control and Data Acquisition) systems, which now control critical national infrastructures and are a point for information security for professionals to focus on," warns Paul Santapau, the CTO of Continuum Security, a company linked to ESPAITEC, the Science, Technology and Business Park of the Universidad Jaume I in Castellón.

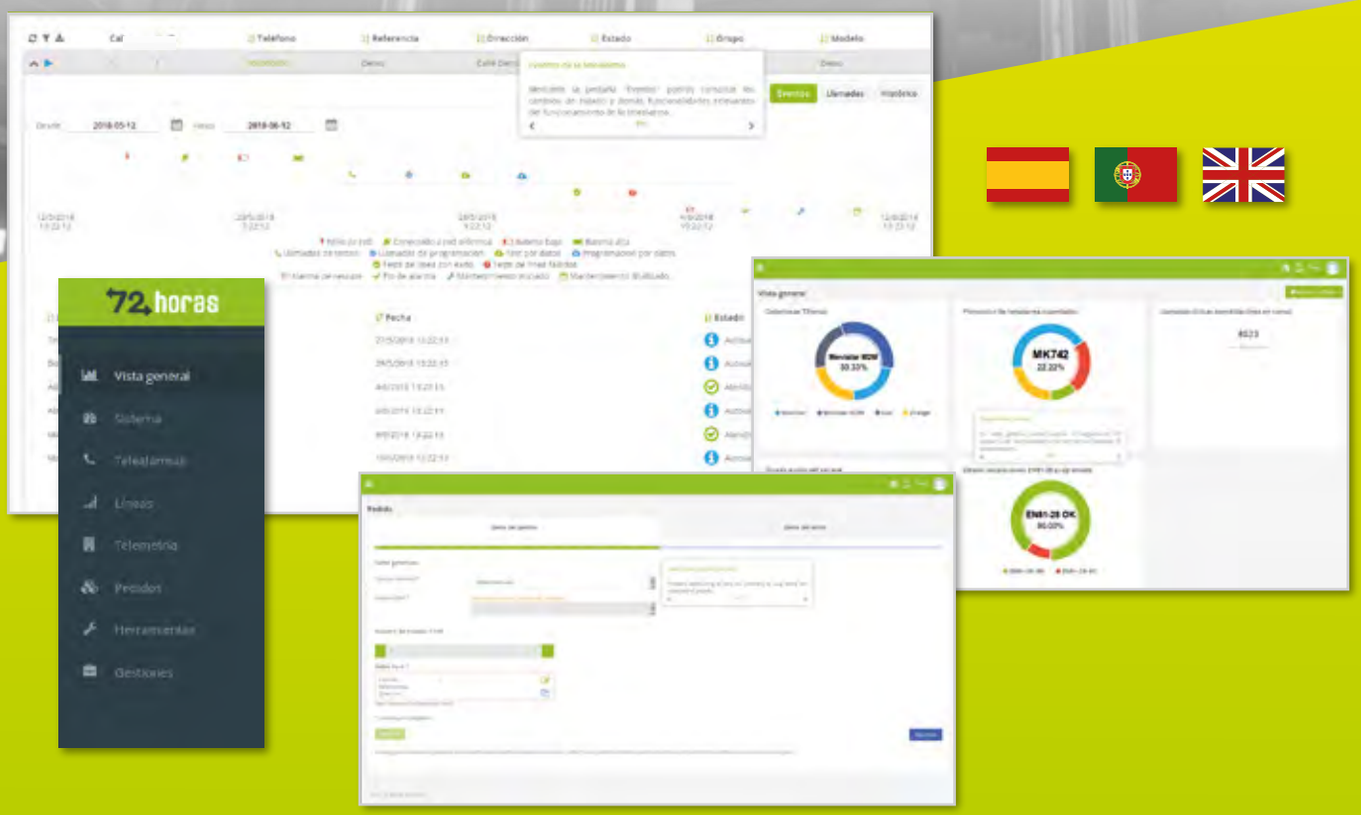
"SMEs will increasingly have to start investing money to digitally secure their businesses"

Yet the solution not only lies in implementing efficient computer and application systems to fight against cyberattacks, but **we must face an awareness problem**. Miguel Hormigo Ruiz, the Director of the Industry Sector of Secure e-Solutions of GMV, a company linked to the Technology Park of Castilla y León, stresses that "from a domestic point of view, users must be made aware that the devices they regularly use (wearables, domestic sensors, actuators, etc.) are both accessible and insecure. More awareness has been raised in industry. It is stressed that IoT equipment is not normally used as a final element, but as an intermediate element (gateway) to allow equipment to be accessed or acted on that was previously well separated or quite accessible in an isolated network".

Basically, the IoT has come to stay and be extended. The fact that all devices are connected will help a vast number of the activities performed by human beings to be managed, and will undoubtedly improve our quality of life. However, we have to be aware of the hazards that "hyperconnectivity" entails, which opens up an unimaginable scenario of business opportunities and technological challenges.

72horas

M2M TECHNOLOGIES



72HORAS MANAGER

Con la nueva plataforma online de 72horas gestiona tus dispositivos de comunicación en tiempo real y de forma sencilla. Toda la información en un clic.

With the new 72horas online platform, you can manage your communication devices in real time and with ease. All your information in one click.

www.72horas.net

NAVARSYSTEMS | 72horas M2M TECHNOLOGIES | ADVERTISIM | net4machines

Fomentar la cultura de la ciberseguridad, una labor de todos

Encouraging Cybersecurity Culture, Everyone's Work

YOLANDA CORRAL | **Ciberseguridad de tú a tú**. Ese es el propósito y el lema que me fijé en el horizonte hace un tiempo para, desde mi papel de periodista y formadora, **acercar la ciberseguridad a todo el mundo en un lenguaje comprensible** no solo para profesionales y aficionados de la seguridad sino para todos. Este era un mundo ajeno a mi trayectoria personal y profesional y hoy ya no hay vuelta atrás: la ciberseguridad me ha atrapado y **cada día pongo lo mejor de mí para contribuir a su divulgación.**

Hoy en día prácticamente todos somos usuarios de tecnología, por eso se hace imprescindible entenderla, conocer sus grandes beneficios pero también sus riesgos y eso conlleva que cada persona sea consciente que **la seguridad digital depende sin excusas de uno mismo.** Todos debemos adoptar medidas de seguridad básicas que minimicen los riesgos. Esa tarea no nos la dan hecha al adquirir tecnología y parte de cada uno el (pre)ocuparse de esto para evitar en lo posible lamentar incidentes que además son de lo más variado: virus, fraudes, extorsiones, accesos indebidos, ciberacoso, problemas con la identidad digital y la reputación online...

"La seguridad digital depende sin excusas de uno mismo"

En pleno siglo XXI es necesario que entendamos que la ciberseguridad no solo es cosa de personal más técnico como pueden ser informáticos, ingenieros,

YOLANDA CORRAL | **One on one cybersecurity.** That is the intention and the motto I set on my horizon some time ago in order to bring, from my role as a journalist and trainer, **cybersecurity closer to everyone in a language easy** to understand not only for security professionals and amateurs but for everybody. It was a foreign world for me because of my personal and professional career, but today there is no turning back, cybersecurity has grabbed me and **every day I do my best to contribute to its dissemination.**

Nowadays, almost everybody uses technology. That is why it is essential to understand it, to know its great benefits as well as its risks, and that implies everyone to be aware that **digital security depends on oneself without excuses**. Everyone must take basic security measures to minimise the risks, which is not done when acquiring technology; it comes up from everyone to care about and take on this in order to avoid, where possible, regretting a wide variety of incidents: virus, scams, blackmailing, inappropriate access, cyberbullying, digital identity problems and online reputation...

"Digital security depends on oneself without excuses"

In the middle of the 21st century it is necessary to understand that cybersecurity is not only a matter of technical personnel such as computer technicians, engineers, analysts or developers. **Cybersecurity concerns**

analistas o desarrolladores. **La ciberseguridad nos atañe a todos** y cada uno de nosotros desde el mismo momento en el que usamos tecnología o nos conectamos a Internet, por eso es básico que entendamos que **desde todos los sectores profesionales se puede contribuir a avanzar** juntos en este camino.

Se necesita **concienciación, educación y sobre todo formación** para que cale este mensaje en todos los sectores de la población, necesitamos prestar más atención a la ciberseguridad pues solo así lograremos hacer frente al cibercrimen y tendremos un Internet más seguro para todos.

El trabajo del personal con conocimientos más técnicos es imprescindible, básico y digno de alabar en todos los sentidos. Nunca me cansaré de decirlo: benditos hackers, esos grandes profesionales de la seguridad, que con su esfuerzo y dedicación diaria nos facilitan el terreno a todos los usuarios para vivir cada día un poquito más seguros en el mundo digital. Sin ellos nada tendría sentido, pero no olvidemos que para que el puzzle encaje es necesario que más allá de la parte técnica, desde otros sectores también se aporte, pues **de la suma del esfuerzo de todos, la cultura de la ciberseguridad en un mundo hiperconectado llegará más lejos.**

"Se necesita concienciación, educación y sobre todo formación para que cale este mensaje en todos los sectores de la población"

¿Cómo aporto yo al mundo de la ciberseguridad? Pues la pregunta es sencilla y la respuesta no tanto. Lo cierto es que trato de hacerlo de múltiples formas que por separado tienen sentido, pero en conjunto mucho más.

Por un lado **informando y divulgando a través de mi canal de ciberseguridad "Palabra de hacker"**. Su

every one of us from the very moment we use technology or connect to the Internet. That is why it is essential to understand that **we can contribute from every professional sector to move forward together.**

Awareness, education and, especially, training are needed for this message to make an impression on every sector of the population. We must pay greater attention to cybersecurity because it is the only way to deal with cybercrime so we all can have a safer Internet.

The work done by people with more technical knowledge is indispensable, fundamental and worthy of praise in every sense. I will never get tired of saying this: blessed hackers, great security professionals who, with their effort and daily dedication, make it easier for users to live every day a little safer in the digital world. Without them nothing would have sense, but let us not forget that, so the puzzle fits in, it is necessary that, apart from the technical area, other sectors also contribute. **With the sum of everybody's efforts, cybersecurity culture will go further in a hyperconnected world.**

"Awareness, education and, especially, training are needed for this message to make an impression on every sector of the population"

How do I contribute to cybersecurity? It is a simple question but not as simple the answer. I try to do it in different ways which make sense separately but make even more sense when combining them.

On one hand, **I inform and spread the word through my cybersecurity channel "Palabra de hacker"** (Hacker word). Its centre is the YouTube channel. However, I work on multiple platforms and I spread the content not only on videos but also on podcasts and creating other resources such as articles, infographics or presentations so that the content reaches more people. In my channel I am surrounded by great cybersecurity professionals who are passionate about sharing their knowledge. **I organise and host live cyberdebates** –like virtual round tables- with professionals about varied topics, leaving the possibility to anyone to ask questions in real time on social networks. In addition, I edit and publish videos with interviews, and talks and workshops that I record in different security events.

On another hand, I attend security events and conferences organised in many places where I always learn a lot. Furthermore, given my lively nature, I have crossed the line of organising events. **I am a founder**

centro neurálgico es el canal de YouTube pero trabajo en multiplataforma y divulgo el contenido no solo en vídeo, sino también en podcast y creando otros recursos como artículos, infografías o presentaciones para que el contenido llegue a más gente. En mi canal me rodeo de grandes profesionales de la ciberseguridad que sienten pasión por compartir su conocimiento. **Organizo y presento ciberdebates en directo** -a modo de mesas redondas virtuales- sobre diversos temas con profesionales con la posibilidad de que cualquier persona en tiempo real puede hacer preguntas a través de las redes sociales y además, edito y publico vídeos con entrevistas, y también charlas y talleres que grabo en diferentes eventos de seguridad.

Por otro lado no solo trato de asistir a eventos y congresos de seguridad que se organizan en diversos lugares en los que siempre aprendo un montón, sino que por mi naturaleza inquieta he pasado al terreno de organizar eventos. Soy **fundadora y organizadora de las Jornadas de Seguridad Informática PaellaCON** que son de carácter gratuito para todos los asistentes y también **dinamizadora de la comunidad Hack&Beers en Valencia.**

“Desde todos los sectores profesionales se puede contribuir a avanzar juntos en este camino”

Y por último canalizo el conocimiento adquirido en una faceta que me encanta: la de formadora. Entre otros temas **realizo talleres y charlas sobre seguridad digital y privacidad para organismos, empresas y allí donde se me solicita**. En este terreno además tengo la suerte de participar como formadora en un programa de formación sobre seguridad en Internet en centros educativos de diversas provincias dando talleres a profesores y alumnos. Esto me permite **tomar el pulso constantemente a los más jóvenes que por su edad son el sector más vulnerable en Internet** y ayudar a la formación del profesorado en cuestiones de seguridad que tanto necesitan. Además también soy **cibercooperante de Internet Segura for Kids-INCIBE** con lo cual sumo más experiencias desde este programa acercando la seguridad a menores y sus familias.

Si yo siendo periodista y sin tener una formación especialmente técnica de base, con esfuerzo, dedicación y tiempo he puesto en marcha todo esto para sumar a la cultura de la ciberseguridad ¿qué no podrás hacer tú que estás leyendo esto? **Recuerda, todos sumamos.**

www.yolandacorral.com
@yocomu

and organiser of the PaellaCON Computer Security Conference, which is free to attend. I am also a **facilitator in the Hack&Beers community in Valencia.**

“We can contribute from every professional sector to move forward together”

Lastly, I channel the obtained knowledge in an aspect I love: being a trainer. **I conduct workshops and talks about digital security and privacy for organizations, companies and wherever I am asked for it**. In this area I am also lucky to participate as a trainer in a programme about Internet security in education centres giving workshops to teachers and students. This allows me **to get a feel for the young people who, because of their age, are the most vulnerable group on the Internet**, and to help training teachers in their most needed security issues. Besides that, **. am a cybervolunteer at Safe Internet for Kids-INCIBE,** where I get more experiences by bringing security closer to children and their families.

If I, being a journalist and with no basic technical training, could implement all this with effort, dedication and time to contribute to cybersecurity culture, what can you reading this not do? **Remember: all of us add up.**

www.yolandacorral.com
@yocomu

NUEVO
NEW
ADVERTISIM
ALL IN ONE 10I

Diseño compacto totalmente enrasado

AUDIO HD ESTÉREO, ACELERÓMETRO Y MAGNETÓMETRO

Completely flushed compact design

STEREO AUDIO HD, ACCELEROMETER AND MAGNETOMETER

CONEXIÓN A LA MANIOBRA · 3G · WIFI · ETHERNET · NOTICIAS · METEOROLOGÍA · VÍDEOS · PUBLICIDAD

CONNECTION TO THE ELEVATOR · 3G · WIFI · ETHERNET · NEWS · WEATHER · VIDEOS · ADVERTISING

TU CANAL DE COMUNICACIÓN CON EL PASAJERO

YOUR COMMUNICATION CHANNEL WITH PASSENGERS

NAYARSYSTEMS | 72 horas | ADVERTISIM | net4machines | empresa Innovadora de base tecnológica reconocida por ANCES e!bt | PYME INNOVADORA

964 066 995 · www.advertisim.com

Conservación del patrimonio cultural a través de redes LPWAN

The conservation of cultural heritage through LPWAN networks

JAIME LABORDA | El Internet de las cosas está llegando hasta sitios insospechables. Esta vez le ha tocado el turno al **patrimonio cultural y su monitorización** a través de sensores permanentemente conectados a la red publicando los parámetros que más importan a los expertos conservadores de patrimonio, con el objetivo de hacer **un seguimiento constante de aquellos parámetros que la degradan y reducir su efecto**. A esta manera de trabajar se la llama **conservación preventiva**, pues permite adelantarse al deterioro y a la tragedia que supone una restauración.

La monitorización del patrimonio mediante nodos conectados ofrece una fuente importantísima de información para los conservadores, ya que esta gran cantidad de datos permite realizar análisis mediante diversos algoritmos para **predecir el comportamiento futuro de dichas obras** y así poder actuar con tiempo antes de que se produzca el daño. "Actuar" en este contexto puede ser tan simple como cambiar un cuadro de lugar o abrir una ventana para que se airee una estancia, o tan complejo como rediseñar el sistema de climatización de un museo.

"La monitorización del patrimonio mediante nodos conectados ofrece una fuente importantísima de información para los conservadores"

Desde el **instituto ITACA** de la UPV se está trabajando en distintos proyectos de monitorización de pinturas,

JAIME LABORDA | The Internet of Things is reaching unsuspected places. On this occasion it is the turn of **cultural heritage and its monitoring** through sensors that are permanently connected to a network, transmitting the parameters that are most useful to conservation experts, the aim being to **constantly monitor those parameters that contribute to degrading, and to reduce their effect**. This way of working is called **preventive conservation**, because it makes it possible to anticipate and prevent deterioration, thus avoiding the tragedy of a restoration.

The use of nodes to monitor patrimony offers conservators a wealth of information because the high volume of data generated allows them to perform analyses using various algorithms **to predict the future behaviour of those artworks**. This allows them to act in time to prevent damage from occurring. "Acting" in this context can range from something as simple as moving a painting or opening a window to air the room, to something as complex as redesigning a museum's air-conditioning system.

"The use of nodes to monitor patrimony offers conservators a wealth of information"

The **ITACA Institute** of the UPV is working on different projects that monitor paintings, sculptures and buildings, testing several long-distance and low-bandwidth wireless-transmission technologies known as **LPWANs**

esculturas o edificios donde se están poniendo a prueba varias tecnologías de transmisión inalámbrica de larga distancia y bajo ancho de banda, tecnologías conocidas como **LPWANs** (Low Power Wide Area Networks), para conectar a la red de Internet diversos sensores que permiten recoger datos en tiempo real como **temperatura, humedad, luminosidad o índice de radiación ultravioleta**. Posteriormente, estos datos son procesados mediante técnicas estadísticas de **"big data"** en el **"cloud"** para poder obtener sugerencias de actuación o generar alarmas que alerten de cualquier anomalía detectada.

LORAWAN

Una de las tecnologías LPWAN que se está empleando es **LoRa/LoRaWAN**. LoRa emplea una modulación inalámbrica apta para aplicaciones long-range low power low-data rate desarrollada por Semtech. LoRa trabaja en el rango de frecuencia libre de 868MHz en Europa y tiene una alta sensibilidad de recepción de datos y una alta inmunidad al ruido, lo que la hace **muy tolerante a las interferencias con un consumo de energía muy bajo**. Todo esto hace que sea una tecnología apropiada para **conexiones a grandes distancias o con poca cobertura celular** con la contraprestación de que la cantidad de datos a enviar deberá ser pequeña. **LoRaWAN es un protocolo de red libre** que usa la tecnología de modulación LoRa para comunicar y administrar los dispositivos, así como de encriptación de los datos que se envían y reciben. Al tratarse de un protocolo libre, **cualquiera lo puede utilizar como base para construir una red privada bajo este protocolo.**

El actual prototipo basado en LoRa/LoRAWAN alcanza un rango de **15 km desde el repetidor más cercano** y con un envío de datos **cada 30 minutos** aproximadamente, el sensor es capaz de funcionar hasta 10 años con una sola batería.

MAKERSUPV

Makers UPV es **una comunidad de estudiantes sin ánimo de lucro** de la Universitat Politècnica de València fundada en abril de 2013, cuyos objetivos son mejorar la experiencia de aprendizaje de los estudiantes añadiendo una componente práctica basada en **"experiential learning", Do it yourself y la Maker Culture.** A través de proyectos, competiciones y talleres impartidos por estudiantes con habilidades especiales (actuando como mentores), la comunidad se ve realimentada y crece.

La comunidad ha obtenido atención internacional gracias a su éxito en competiciones en todo el mundo, como el premio al **"Mejor Diseño Conceptual"** y el premio al **"Mejor Subsistema de Propulsión"** con el proyecto **Hyperloop UPV** en la competición Hyperloop Pod

(Low Power Wide Area Networks), to connect to the Internet various sensors gathering real-time data such as **temperature, humidity, brightness or UV index**. These data are subsequently processed in **the cloud** using **big-data** statistical techniques in order to suggest actions or sound the alarm when anomalies are detected.

LoRaWAN

One of the LPWAN technologies being used is **LoRa/LoRaWAN**. LoRa is a wireless modulation technology developed by Semtech that is suitable for long-range low-power low-data-rate applications. It works in the license-free 868 MHz frequency band in Europe and combines high reception sensitivity with high noise immunity, resulting in **very high interference tolerance and very low power consumption**. All of this makes LoRa technology very well suited **for long-distance or poor-reception connections**, provided the volume of data to be transmitted is small. **LoRaWAN is a free network protocol** that uses LoRa modulation technology for device communication and management, and encrypts incoming and outgoing data. Because of its open-source nature, **anyone can use this protocol as the base for their own private network.** The current LoRa/LoRAWAN-based sensor prototype has a range of up to **fifteen kilometers from the closest antenna** and can operate for up to ten years on one battery at a data-transmission frequency of approximately **every thirty minutes.**

MAKERSUPV

Makers UPV is a **non-profit student community** from the Polytechnic University of Valencia (Spain) founded in April 2013. Its objective is to enhance the learning experience of students by adding a practical approach based on **"experiential learning", Do It Yourself and the Maker Culture.** Through projects, competitions, and workshops taught by students with special abilities (acting as mentors), the community feeds back on itself and grows.

Competition (SpaceX, 2016), el premio **"Top People's Choice"** con el proyecto NextVision (2014) en el concurso **International Space Apps Challenge de la NASA** así como **"Global Top 5 Best Use of Hardware"** con el proyecto GoSat (2015) y Mars UPV (2016) entre otros.

Dentro del proyecto MakersUPV se llevan a cabo talleres abiertos a la comunidad universitaria destinados a **dar a conocer las tecnologías más innovadoras**. Son talleres meramente prácticos donde la comunidad se retroalimenta y aprende haciendo. Dichos talleres sirven de inspiración a los Makers más novatos. Además, se organizan diferentes eventos durante el año como **concursos de robótica** (Olympic Robotic Challenge), de **construcción de aeronaves** (Flight Challenge VLC), o reuniones con otros creadores (Be Maker Fest). Estos eventos tienen como objetivo el reforzar las competencias transversales que se desarrollan en la universidad como el trabajo en un equipo multidisciplinar, el diseño electrónico o la programación, que **le permite al estudiante prepararse para el mundo laboral.**

"Son talleres meramente prácticos donde la comunidad se retroalimenta y aprende haciendo"

Otro de los proyectos dentro de MakersUPV es el de los **talleres para los makers más pequeños** (entre 8 y 12 años), que se imparten los sábados en colaboración con el **American Space Valencia**. Con esto se intenta transmitir la **cultura maker** desde bien pequeños, a la vez que se les acerca a la ciencia mediante workshops divertidos y meramente prácticos.

INSTITUTO ITACA

El Instituto Universitario de Tecnologías de la Información y Comunicaciones (ITACA) de la Universidad de Valencia tiene la misión de mejorar la sociedad a través de **la aplicación de la investigación en el campo de las tecnologías de la información y la comunicación** (TIC). Cuenta con más de 100 investigadores con una estrecha colaboración con otros centros de investigación e industrias, facilitando la aceleración de la innovación y fomentando una **cultura de emprendimiento en el sector de las TIC.**

El instituto ITACA trabaja cubriendo un amplio espectro de disciplinas relacionadas con las TIC como el diseño de sistemas electrónicos, electrónica industrial, sistemas de telecomunicaciones, uso de las TIC en medicina, integración de sensores, compatibilidad electromagnética, electromagnetismo y microondas.

The community has gained international attention thanks to its success in competitions all over the world, receiving the **"Top Hyperloop Design Concept"** and **"Best Propulsion Subsystem"** awards for its Hyperloop UPV project at the Hyperloop Pod Competition (SpaceX, 2016), the **"Top People's Choice"** award for the NextVision project (2014) at **NASA's International Space Apps Challenge**, as well as the **"Global Top 5 Best Use of Hardware"** award with its GoSat (2015) and Mars UPV (2016) projects, among others.

The MakersUPV project organises workshops aimed at **presenting the most innovative technologies** to the university community. These are simply practical workshops in which the community feeds back on itself and learns by making. The woprkshops are also meant to inspire newbie makers. Other events are also held throughout the year, such as **robotics** (Olympic Robotic Challenge) and **airplane-construction competitions** (Flight Challenge VLC), and meetings with other creators (Be Maker Fest). The objective of these events is to strengthen the cross-disciplinary skills that are developed in the university, such as multi-disciplinary teamwork, electronic design, or programming, which **help students prepare for their entry into the labour market.**

"These are simply practical workshops in which the community feeds back on itself and learns by making"

Another MakersUPV project is the **workshops for junior makers** (aged 8 to 12) that are taught on Saturdays in collaboration with American Space Valencia. These workshops aim to transmit maker culture from a very early age, while also introducing science through fun, practical workshops.

ITACA INSTITUTE

The mission of the Institute of Information and Communication Technologies (ITACA) of the Polytechnic University of Valencia (UPV) is to improve society through **the application of knowledge from research in the field of Information and Communications Technology** (ICT). The institute has more than 100 researchers who collaborate closely with other research centres and industries, facilitating the acceleration of innovation and encouraging an **entrepreneurial culture in the ICT sector.**

ITACA's research covers a wide spectrum of disciplines related to ICT, such as electronic-system design, industrial electronics, telecommunications systems, ICT systems in healthcare, sensor integration, electromagnetic compatibility, electromagnetism and microwaves.

IoT&ELEVATORS

¿QUIERES APARECER EN EL PRÓXIMO NÚMERO?

DO YOU WANT TO APPEAR IN OUR NEXT ISSUE?

Contacta con nosotros en / Contact us at
comunicacion@nayarsystems.com

Escanea este código QR para leer el nº 1 de IoT&Elevators

Scan this QR code to read IoT&Elevators #1

El nuevo paradigma del liderazgo en la empresa tecnológica

The new paradigm of the leadership in the technological enterprise

OFELIA SANTIAGO
Directora de Santiago Consultores
Managing Director of Santiago Consultores

Asistimos a una época que supondrá uno de los mayores desafíos a la capacidad de gestión actual **tanto desde la esfera económica, como desde la política e institucional**.

A estos tiempos de incertidumbre y de inmediatez en la toma de decisiones, se suma el requerimiento de una urgente digitalización de todas las organizaciones que conforman tanto el sector empresarial internacional, como el institucional y gubernamental. Varios son los intentos de acometer esos procesos, que nosotros llamamos de transformación organizacional, desde una perspectiva meramente tecnológica, lo que tiene como resultado una miopía estratégica, así como un paradigma económico equivocado, no basado en la **sostenibilidad**, que es el eje en el que debemos de basarnos para afrontar con éxito el reto que nos plantea esta actual situación.

"Toda solución tecnológica debe de estar puesta al servicio del desarrollo de las personas y no al contrario"

Por tanto, debemos analizar primero y detenidamente todos y cada uno de los componentes que conforman el panorama estratégico mundial, sin olvidar que toda solución tecnológica debe de estar puesta **al servicio del desarrollo de las personas** y no al contrario. Para todo ello, debemos de contar con perspectivas estratégicas que resuelvan esta situación, desde el

We are living in an era that will suppose one of the major challenges to the **economic, political and institutional management capabilities.**

In this uncertain times is fundamental to have immediate decision making processes and there is also the additional requirement of an urgent digitalization of all organizations involved in international business, institutional and governmental sector. Several are the attempts to develop this process, that we call organisational transformation, if we look it from a merely technological perspective the result is strategic myopia, as well as an inaccurate economic paradigm not based on **sustainability**, which is at the heart of the challenge that we have to face in order to succeed in the current situation.

"Any technological solution has to be dedicated to the development of people and not vice versa"

It is important examining carefully all the components that shape the world strategic panorama, without forgetting that **any technological solution has to be dedicated to the development of people and not vice versa**. For all those reasons, we should rely on strategic perspectives to overcome this situation, the analysis of the different factors from the beginning has to contemplate all the stakeholders or interest groups that form part of the company.

mismo comienzo del análisis de los distintos factores, contemplando todos los stakeholders o grupos de interés que forman parte de la compañía.

Se ha demostrado en los últimos años que todo proyecto que sea abordado directamente, basándose solo en las aportaciones de las nuevas tecnologías, puede correr el riesgo de terminar en profundos fracasos. Esto es lo que se está poniendo de manifiesto en muchos de los congresos sobre empresa 4.0 a los que he tenido el placer de asistir, en los que todos los ponentes coinciden en que, como ya están haciendo en lugares como el MIT y Silicon Valley, debemos de centrarnos en el *customer experience* y ya no solo en el producto, como se viene haciendo hasta ahora.

"Debemos de centrarnos en el *customer experience* y ya no solo en el producto"

Pero esto es imposible sin tener integrado **un paradigma holístico que contemple a todos los actores de la nueva economía/empresa**, sin olvidar que la misma ya no está diseñada como un concepto jerárquico y lineal, sino como una empresa extendida, que está perfectamente integrada en el modelo de economía circular.

La empresa extendida es aquella en cuya estrategia, se tiene en cuenta la integración de todos los agentes implicados en su actividad empresarial bajo una perspectiva colaborativa y sostenible. Hemos de incorporar en los proyectos **la voz de todos los grupos de interés** que forman parte de nuestro radio de alcance como empresa, para estar alineados con sus expectativas y necesidades, incluyendo a clientes internos y externos, proveedores, accionistas, agentes de conocimiento, administraciones públicas, etc.

Para ello, hace falta resolver urgentemente esa aparente **brecha cultural y funcional** existente entre, por una parte, la innovación que se genera en los


© Tsung-Lin Wu

In last years it has been demonstrated that any project approached directly, based only on the contributions of the new technologies, may be at risk of ending in deep failures. This is what is revealed in recent congresses about enterprise 4.0, where I had the pleasure of attending, during this events all the rapporteurs agreed on the necessity to change the focus from the product to the *customer experience,* example of this can be found in places like the Massachusetts Institute of Technology (MIT) and Silicon Valley.

"The necessity to change the focus from the product to the customer experience"

This change is impossible without having **an holistic paradigm integrated including all the stakeholders of the new economy/enterprise**, without forgetting that it is not designed as a linear hierarchic concept, but rather as an extended enterprise, that is perfectly integrated in the circular economy model.

The strategy of an extended enterprise takes into account, from a collaborative and sustainable perspective, the integration of all the actors involved. We have to incorporate in the projects **all the stakeholders** that as enterprise are part of our blast radio, in order to stay in line with their expectations and needs, including internal and external clients, suppliers, shareholders, agents of knowledge, public administrations, etc.

For it, it is necessary to resolve urgently this apparent **functional and cultural gap** that exists among, on the one hand, the innovation that is generated in the departments of I+D+i and the product managers who devote themselves to offer technological solutions, and on the other, the business and analytical profiles of the market, that speak even different languages and not always they are communicating, in order to find together common solutions. We have to enable the adequate channels of internal and external communication and to work in a coordinate manner a I+D+i, and our product managers, in constant contact with our sales teams, they know these needs and can give an effective response to them.

"We have to enable the adequate channels of internal and external communication"

On the other hand, **the role of the development of the knowledge and of the human capital it is not possible to leave it to the improvisation** or treat it as a secondary way. Any technological company has to rely on a real analysis, detection, management and development of the knowledge and of the human capital that should integrate, feed and nourish to each and every of the departments and persons of

departamentos de I+D+i y los product managers que se dedican a ofrecer soluciones tecnológicas, y por otra, los perfiles más comerciales y analíticos del mercado, que hablan incluso distintos lenguajes y que no siempre están comunicados, para buscar juntos, soluciones comunes. Hemos de tener habilitados los canales de comunicación interna y externa adecuados para ello, y poner a trabajar de forma coordinada a I+D+i, y nuestros product managers, que en contacto continuo con nuestros equipos comerciales, ahora sí, conocen esas necesidades y pueden dar una respuesta eficaz a las mismas.

“Hemos de tener habilitados los canales de comunicación interna y externa adecuados”

Por otra parte, **el papel del desarrollo del conocimiento y del capital humano no se puede dejar a la improvisación** o tratarlo de manera secundaria. Toda empresa tecnológica ha de contar con un verdadero análisis, detección, gestión y desarrollo del conocimiento y del capital humano que integre, alimente y nutra a todos y cada uno de los departamentos y personas de la empresa bajo una perspectiva de liderazgo nueva, diferente, emocional, inclusiva e inspiradora.

El universo esta regido por dos fuerzas que se encuentran en continua atracción -el yin y el yang del taoísmo, los Shiva y Shakti hinduistas o, bajo el paradigma de la física, el polo positivo y negativo-. Representan dos fuerzas que están en permanente relación dinámica. Pues bien, todos somos mezcla de estas dos fuerzas y **nuestro trabajo es lograr su perfecto equilibrio**, aspirar a su homeostasis.

El modelo imperante de liderazgo en nuestra sociedad, en el ámbito económico, político y empresarial está basado en un paradigma masculino, estableciendo este rol por defecto. La empresa tecnológica no se aleja de este paradigma. Esta cuestión impide la afloración tanto de valores, como de deseos y sentimientos de todos los miembros del equipo, que deben estar puestos al servicio de un bien superior y común. Asimismo, limitan la expresión del verdadero Ser, cuando las necesidades actuales de gobernanza requieren justamente lo contrario. Se necesita un modelo de liderazgo que abarque los intereses de todos, desde **un prisma empático, conciliador y cooperativo, que trabaje para todos.**

“Se necesita un modelo de liderazgo que abarque los intereses de todos”

No es una perspectiva de diferencia de género, sino de **estilo de liderazgo**, de líderes y lideresas que sean personas nutritivas, conciliadoras, que escuchen, que


© Kantver

the company under a new, different, emotional, inclusive and inspiring perspective of leadership.

The universe is governed by two forces that are in continuous attraction - the yin and the yang of the Taoism, the Hindu Shiva and Shakti or, under the paradigm of the physics, the positive and negative pole. They represent two forces that are in permanent dynamic relation. Well then, we all are a mixture of these two forces and **our work is to achieve their perfect balance**, to aspire to their homeostasis.

In our society the commanding model of leadership, in the economic, political and managerial area it is based on a masculine paradigm, establishing this role for default. The technological enterprise does not move away from this paradigm. This question prevents the growth of values, desires and feelings of all the members of the team, who have to be at the service of a superior and common good. Likewise, they limit the expression of the real Being, when the current needs of governance need exactly the opposite. We need a model of leadership that include the interests of all, **an empathic and cooperative leadership that works for all.**

“We need a model of leadership that include the interests of all”

sepan trabajar los silencios, que no hablen sino para servir a los intereses de la empresa y todos sus grupos de interés, habiéndose tomado el tiempo necesario para sentirlos y analizarlos con exactitud. Y solo entonces pasar a una fase reflexiva donde los equipos, perfectamente seleccionados y capacitados, ofrezcan soluciones basadas en la excelencia y sean competentes para la toma de decisiones eficaces y la correspondiente implementación de las medidas necesarias.

Por tanto, frente a los egos individualistas que ofrecen sistemas en perpetua competencia se necesita urgentemente, implementar una alternativa de liderazgo **acogedora y aglutinadora**. Centrada en el valor de cooperación, la nutrición, la empatía y que pueda albergar el nuevo modelo de economía circular basada en el concepto de organizaciones y empresas extendidas, que resuelvan por fin la anterior competencia.

En este nuevo paradigma, por fin, todos los stakeholders se verían integrados y conectados trabajando para un bien común, y solo así podrán comprometerse con la nueva misión, visión valores del proyecto empresarial.

© Le Moal Olivier

“En este nuevo paradigma, todos los stakeholders se verían integrados y conectados trabajando para un bien común”.

Pero como decía Tom Peters: “*Hacer las cosas es mucho mejor que hablar de ellas. Actúa*”. Es la única forma de avanzar, es el primer paso para la transformación.

© Egor Kotenko

It is not a difference perspective of genre, but a **style of leadership**, of leaders that are nourishing persons, conciliatories, that listen, that can work the silences, which they do not speak but to serve to the interests of the company and all their stakeholders, having taken the time necessary to feel them and to analyse them with accuracy. And only then to go on to a reflexive phase where the teams, perfectly selected and qualified, offering solutions based on the excellence and competence in order to take effective decisions and to implement the necessary measures

Therefore, opposite to the individualistic egos that offer systems in perpetual competition it is urgent to implement an alternative **friendly and agglutinative** leadership. A Leadership based on the value of cooperation, the nutrition, the empathy and that could shelter the new model of circular economy based on the concept of extended organizations and enterprises, which could solve finally the previous competition.

The idea of this new paradigm is to have all the stakeholders integrated and connected working for a common good, only in this way they will be able to compromise themselves with the new mission, vision and values of the managerial project.

“The idea of this new paradigm is to have all the stakeholders integrated and connected working for a common good”

But as Tom Peters said: "*Doing things is much better than talking about them. Act*". It is the only way to move forward, the first step to transformation.

¿Comunicas?... ¡Existes! La estrategia de comunicación como herramienta fundamental para el éxito empresarial

Do you communicate? Then you exist! Communication strategy as an essential tool for business success

Lo que no se comunica, no existe. Es una frase que seguramente habrás escuchado en numerosas ocasiones. Tantas, que en cierto modo se ha vuelto manida y la damos por hecho sin analizar la veracidad e importancia para las organizaciones de estas palabras.

A lo largo de este número, hemos comprendido la importancia y necesidad de invertir en ciberseguridad, y cómo esta se vuelve prioritaria para empresas e instituciones. Yendo más allá, desde el Servicio de Seguridad de la Generalitat Valenciana, por ejemplo, se afirma que **las empresas que no hayan pensado en ciberseguridad tendrán un futuro poco prometedor,** pues la inversión en soluciones de seguridad se convierte en un **factor de excelencia** que permitirá a las empresas ser más competitivas y destacar en el mercado.

Ahora bien, esta inversión **debe ser comunicada** para que exista en la mente de los **stakeholders** o públicos estratégicos de la empresa. Es más, **debe formar parte del ADN de la organización y transformarse en un valor de marca**. Y para conseguirlo, el primer paso es confiar en profesionales de la comunicación.

Comunicar el esfuerzo que tu organización lleva a cabo para consolidarse como una empresa que vela por la seguridad de la información es **una línea estratégica** que debe contemplarse en el plan de

What is not communicated does not exist. Probably you have heard this sentence many times. So many that, in some way, it has become trite and we take it for granted without analysing the truthfulness and importance of these words for organizations.

Throughout this issue, we have understood the importance and necessity of investing in cybersecurity, and how it becomes a priority for companies and institutions. Further beyond, from the Security Service of the Generalitat Valenciana, for example, it is stated that **there is an unpromising future for companies that have not considered cybersecurity,** since investment in security solutions turns into a **factor of excellence** that will make companies more competitive and stand out in the marketplace.

Nonetheless, this investment **must be communicated** so it exists in the minds of the company's **stakeholders** or strategic customers. Moreover, **it must be part of the organization's DNA and transform into a brand value**. And to achieve this, the first step is to trust communication professionals.

Communicating the effort your organization is carrying out to become established as a company that safeguards information security is a **strategic line** to be considered in the yearly communication plan of your company.

comunicación anual de tu compañía. Se trata de un documento donde todo queda estipulado. Parte de una primera fase de **contextualización e investigación de la situación actual de la empresa**, donde se marca la identidad corporativa de la misma, se identifican sus públicos estratégicos, cuáles son sus ventajas competitivas y las carencias clave, y se determinan una serie de objetivos corporativos que se desean cumplir.

“La inversión en ciberseguridad [...] debe formar parte del ADN de la organización y transformarse en un valor de marca”

En base a esta información, se traza **la forma en la que la compañía se relacionará con dichos públicos y se determinan las líneas estratégicas a seguir**. Asimismo, se planifican una serie de acciones que se llevarán a cabo **con el fin de cumplir los objetivos** propuestos**.** Gracias al plan de comunicación, se planifica de forma estratégica y ordenada las líneas de actuación de la organización, para transmitir siempre **mensajes coherentes con su identidad y con miras al largo plazo**. Por lo tanto, una estrategia de comunicación adecuada y efectiva será vital para comunicar adecuadamente el esfuerzo realizado en materia de ciberseguridad por la empresa en cuestión.

Pero vayamos más allá. **Toda la plantilla debe estar concienciada de la inversión en ciberseguridad que lleva a cabo la compañía** y erigirse como la mejor prescriptora, comunicando adecuadamente los valores corporativos de la organización. Y para conseguir que tus empleados sean los mejores embajadores de tu marca, también necesitas gestionar adecuadamente la **intracomunicación**. Esa extraña palabra, que va más allá del concepto de comunicación interna. La intracomunicación evita conflictos, fomenta la colaboración y el compromiso, incrementa la confianza de los empleados, ayuda a gestionar el conocimiento, mejora la toma de decisiones efectivas, ayuda a alcanzar buena reputación, entre otros muchos beneficios. Dado que la ciberseguridad es un asunto que concierne a toda la empresa, su adecuada comunicación debe quedar reflejada en el plan de comunicación anual de la compañía.

Finalmente y en cuanto a la comunicación externa, también tienes que pensar **cómo vas a acercarte a tus stakeholders y cómo vas a comunicarles que eres una empresa responsable y segura,** que invierte sus recursos en soluciones de seguridad.

Y ahora dinos **¿Realmente lo estás comunicando?**

info@agenciarespira.com
www.agenciarespira.com

This is a document where everything is stipulated. It starts from a first stage on **which the company’s current situation is contextualised and examined**; the corporate identity of the company is set; their strategic customers, their competitive advantages and key shortages are identified; and a series of corporate objectives to accomplish are defined.

“The investment in cybersecurity [...] must be part of the organization’s DNA and transform into a brand value”

The way in which the company will relate to those customers is drawn up and the strategic lines to follow are determined based on this information. A series of actions are also planned **in order to achieve the decided objectives**. The lines of action of the company are strategically and orderly planned thanks to the communication plan to always transmit **messages consistent with its identity and with a view to the long run**. Therefore, an adequate and effective communication strategy will be vital to adequately communicate the effort made by the company in question in matters of cybersecurity.

Let us go further. **All the personnel must be aware of the investment in cybersecurity carried out by the company**, and must become the best opinion leaders who adequately communicate the organization’s corporate values. To get your employees to be the best ambassadors of your brand, you also need to adequately manage intracommunication. This weird word goes beyond the concept of internal communication. **Intracommunication** avoids conflicts, encourages collaboration and compromise, increases employees’ confidence, helps managing knowledge, improves effective decision-making, and helps attaining good reputation, among many other advantages. Given the fact that cybersecurity is something that concerns the whole company, its adequate communication must be reflected in the company’s yearly communication plan.

Finally, as for external communication, you also have to consider **how to approach your stakeholders and how to communicate them that you are a responsible and secure company** which invests its resources in security solutions.

Now tell us, **are you really communicating it?**

info@agenciarespira.com
www.agenciarespira.com

Calendario de eventos

Calendar of events

AGOSTO / AUGUST 2018

IOTE SHENZHEN
JUL-AG 31 · 2
Shenzhen Convention & Exhibition Center
Shenzhen (China)
www.iotexpo.com.cn

SEPTIEMBRE / SEPTEMBER 2018

E2 FORUM FRANKFURT
SEP 18 · 19
Messe Frankfurt · Frankfurt (Alemania / Germany)
https://e2forum-frankfurt.messefrankfurt.com/frankfurt/de.html

LIFT & ESCALATOR SYMPOSIUM
SEP 19 · 20
Highgate House Conference Center · Northampton (UK)
https://liftsymposium.org/

ASIA ELEVATOR ESCALATOR EXPO
SEP 28 · 30
India Expo Center · Noida, Delhi (India)
http://elevatorexpo.co.in/

OCTUBRE / OCTOBER 2018

GLOBAL LIFT AND ESCALATOR EXPO
OCT 4 · 6
Bashundhara Convention Center · Dhaka (Bangladesh)
http://www.gleexpo.com/index.html

IOT SOLUTIONS WORLD CONGRESS
OCT 16 · 28
Fira de Barcelona (Gran Via Venue)
Barcelona (España/Spain)
http://www.iotsworldcongress.com/

CTBUH 2018 CONFERENCE
OCT 20 · 25
JW Marriott Marquis Dubai · Dubai & Abu Dabi (UAE)
http://ctbuh2018.org/

NOVIEMBRE / NOVEMBER 2018

INTERNET OF THINGS WORLDFORUM 2018
NOV 8 · 9
20-22 Wenlock Road · London (UK)
http://iotinternetofthingsconference.com/

SMART CITY EXPO WORLD CONGRESS
NOV 13 · 15
Fira de Barcelona (Gran Via Venue)
Barcelona (España / Spain)
http://www.smartcityexpo.com/en/home

IOT TECH EXPO NORTH AMERICA
NOV 28 ·29
Santa Clara Convention Center · California (USA)
https://www.iottechexpo.com/northamerica/

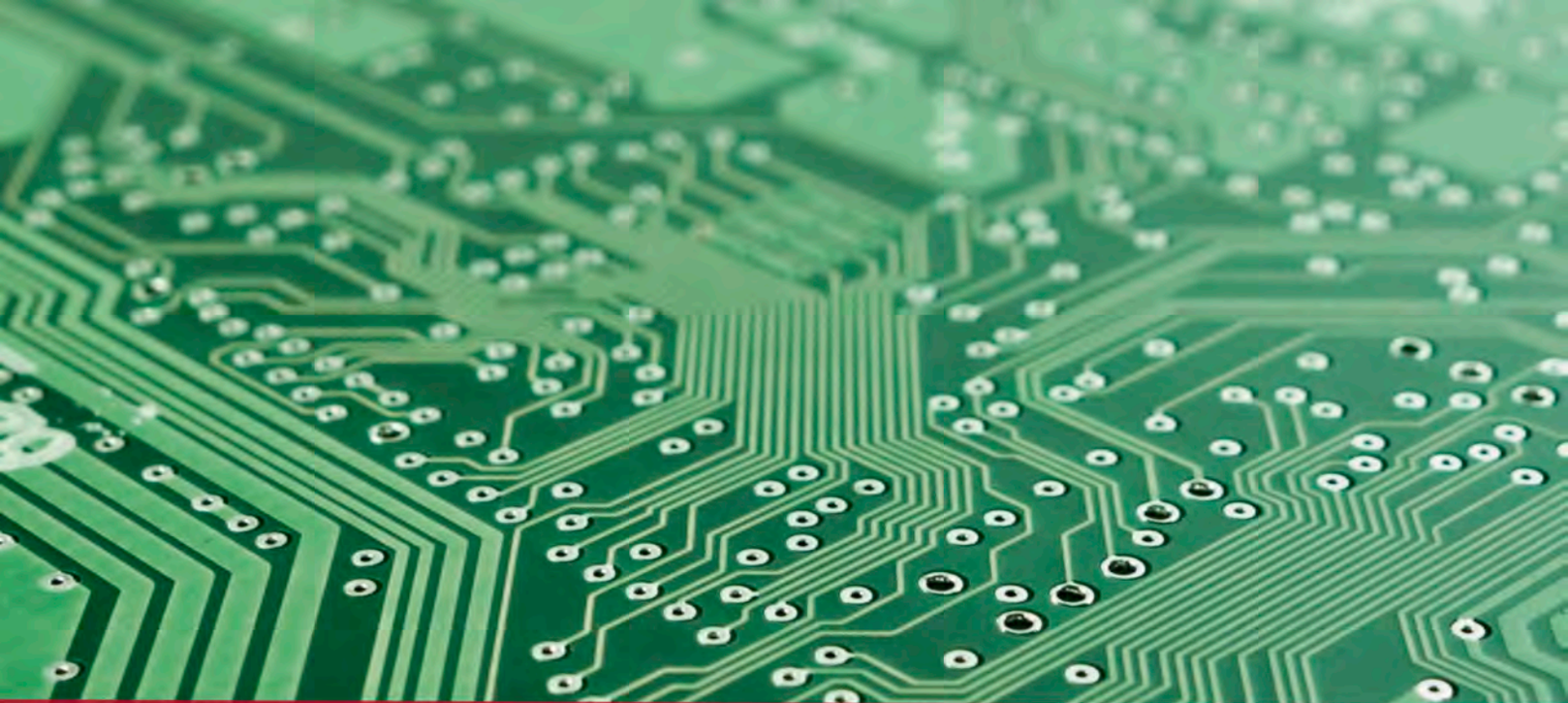
inspira
espira
respira

breathe in
breathe out

www.agenciarespira.com

Comunicación y marketing Communication and marketing
Organización de eventos Event management
Producción audiovisual Video production
Diseño gráfico Graphic design
Redes sociales Social media
Diseño web Web design

_RESPIRA
comunicación



Somos **Innovación.** Somos **Castellón**
*We are **Innovation.** We are **Castellón***

La provincia de Castellón (España) es una tierra que provoca el talento, llama al talento y requiere del talento para seguir creciendo. Contamos con el entorno más competitivo, con **grandes ideas** y con los **mejores recursos públicos** para ayudar a convertir a nuestras empresas en **referentes mundiales** en **desarrollo tecnológico**, **creatividad** e **innovación**. Esta es nuestra apuesta de presente y futuro.

SOMOS INNOVACIÓN. SOMOS CASTELLÓN

*The province of Castellón (Spain) is a land that causes talent, calls talent and requires talent to keep growing. We have the most competitive environment, with **great ideas** and with the best **public resources** to help turn our companies into world leaders in **technological development**, **creativity** and **innovation**. This is our present and future bet.*

WE ARE INNOVATION. WE ARE CASTELLÓN

DIPUTACIÓ DE CASTELLÓ

SOM **INNOVACIÓ**
SOM **PROVÍNCIA**