Secure &MAGAZINE

Número 5 | Enero 2019

ENTREVISTA

César Mejías

CIO del despacho de abogados Garrigues

PREVISIONES DE CIBERSEGURIDAD PARA 2019

CIBERSEGURIDAD INDUSTRIAL

El coste de no tomar las medidas adecuadas

Los cambios más importantes en protección de datos

JUEGA SEGURO Y APRENDE CIBERSEGURIDAD

Consejos y sugerencias para aprender jugando

Secure&IT
www.secureit.es

Editorial

Estimados lectores,

Vamos a empezar esta edición de nuestra revista ***Secure&Magazine,*** con la que inauguramos 2019, con una afirmación: este año será más peligroso debido a la sofisticación y agresividad de los ataques (nuevas variantes de *malware*, ataques dirigidos más avanzados, aumento de los ataques DDoS, etc.).

Los ciberataques son considerados uno de los principales riesgos en mercados que representan el 50% del PIB mundial. Por tanto, empresas y gobiernos van a necesitar fortalecer la ciberseguridad si quieren mantener la confianza en este mundo totalmente conectado. De nuevo, los incidentes han sido los encargados de poner a la ciberseguridad en el candelero informativo: British Airways (sufrieron el robo de los datos personales y la información bancaria de 400.000 usuarios); Ticketmaster (quedaron expuestos los datos personales y bancarios de 40.000 usuarios) o Under Armour (afectó a unos 150 millones de cuentas de usuario). Estos y otros sucesos han demostrado, una vez más, que las necesidades no van a ser solo tecnológicas sino, también, de concienciación y formación de empleados, cumplimiento normativo, etc.

Si hablamos de previsiones y tendencias, no podemos olvidar que los entornos industriales están en el punto de mira de los ciberdelincuentes. El motivo es sencillo: los sistemas industriales y la tecnología operativa (OT, por sus siglas en inglés) están cada vez más conectados y esto supone un aumento exponencial de las ciberamenazas. Por eso, es importante que los responsables de las compañías tomen conciencia y apuesten por la ciberseguridad industrial como una inversión. Debes saber que en **Secure&IT** podemos ayudarte a conocer el estado de tu instalación, detectar los riesgos y asesorarte en las soluciones. En este número de nuestra revista te contamos cómo llevarlo a cabo: auditorías de seguridad, consultoría y planificación de seguridad, Sistema de Gestión de Ciberseguridad Industrial (SGCI), análisis y gestión de riesgos, cumplimiento (ENS, Ley de Protección de Infraestructuras Críticas y protección de datos) y formación.

El cumplimiento normativo, en concreto la protección de datos, sigue siendo uno de los aspectos que más preocupa a las organizaciones. 2018 ha sido un año clave en este sentido: en mayo, se empezó a aplicar el Reglamento General de Protección de Datos (RGPD) y, en diciembre, se publicó la nueva Ley Orgánica de Protección de Datos y garantía de los derechos digitales (LOPDgdd), que se encarga de concretar algunos puntos del RGPD en el marco de la normativa española. Lo cierto es que en **Secure&IT** hemos dedicado gran parte de nuestros esfuerzos (eventos, artículos, especiales de la revista…) a este tema y queremos seguir facilitándoos toda la información que podamos. En este número, tratamos de resumir cuáles son los cambios más importantes que ha introducido la LOPDgdd.

Tampoco hemos querido olvidarnos de los más pequeños de la casa, los niños y niñas que son el presente y serán el futuro de la ciberseguridad. Es una realidad que los columpios y las pelotas están dejando paso, cada vez más, al ordenador, el móvil o la *tablet*. Solemos pensar que en casa están más seguros, pero, ¿somos conscientes de a qué páginas web acceden? ¿sabemos, realmente, qué hacen en Internet? Además de ofreceros algunos consejos sobre cómo comunicaros con vuestros hijos en este sentido, os proponemos algunos juegos que les entretendrán y les enseñarán a navegar seguros en la Red.

Como siempre, en este número contamos con la participación de varios colaboradores a los que queremos agradecer su dedicación; sin sus aportaciones esta revista no sería lo mismo: Horatiu Bandoiu (Bitdefender) y Sara Crespo (Fortinet).

El equipo de Secure&IT

Sumario

4 Entrevista

César Mejías, CIO del despacho de abogados Garrigues

8 Previsiones y tendencias para 2019

Los ciberataques serán más sofisticados y violentos en 2019

10 Una lucha constante contra la evolución del malware

Sara Crespo, Channel Accounts Manager de Fortinet

12 Ciberseguridad industrial

El coste de no tomar las medidas adecuadas

14 Los cambios más importantes en materia de protección de datos

16 Directiva NIS: algunas reflexiones acerca de su implementación

Horatiu Bandoiu, ISO 27001 LA y Channel Marketing Manager de Bitdefender

18 Las aventuras (y desventuras) de Cyberlawyer

Santiago Arellano, Marketing de producto y desarrollo de servicios en Secure&IT

21 Reconocimiento

Secure&IT reconocida como "Mejor partner" de Thycotic

22 Juega seguro y aprende ciberseguridad

Consejos y sugerencias para aprender jugando

César Mejías

"La seguridad es un reto permanente y, como en todos los sectores, tenemos que tener siempre presente este componente"

César Mejías es en la actualidad el CIO (Chief Information Officer) del despacho de abogados Garrigues. Cuenta con más de 20 años de experiencia en la dirección y gestión de departamentos de tecnologías de la información en organizaciones (de más de 2000 empleados) del ámbito legal y consultoría de negocio. Entre sus especialidades se encuentra el desarrollo de negocio desde una perspectiva IT, la innovación en los procesos, el outsourcing y la dirección de equipos. Es el principal responsable de la puesta en marcha de la estrategia de inteligencia artificial de Garrigues.

Llevas 25 años trabajando en Garrigues, ¿cómo ha sido el proceso de transformación digital en la empresa? Y, ¿en qué medida la tecnología os ayuda a simplificar las tareas?

En este sentido, nuestro objetivo es ayudar a nuestros trabajadores y aportar valor a nuestros clientes. Hace tres años empezamos un proceso que consiste en buscar aquellas tareas que son más repetitivas y que pueden ser susceptibles de automatizarse. Llevamos tres años con esta labor, con el objetivo de aumentar nuestra productividad, agregar valor a nuestros clientes y ofrecer un servicio de mayor calidad. Un ejemplo de esto sería *Proces@*, un sistema (me gusta llamarlo robot) que sacamos hace dos años y que ha tenido bastante repercusión nacional e internacional. Nos permite coger la documentación que nos llega (en formato papel, electrónico, audios o vídeos), procesarla y convertirla en textos. De esta manera, además de ahorrarnos la transcripción del audio o del vídeo, conseguimos que nuestros abogados puedan buscar, dentro de todo ese texto, datos relevantes para el asunto que estén tratando.

"Nuestro objetivo es ayudar a nuestros trabajadores y aportar valor a nuestros clientes"

¿Qué impacto va a tener (o está teniendo) la inteligencia artificial en vuestro sector?

Hay opiniones de todo tipo, incluso, hay gente que dice que la inteligencia artificial va a revolucionar el sector. Yo creo que lo que va a pasar, como en todo, es que nos tendremos que quedar con lo mejor de estas tecnologías y adoptarlo, que es precisamente lo que ya hacemos: buscar aquello que es realmente útil y traerlo a nuestro ámbito. El sector legal no es distinto al resto y nos va a pasar como a los demás, tendremos que adaptarnos a las novedades. Por ejemplo, en los procesos de diligencia debida (tienes que hacer una revisión completa de toda la documentación de un asunto) ya hay herramientas que usan la inteligencia artificial y que permiten identificar, por ejemplo, contratos que tienen algo "raro" o distinto. De esta forma, te obligan a revisarlos.

La tecnología nos facilita la vida y, a la vez, podemos decir que nos la complica. El Internet de las Cosas, la tecnología Cloud, los dispositivos móviles, etc. tienen un impacto positivo en nuestra vida, pero también se convierten en "nuevos puntos de entrada" para los ciberdelincuentes. ¿Cuáles son los mayores desafíos a los que os enfrentáis y qué acciones estáis llevando a cabo?

La seguridad es un reto permanente y, como todos los sectores, tenemos que tener siempre presente este componente. Esta máxima la aplicamos en todos los proyectos que hacemos. De hecho, a finales de 2017 nos certificamos en ISO 27001 (hemos sido el primer despacho en España en hacerlo), porque sabíamos que teníamos que introducir ese elemento de seguridad, bien organizado, en todos nuestros procesos. Sobre todo, en aquellos que afectan a nuestros clientes. En paralelo, montamos un Plan Director de Seguridad, que ya hemos ejecutado. Y ahora nos encontramos renovándolo y haciendo uno nuevo. Teníamos claro que era necesario revisar esos procesos de principio a fin y dotarlos de seguridad. Al hilo de eso, incorporamos varias herramientas interesantes de seguridad, montamos un SOC externo que nos permite tener controlada la seguridad 24x7... en definitiva, tenemos claro que la seguridad es fundamental.

En un despacho de abogados, la información tiene un valor incalculable. ¿Crees que, en general, se es consciente de los riesgos de no protegerse en condiciones y de las consecuencias que puede tener?

Creo (y me gusta creerlo) que hay más conciencia de lo importante que es la seguridad. Pero, además, como este sector tiene que acceder a la información y lo tiene que hacer con mucha cautela y mucho cuidado, considero que cada vez hay menos gente que no esté al corriente de esto. Y es que vemos ejemplos casi a diario (la detención en Portugal por el caso de "*Football leaks*", los "Papeles de Panamá", los "Papeles de la Castellana", etc.), que te hacen darte cuenta de la importancia que tiene.

"Este proceso de transformación digital está haciendo ver a los directivos que la tecnología (y la ciberseguridad, como subconjunto de la tecnología) no es un gasto, sino una inversión que tienes que hacer para no quedarte atrás"

¿Crees que se percibe más la ciberseguridad como una inversión o como un gasto?

Hasta hace muy poco la tecnología, en general, se consideraba un gasto y no una inversión. Y ocurría en todos los sectores, salvo en aquellos más tecnológicos. Esto también está cambiando para bien, no solo en el área de seguridad sino en cualquiera de las áreas.

Este proceso de transformación digital en el que estamos todos inmersos está haciendo ver a los directivos que la tecnología (y la ciberseguridad, como subconjunto de la tecnología) no es un gasto, sino una inversión que tienes que hacer para no quedarte atrás.

¿Qué importancia tiene la implicación de la alta dirección en seguridad de la información?

Para nosotros su implicación es fundamental. Y, además, deben ser conscientes de que la seguridad total no existe. Te digo esto porque, cuando montamos el primer Plan director de Seguridad (hace aproximadamente dos años), fuimos a ver a nuestro Presidente, Fernando Vives, y nos lanzó la pregunta que nos hace temblar a todos: "Pero, ¿estamos seguros al cien por cien?". Y el que responda "sí", se equivoca absolutamente. Si yo dijera que estamos totalmente seguros estaría mintiendo. Lo que tenemos que hacer es tratar siempre de llegar a ese cien por cien, mejorando de forma continua.

"Hay que ser conscientes de que la seguridad total no existe"

Como te decía, es fundamental que estén implicados; que desde "arriba" tengan claro que hay que invertir y dejar a los equipos de seguridad hacer su trabajo. Pero, también es necesario mantenerles informados de lo que ocurra, para que esa concienciación sea efectiva.

Sois un despacho puntero, también en las tecnologías que utilizáis. Y, en este sentido, vuestros profesionales están siempre formándose. Pero, ¿cómo de fácil o difícil es hacer entender a los trabajadores la importancia de aplicar todas esas tecnologías con seguridad? ¿Son conscientes de los riesgos?

Nosotros aprovechamos cada una de nuestras presentaciones para reiterar a nuestros abogados que el eslabón más débil de la cadena de seguridad es el usuario. Nuestro trabajo, o la inversión que hagamos en seguridad, no sirve de nada si uno solo de nuestros empleados deja su contraseña apuntada en un papel, pegada en la pantalla o encima de su mesa. Nos "peleamos" mucho para concienciarles de que tienen que colaborar y ser muy proactivos. Tenemos formación presencial y *online* y, también, ofrecemos charlas.

GARRIGUES

Garrigues es una firma internacional de servicios legales y tributarios que asesora en derecho empresarial en los principales escenarios económicos del mercado global.

Fundada en 1941, su equipo está integrado por unas dos mil personas de veinticuatro nacionalidades diferentes que, bajo una dirección única e integrada y con los mismos estándares de calidad, opera en trece países de Europa, América, Asia y África.

Garrigues es uno de los grandes despachos de abogados internacionales, y está entre las firmas globales de abogacía más importantes del mundo. Tiene un equipo de especialistas que asesora en derecho empresarial en las operaciones más complejas e importantes del mercado.

Además, desde hace año y medio, en todas las reuniones de grupo (hacemos varias al año) siempre hay un apartado de seguridad en el que yo mismo, o el CISO, damos una charla de concienciación. También tenemos un boletín de seguridad en el que publicamos "píldoras informativas" con las alertas que lanzan entidades como INCIBE (campañas de *phishing*, extorsiones, etc.). Tratamos de que, poco a poco y con todas estas acciones, el mensaje acabe calando. Es verdad que cuesta, porque la gente no era consciente de los riesgos que supone perder una contraseña, compartirla con el compañero o dejar el móvil desbloqueado encima de la mesa. Nosotros tenemos que poner los medios para que nada de esto pase, pero ellos deben ser conscientes de los riesgos que pueden entrañar acciones como las que acabamos de comentar.

"Creo que [el nuevo modelo de protección de datos] es muy positivo desde el punto de vista de las empresas y, también, de las personas"

¿Ha supuesto la llegada del RGPD un doble reto para los despachos de abogados? (Debéis aplicarlo y, a la vez, asesorar a vuestros clientes en la aplicación).

Sí, lo ha sido. El área dedicada a la protección de datos ha estado trabajando, en los últimos dos años, en ayudar a nuestros clientes. Y, por supuesto, también se ha trabajado mucho internamente. Tenemos un comité de protección de datos que forma parte de nuestro comité de seguridad. Ha habido que hacer mucho trabajo y ha supuesto un reto. Pero, lo cierto es que la certificación ISO 27001 nos ha ayudado muchísimo a poner orden en todos los temas relacionados con protección de datos y, también, a prepararnos para la aplicación del RGPD.

En relación con tu trabajo ¿cómo valoras este nuevo modelo de protección de datos?

Creo que es muy positivo. Entraña sus riesgos, porque las sanciones son enormes y pueden suponer el fin de una empresa. Nos ha generado mucho trabajo, pero creo que es muy positivo desde el punto de vista de las empresas y, también, de las personas.

Hablando del futuro del sector, en algunas ocasiones has mencionado la figura del "abogado renacentista", que sea capaz de desenvolverse en todas las áreas y que cuente con habilidades tecnológicas. ¿Crees que es una tendencia generalizada en todos los sectores?

Quiero pensar que sí. A veces, cuento una anécdota que me ocurrió con un abogado senior de la casa. Un día, hablando sobre contratos inteligentes, me comentó que el planteamiento que yo le hacía implicaba, casi, aprender a programar. Le aclaré que, en este sentido, había tres opciones: contratar un perfil capaz de hacer ambas cosas (no es necesario que sea un técnico, pero sí que entienda lo que dice, por ejemplo, uno de estos *smart contracts*); aprender e ir formándose en la materia, o tener a un técnico al lado, con el que exista confianza plena, para poder desarrollar uno de estos contratos. Y, seguramente, de aquí en adelante todos querremos estos perfiles que aúnen ambas cosas. Y a eso me refiero cuando hablo del "abogado renacentista", que sea capaz de entender casi todas las áreas. Estos perfiles serán los más demandados en los próximos años, aquellos que tengan conocimientos más horizontales de las materias.

Previsiones y tendencias para 2019

Los ciberataques serán más sofisticados y violentos en 2019

En lo que a ciberdelincuencia se refiere, 2019 será un año más peligroso que el que ha terminado, especialmente por la sofisticación y agresividad de los ataques. Las empresas y organizaciones son conscientes de ello: la encuesta global a directivos del Foro Económico Mundial revela que los ciberataques son una de las principales preocupaciones para las empresas europeas (también en Asia Oriental, Pacífico y América del Norte los ciberataques son el principal riesgo). A esto hay que añadir que las amenazas son cada vez más sofisticadas y agresivas y que, en muchos casos, sigue habiendo una falta de formación y concienciación que implica riesgos, no solo externos, sino dentro de las propias compañías.

¿Qué significa esto? Los ciberataques son considerados el principal riesgo en mercados que representan el 50% del PIB mundial. Por tanto, empresas y gobiernos van a necesitar fortalecer la ciberseguridad para mantener la confianza en este mundo totalmente conectado; la seguridad avanzada es una necesidad vital para hacer frente a la ciberdelincuencia.

Incidentes ocurridos en 2018, como el de British Airways (sufrieron el robo de los datos personales y la información bancaria de 400.000 usuarios); Ticketmaster (también quedaron expuestos los datos personales y bancarios de 40.000 usuarios), o Under Armour (afectó a unos 150 millones de cuentas de usuario), ponen la ciberseguridad en el candelero y revelan que las necesidades no van a ser solo tecnológicas sino, también, de concienciación y formación de empleados, cumplimiento normativo, etc.

¿Cuáles van a ser las tendencias en ciberseguridad este 2019?

- **Nuevas variantes de *malware***

El *malware* es una importante fuente de ingresos para los ciberdelincuentes. Todo tipo de usuarios y empresas han sido (o serán en algún momento) víctimas de estos ataques.

Las nuevas variantes de *malware* crecen a un ritmo alarmante. Según el informe *Threat Landscape Report* de Fortinet, las variantes únicas de *malware* aumentaron en el último trimestre de 2018 un 43%.

Habrá que prestar especial atención a los dispositivos móviles, porque el *malware* móvil está en auge. Pero, también, a los dispositivos IoT (Internet of Things). Un ejemplo serían los dispositivos sanitarios (como los marcapasos), ya que los delincuentes podrían utilizarlos para chantajear a las víctimas, ya no solo con sus datos, sino con su propia vida.

- **Ataques dirigidos más sofisticados y avanzados**

Las amenazas persistentes avanzadas (conocidas como APT, de inglés *Advanced Persistent Threat*) emplearán nuevas y sofisticadas técnicas, mucho más difíciles de detectar.

Uno de los principales objetivos de las APT será el ciberespionaje. Tanto el crimen organizado, como los propios países, desarrollarán nuevos sistemas y herramientas para conseguir la información que necesitan (secretos de Estado, propiedad intelecutal, etc.).

- **Aumentan las amenazas en los entornos industriales**

Los entornos industriales están cada vez más conectados, eso los hace más vulnerables y los convierte objetivo de los ciberdelincuentes. En este sector, las pérdidas por ciberdelitos se han duplicado en los últimos dos años y las amenazas no dejan de aumentar: ataques dirigidos y de código malicioso, robos de información, pérdida de disponibilidad de los sistemas o alteración de los procesos, son algunos ejemplos de los problemas a los que se va a enfrentar la "Industria 4.0".

- **Aumento de los ataques de denegación de servicio (DoS-DDoS)**

Los ataques DDoS siguen siendo una gran amenaza y, en los últimos años, no han dejado de crecer. En este 2019, aumentarán de forma generalizada, pero habrá que poner atención en aquellos dirigidos a telefonía: los conocidos como (TDoS, *Telephony Denial of Services*). La denegación de servicios de telefonía funciona igual que la de la red de datos tradicional: usuarios no autorizados lanzan demasiadas solicitudes de acceso y consiguen que los usuarios legítimos no puedan acceder al sistema. No solo afectan a la disponibilidad de la red, también pueden ser un medio para el fraude.

Esta sofisticación en los ataques, también nos llevará al aumento de los PDoS o Denegación Permanente de Servicio (*Permanent Denial of Service*), dirigidos sobre todo a centros de datos y dispositivos IoT.

- **Los entornos *cloud* como objetivo**

Algunos fabricantes afirman que muchos de los incidentes gestionados el año pasado están relacionados con la tecnología cloud. El aumento de su uso hace que los ciberdelincuentes estén más interesados en utilizarla para acceder a las empresas o distribuir *malware*. En este sentido, evitar las fugas de información seguirá siendo un reto para las compañías.

- **Ataques a través de las redes sociales**

Podemos decir que las redes sociales son una autopista perfecta para los ciberataques, por varios motivos: a través de ellas, ofrecemos muchísima información (personal y profesional); son el lugar perfecto para distribuir *malware*, y las utilizamos de forma masiva (eso les proporciona a los ciberdelincuentes acceso a un gran número de potenciales víctimas).

Por este motivo, seguirán creciendo los ataques a través de estas plataformas, en forma de ingeniería social o robo de identidad, entre otras.

Apostar por la seguridad de la información es clave. Las necesidades no son solamente tecnológicas, es preciso apostar por la concienciación y la formación de empleados o el cumplimiento normativo. Aumentar los recursos en este sentido podría ser un gran propósito para 2019 y, en **Secure&IT**, estaremos encantados de ayudarte.

Una lucha constante contra la evolución del *malware*

El *malware* se está volviendo cada vez más destructivo. Los enjambres de dispositivos independientes pero controlados centralmente sin un usuario designado y, a menudo sin parches o actualizaciones, se han convertido en la última tendencia en amenazas.

Lucha contra el *malware*

Resulta extremadamente difícil defenderse contra un enjambre de dispositivos comprometidos de IoT que no solo pueden aprender y adaptarse, sino que también están programados para destruir en última instancia los dispositivos que infectan. Unirlos para que participen en ataques masivos, casi con toda seguridad, haría que un segmento considerable de la economía digital se detuviera.

Afortunadamente, las organizaciones tienen recursos para prepararse y defenderse contra el *malware*.

- **Agregue la tendencia de *botnets* a su actual estrategia de análisis de riesgo/ consecuencia**. Su equipo de TI debe conocer sus opciones, como el almacenamiento fuera del sitio de las copias de seguridad del sistema, disponer de sistemas redundantes en su lugar y poder bloquear segmentos de red cuando se detecte un ataque.
- **Identifique todos los activos y servicios críticos en su red y aumente los esfuerzos para identificar y parchear los sistemas vulnerables, reemplazar los sistemas más antiguos** que ya no son compatibles **o mejorar las herramientas de seguridad** para la compensación. Esto probablemente signifique implementar algún tipo de solución de gestión y seguimiento de activos.
- **Utilice la segmentación de la red para que los dispositivos de IoT se separen automáticamente de su red de producción hasta que puedan ser protegidos**. La autenticación del dispositivo debe ocurrir en los puntos de acceso de IoT. Lo que significa que sus puntos de acceso inalámbrico deben manejar muchas más conexiones simultáneas de las que actualmente están diseñados para administrar y, al mismo tiempo, necesitan poder identificar y autenticar dispositivos, administrar el acceso, inspeccionar el tráfico y encaminar el tráfico de IoT hacia segmentos de red seguros, todo a velocidad de cable. Aun así, debe supervisar cuidadosamente el tráfico que pasa entre los segmentos de red, en busca de comportamientos anómalos, *malware* y sofisticados ataques de múltiples vectores.
- Ya **no puede permitirse el lujo de correlacionar manualmente los datos de amenazas** para detectar estas o responder a una velocidad inferior a la de la máquina. La inteligencia de amenazas en tiempo real es crítica para identificar y detener un ataque.

El malware se está volviendo cada vez más destructivo

- Recuerde: la inspección a fondo de los datos no estructurados, como los datos en bruto que fluyen de muchos dispositivos IoT, consumen entre 50 y 100 veces más potencia de procesamiento que el tráfico convencional. **Es probable que muchos de sus dispositivos de seguridad heredados no estén preparados para desempeñar su trabajo.**

Una defensa integral

El proceso evolutivo actual pronto traerá un nuevo *malware* diseñado con aprendizaje adaptativo y basado en el éxito para mejorar la eficacia de los ataques. Esta nueva generación de *malware* comprenderá el entorno en el que se encuentra y tomará decisiones calculadas sobre qué hacer a continuación. A medida que la guerra cibernética se intensifica, las organizaciones deberán luchar contra la automatización con su propia automatización e implementar sistemas de seguridad integrados que puedan recopilar, correlacionar, compartir y responder automáticamente a las amenazas de manera coordinada. Los pasos enumerados anteriormente ayudarán a detectar y anular las sofisticadas redes de *malware* y mantener el negocio y su reputación intactos.

Sara Crespo
Channel Accounts Manager de Fortinet

Ciberseguridad industrial: el coste de no tomar las medidas adecuadas

Los sistemas industriales y la tecnología operativa (también conocida como OT, por sus siglas en inglés) están cada vez más conectados y esto supone un aumento exponencial de las ciberamenazas en la industria. Los equipos de automatización industrial han heredado las tecnologías de la informática corporativa y, con ellas, sus problemas en lo que a seguridad de la información se refiere.

El INCIBE-CERT ha informado de que, durante 2018, se han publicado 228 avisos de vulnerabilidades relacionadas con este sector, lo que supone un incremento considerable con respecto a 2017 (se registraron 199 avisos). De todos ellos, casi un 45% han tenido una criticidad alta y, un 33% han sido críticos. Y, la tendencia se mantiene: las previsiones auguran que el número de avisos seguirá incrementándose este 2019.

La transformación del entorno industrial

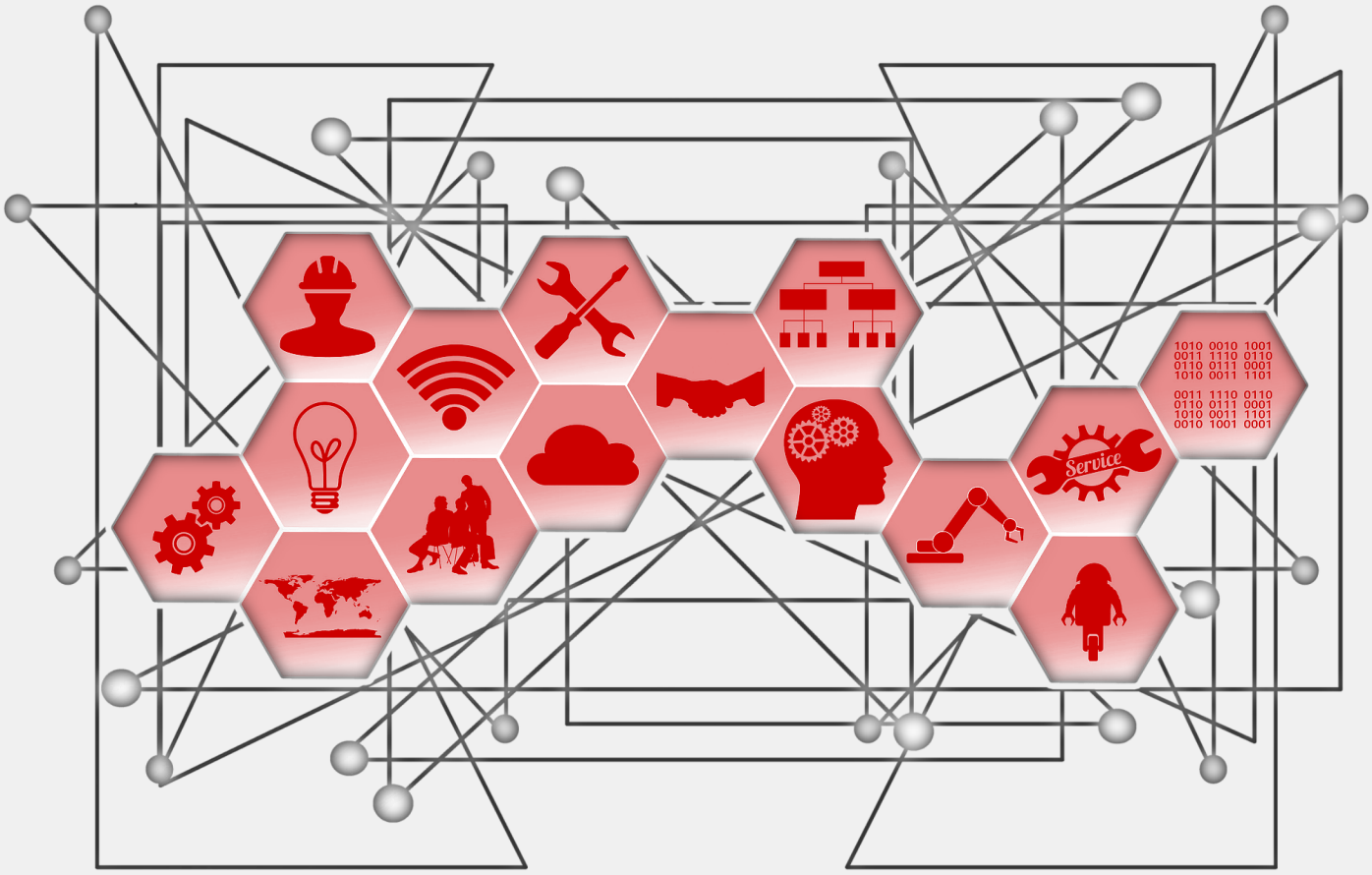
A lo largo de la historia, se han conocido multitud de vulnerabilidades, asociadas tanto al *hardware* como al *software* que componen los sistemas de control industrial (*Industrial Control System* o ICS). Lo cierto es que esas vulnerabilidades no son nuevas, siempre han estado ahí, pero se asumían porque había poca probabilidad de que fueran explotadas. El motivo era sencillo: **los sistemas estaban aislados.** En lo que a seguridad se refiere, podemos decir que en los ICS se ha primado la disponibilidad y la funcionalidad (las tecnologías de la información tratan de priorizar la confidencialidad de los datos por encima de otros aspectos). Pero, no se puede seguir en esa línea; el hecho de **no tomar las medidas adecuadas puede suponer un coste incalculable para las industrias**.

En lo que llamamos "Industria 4.0" esta tendencia cambia; cada vez más dispositivos de control industrial utilizan tecnologías de la información (TI) genéricas: interfaces y protocolos estándar; PCs o sistemas operativos como Windows o Linux. Y, ¿por qué lo hacen? Entre otras cosas, porque son más fáciles de utilizar, amplían las funcionalidades y son más baratas. Pero, como ya hemos comentado, también se heredan los problemas, por ejemplo, las vulnerabilidades. Y, no solo se heredan, también se agravan; en estos entornos no es sencillo realizar paradas, ni siquiera para llevar a cabo el mantenimiento, la actualización, el parcheado o el aislamiento de los sistemas de control.

El hecho de que los entornos industriales estén conectados los hace más vulnerables y, por tanto, los convierte objetivo de los ciberdelincuentes. De hecho, algunas encuestas revelan que las pérdidas por ciberdelitos se han duplicado en los últimos dos años. A este ámbito afectan también el ciberespionaje (por motivos económicos o políticos, entre otros) o el ciberterrorismo.

Las amenazas en el mundo OT

En general, proteger o securizar los sistemas industriales es más complejo. Hay una falta de convergencia entre las tecnologías; existe una falta de seguridad en las fases iniciales de diseño de los sistemas; tienen un ciclo de vida elevado; es difícil detener los sistemas para aislar-



los, actualizarlos, parchear, etc.; entre los expertos en la operación suele haber desconocimiento ante ciberamenazas o ciberseguridad y, por todo ello, son de más fácil acceso. En definitiva, **las amenazas aumentan**:

- Aumento de ataques de código malicioso y ataques dirigidos (los sistemas están expuestos a sufrir los mismos ataques que los dispositivos empresariales).
- Robos o usos indebidos de la información confidencial (tanto internos como externos).
- Pérdida de disponibilidad del sistema.
- Alteración de los procesos, comprometiendo la calidad del producto, la capacidad de producción, la seguridad o las emisiones al medio ambiente.
- Parada de líneas y pérdida de producción.
- Incumplimiento legal.
- Pérdida de reputación y, por tanto, de la confianza de los clientes.
- Incalculables pérdidas económicas.
- Etc.

¿Cómo podemos ayudarte?

Los ciberdelincuentes han puesto sus miras en la industria, por eso, es importante que los responsables de las compañías tomen conciencia y apuesten por la ciberseguridad industrial como una inversión. Desde **Secure&IT** podemos ayudarte a conocer el estado de tu instalación, detectar los riesgos y asesorarte en las soluciones:

- Auditorías de seguridad
- Consultoría y planificación de seguridad
- Sistema de Gestión de Ciberseguridad Industrial
- Análisis y gestión de riesgos
- Continuidad de negocio
- Cumplimiento:
  - √ Esquema Nacional de Seguridad
  - √ Ley de Protección de Infraestructuras Críticas
  - √ Protección de Datos
- Formación

Los cambios más im
de protecci

La Ley Orgánica de Protección de Datos y garantía de los derechos digitales (LOPDgdd) se encarga de concretar algunos puntos del Reglamento General de Protección de Datos en el marco de la normativa española. Esta ley complementa ciertos aspectos del Reglamento y aclara otros, por tanto, es necesario manejar las dos normativas (LOPDgdd y RGPD) a la vez. Pero, ¿cuáles han sido los cambios más importantes que se han producido en materia de protección de datos? ¿Qué debes tener en cuenta?

- La nueva LOPDgdd **hace referencia a la figura del Delegado de Protección de Datos** (DPD, o DPO por sus siglas en inglés) y a la cualificación que esta persona, física o jurídica, debe tener. La Ley también recoge varias infracciones graves para las empresas que estén obligadas a contar con esta figura y no lo hagan. Cabe recordar que el DPD es un profesional, o un equipo de profesionales, muy cualificado (puede ser interno o contratado de forma externa), que se encarga de asesorar, supervisar que las cosas se hagan de forma correcta, informar o resolver dudas (todo ello, manteniendo un contacto muy fluido con la alta dirección de la empresa). Pero, es necesario matizar que es la empresa la que debe cumplir la normativa, no el DPD.
- En su artículo 34, la Ley **establece las empresas que están obligadas a contar con la figura del Delegado de Protección de Datos**. Aunque, hay que tener en cuenta que no es una lista cerrada.
- **Se añaden los nuevos derechos de limitación del tratamiento, portabilidad y oposición**, que aparecieron con el RGPD.
- **Se incluye el principio de trasparencia**. Así, los usuarios deberán ser informados (de forma clara y precisa, con un lenguaje entendible) del tratamiento que se va a hacer de sus datos. También se establece este principio en relación a brechas de seguridad, incidencias que afecten a la privacidad de la información, o denuncias recibidas a través del canal de denuncias.
- **Se ha destinado un título** (el quinto) **a las figuras del responsable y del encargado del tratamiento**, en el que, entre otras cosas, se explican sus funciones y sus responsabilidades.
- **Se establecen los códigos de conducta** a los que se hacía referencia en el RGPD, y que deberán de ser aprobados por la AEPD.
- **Se establecen las sanciones a aplicar por las autoridades de control** (en España, la Agencia Española de Protección de Datos). En este caso, la normativa diferencia entre sanciones leves y graves, establece la aplicación de medidas correctivas y, también, los plazos de prescripción.
- **Queda prohibido el envío de comunicaciones sin el consentimiento del interesado**, salvo las excepciones que ya planteaba la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (que exista una relación contractual previa o que los productos o servicios que se publiciten sean similares a los contratados).

portantes en materia
ión de datos

- **Las asociaciones u organismos sin ánimo de lucro** (con una finalidad política, religiosa, filosófica o sindical) **podrán llevar a cabo el tratamiento de datos personales sin consentimiento expreso de los interesados**, siempre que se refiera a miembros actuales o antiguos (o a beneficiarios de sus ayudas).
- Uno de los puntos más novedosos de la nueva LOPDgdd es el **reconocimiento expreso de los derechos digitales**, que trata de establecer un equilibrio adecuado entre la vida profesional y la personal de los trabajadores. En el ámbito empresarial, tiene especial interés el derecho a la desconexión digital. Establece que, fuera de su horario laboral, los trabajadores no están obligados a utilizar dispositivos electrónicos con motivos profesionales.
- **En transferencias internacionales, la LOPDgdd remite directamente al Reglamento**, que en el capítulo V (de los artículos 44 al 50) recoge las transferencias de datos personales a terceros países u organizaciones internacionales.
- **En el caso de las categorías especiales de datos, la LOPDgdd también remite al Reglamento**. En este caso, al capítulo II, artículo 9.
- **En el canal de denuncia se deberán admitir a trámite las denuncias anónimas** (con la anterior normativa era necesario identificar al denunciante).
- **Un menor de edad solo podrá dar su consentimiento para el tratamiento de sus datos personales cuando sea mayor de trece años.** Aunque por motivos legales puede haber excepciones, el tratamiento de los datos de menores de trece años solo será lícito si cuenta con el consentimiento del titular de la patria potestad o la tutela del menor (con el alcance que esta persona determine).

Además de las novedades, conviene recordar algunos puntos que se mantienen como en la anterior normativa:

- Igual que hacía la anterior LOPD, la nueva establece que **el tratamiento de los datos de contacto de empresarios individuales y profesionales liberales**, así como de quien actúe en nombre o representación de una persona jurídica, **no requerirá de consentimiento expreso** (queda amparado en el interés legítimo del artículo 6.1f del RGPD, así como en el artículo 19 de la LOPDgdd)
- Por otro lado, y aunque la LOPD de 1999 ha quedado debidamente derogada, se mantiene en vigor lo establecido en el Real decreto de desarrollo de la misma (aquello que no contradiga el RGPD). Es necesario tener en cuenta este aspecto, de cara a las medidas de seguridad a aplicar en materia de protección de datos y privacidad de la información. En este sentido, el RGPD establece que, en cuanto a la protección de datos, y en especial a las medidas de seguridad, se debe fomentar en todo momento la mejora continua, lo que conlleva en la práctica aplicar metodologías y estándares reconocidos en la industria (por ejemplo, la norma ISO 27001).

Directiva NIS: algunas reflexiones acerca de su implementación

Con la Directiva NIS (EU Directive 2016/1148) nos encontramos con la primera directiva específica de la Unión Europea que impone medidas concretas de protección frente a ataques y vulneraciones en las redes y sistemas de información de importancia primordial para los Estados miembros: las denominadas infraestructuras críticas.

La idea y el mensaje esencial de la Directiva NIS es fomentar la comunicación y la colaboración entre los países de la UE. Una primera medida para cada país ha sido establecer un CSIRT –centro de respuesta ante las incidencias de seguridad– que tiene un papel esencial en la gestión de los riesgos de seguridad y en la colaboración con organismos similares de otros países, pero también en la selección y recomendación de arquitecturas y soluciones de seguridad para las entidades que son objeto de la Directiva.

Hablando de estas entidades objeto de la Directiva NIS, la mayoría de ellas son los proveedores de servicios esenciales de suministro, comunicaciones, transporte, banca, sanidad y proveedores de las infraestructuras digitales. Todos ellos tienen que poner en funcionamiento estructuras, procesos y soluciones para identificar y mitigar los riesgos operacionales que pueden poner en peligro su funcionamiento y/o suministro.

Una parte importante en la adecuación a la Directiva NIS es la **organización y la planificación de todo el mecanismo, para la identificar y gestionar adecuadamente los puntos críticos, los activos más importantes y los riesgos de seguridad que les puedan afectar.**

Pero, de igual importancia es la preparación y capacidad técnica para prevenir, identificar, responder y mitigar las incidencias de seguridad. Esto significa implementar estructuras, procesos y controles técnicos para la detección, contención y respuesta a los ataques dirigidos avanzados, y a las intrusiones más sutiles y difíciles de detectar.

Cualquier profesional de la ciberseguridad sabe que es difícil o, mejor dicho, imposible encontrar en una solución de seguridad la respuesta a todas las necesidades de una infraestructura crítica. A medida que crece la importancia de los activos, sabemos que un único control de seguridad no es suficiente. Así que, **para adecuarse a la Directiva NIS, se necesita tener probablemente conjuntos de controles de seguridad, tanto a nivel del *endpoint* como de la red**, doblados por controles de continuidad de negocio, de correla-

ción de eventos y analíticas de seguridad; todo gestionado en plataformas de alerta, priorización y gestión de incidencias y/o SOCs.

Nuestra recomendación, como proveedor involucrado activamente en proporcionar soluciones y buenas practicas para cubrir los riesgos de seguridad, es de **construir una arquitectura de seguridad redundante, que reúna la protección de los *endpoints* pero también soluciones y servicios de detección temprana y respuesta a las incidencias (EDR), y soluciones de detección y analíticas a nivel de la red** (como pueden ser un *network sandbox* o una solución de análisis del trafico de red). El resultado de la combinación de este tipo de tecnologías es un incremento importante de la precisión en la detección, la eliminación de los falsos positivos y la posibilidad de priorizar las incidencias de verdad importante.

Otra reflexión que debemos hacer se refiere a los proveedores de suministros. La mayoría de ellos usan plataformas de adquisición y control tipo ICS y SCADA y otros dispositivos IoT/OT. El reto de cubrir todos los frentes es extremadamente importante ante lo que es, como ya hemos visto en los años anteriores, la antecámara de una "ciberconfrontación" con estados que nos son miembros de la UE (nos referimos principalmente a ataques avanzados a las infraestructuras de suministro de energía como Energetic Bear o a las infraestructuras de transporte – Deutsche Bahn). La dificultad de asegurar los activos IoT / OT es conocida, los modelos tradicionales de seguridad por *air-gapping* de la red OT ya se han mostrado vulnerables a los ataques.

Muchas veces, las plataformas que interactúan con los controles industriales no están bajo la gestión del departamento TI, haciéndolas aún más vulnerables. En este caso vemos como posible solución la implantación de controles complementarios de seguridad a nivel de analíticas del trafico de red, capaces de aprender los patrones del tráfico legítimo y detectar el tráfico sospechoso, así como las conexiones a zonas peligrosas del Internet.

Como conclusión, podemos decir que el camino para la aplicación de la Directiva NIS es largo y la mayoría de los actores involucrados están en algún punto, más avanzado o más incipiente. **El objetivo final es complejo, pero es alcanzable con paciencia, dosificación del esfuerzo y pensando que cada largo viaje se hace un paso tras otro.** Nosotros, como siempre, nos ofrecemos acompañarle en el camino.

Horatiu Bandoiu,
ISO 27001 LA
Channel Marketing Manager de Bitdefender

Bitdefender

La irrupción de una nueva religión

La religión emergente más interesante es el ***dataísmo****, que no venera ni a dioses ni al hombre: adora a los Datos.*

Esta sentencia extraída del libro *Homo Deus: Breve historia del mañana* del historiador y escritor israelí Yuval Noah Harari, pone de manifiesto algo que venimos corroborando día tras día: la importancia de los datos.

Ilustración: Ernesto Martín

Los datos son ya el mayor activo de las compañías; el nuevo *combustible de la economía;* el moderno maná, pero en lugar de enviarlo el Dios Yavhé al pueblo hebreo en el desierto, los generamos los humanos en cantidades ingentes para deleite de la computación.

La tecnología ha tenido y tiene un tremendo impacto que ha afectado de manera positiva, y también de forma negativa, a nuestra sociedad, pero ya es algo imprescindible para todos. Las invenciones tecnológicas, motor fundamental del progreso, mejoran nuestra calidad de vida, pero también menoscaban nuestra privacidad.

En esta nueva realidad, virtual o no, no queremos atesorar ideas y conocimientos, queremos compartirlos y ponerlos en común. El empleo y manipulación que realicemos de la información es un reto para la sociedad y se hace necesario una participación más activa y comprometida con su desarrollo e impacto generalizado.

El marco legal establece los límites y, además, controla su cumplimiento para que las personas decidamos lo que queremos hacer con nuestros datos.

Por otra parte, las soluciones de ciberseguridad garantizan el entorno seguro y el nivel adecuado de las organizaciones que usan y aprovechan la información.

Un nuevo perfil profesional ha llegado

El término *cyborg* hace referencia a una criatura compuesta de elementos orgánicos y dispositivos cibernéticos, generalmente, con la intención de mejorar las capacidades de la parte orgánica mediante el uso de tecnología.

Definiendo a la criatura "*cyberlawyer*" podemos coincidir en referirnos a un ser humano mejorado que podría sobrevivir y ayudar a otros en el entorno tecnológico actual y futuro. Se trataría de un experto en derecho, especializado en protección de datos, al que se le haya implantado un conocimiento tecnológico importante o, dicho de otra manera, un especialista en tecnología con aptitudes de ciberseguridad, que mediante una serie de prótesis legales le permita acceso al difícil mundo interpretativo de las normas.

No estoy diciendo que debamos instalarnos un dispositivo en la cabeza para poder escuchar normas y soluciones de seguridad, y conseguir que finalmente las autoridades lo acepten (como ocurrió en 2004 con el artista británico que se implantó un ojo electrónico para *escuchar* los colores que le rodean). Lo que mantengo, es que es hora de que ambas figuras se fusionen y den lo mejor de sí mismas.

El culto al dato hace que la barrera entre abogados y técnicos se desplome y que emerja la figura de un único profesional que unifique las disciplinas legal e informática, componiendo alianzas sobre las actuales grietas académicas y expanda de manera sencilla ideas e innovaciones, a través de los límites de ambas disciplinas.

La asociación abogado/técnico será a la seguridad informática lo que la convergencia IT/OT es a la tecnología.

Hasta hace muy poco el universo OT (*Operation Technology)* para entendernos, "lo industrial", y el mundo IT (*Information Technology*), habían permanecido aislados, autónomos, con caminos paralelos. Es indudable hoy que el mundo OT se ha aprovechado y, por lo tanto, beneficiado, de todos los avances del mundo IT y ha conseguido, además, una considerable reducción de costes. El universo IT, por su parte, ha visto un inesperado progreso con el incremento constante de negocio e inversión. Se ha cumplido finalmente que, a más convergencia, mayor complejidad de los sistemas tecnológicos, y esto, se ha traducido en un incremento considerable de ventas.

No soy abogado, y no menos importante, he de decir que tampoco soy "informático". Con razón cabe preguntarse qué hago opinando entonces y esa, precisamente, es la razón: no pertenezco a ninguno de estos dos mundos y estoy vinculado a ambos. Esta situación privilegiada es la que me habilita para expresar de manera contundente que los dos campos deben unirse o, al menos, interrelacionarse para cumplir con los mejores estándares de la privacidad y la seguridad. Ambos tienen, es más, necesitan desarrollar nuevas capacidades que les permitan una visión más integral de la problemática que gira en torno a los datos.

El marco legislativo y la adopción de medidas de ciberseguridad colocarán en una situación inmejorable a las empresas que coordinen ambas especialidades. Además, la protección con garantías de los derechos y libertades de las personas será un acicate para el desarrollo tecnológico que se verá libre de sospechas al incrementarse la confianza de los interesados dentro de un marco de cumplimiento legal de las organizaciones.

No lo digo yo, la AEPD en la guía para la gestión y notificación de brechas de seguridad dice que: "*La gestión de la privacidad y de la seguridad son entidades distintas con objetivos comunes: salvaguardar los derechos y libertades de las personas y garantizar la seguridad de la información. Responsables de seguridad y delegados de protección de datos están obligados a trabajar juntos estableciendo vínculos colaborativos y ambos son clave cuando se trata de salvaguardar la seguridad de los tratamientos*".

Una cuestión de responsabilidad

El *dataísmo* según cuenta Harari, posee también mandamientos, el primero y principal indica que se debe maximizar el flujo de datos conectándose cada vez a más medios y produciendo y consumiendo más información y, salvo raras excepciones, esto ya está ocurriendo. El siguiente precepto, apunta a que todo debe ser conectado, incluidos los "herejes" que no quieren ser conectados y, aquí, con la iglesia no *dataísta*, obviamente, hemos topado.

Si bien, con los avances de las soluciones y servicios de ciberseguridad podremos proteger cada vez mejor las comunicaciones y los datos, no soy partidario de la libertad de información que suponga sacrificar la privacidad, la autonomía y la individualidad de las personas, al menos, en aquello que consciente e informadamente no convengan de acuerdo con el marco legal que lo regule.

El propio Presidente Ejecutivo de Apple, Tim Cook defiende el RGPD europeo y lo plantea para el resto del mundo. En una parte de su discurso ante el Parlamento Europeo referida a la inteligencia artificial dice lo siguiente: *Si queremos que ésta sea verdaderamente inteligente, debe respetar los valores humanos incluyendo la privacidad. Los peligros son muy grandes si no lo conseguimos. Podemos conseguir al mismo tiempo una gran inteligencia artificial y unos grandes estándares de privacidad. No es sólo una posibilidad, es una responsabilidad.*

De esta **responsabilidad** que atañe a la sociedad emerge como figura reveladora el ***Cyberlawyer***.

Y para finalizar este capítulo, algo importante, ¿cómo detectar a un *cyberlawyer*? Complicado, teniendo en cuenta que no sólo parece humano, suda, huele, sangra y puede imitar voces humanas. Como en *Terminator* nos dejaremos ayudar por los perros, capaces de advertir la presencia de la máquina.

Santiago Arellano

Marketing de producto y desarrollo de servicios en Secure&IT

Ilustración: Ernesto Martín

Secure&IT reconocida como "Mejor partner" de Thycotic

Carlos Ferro entrega a Francisco Valencia el premio como "Mejor Partner del año"

Secure&IT ha sido la empresa reconocida como "Mejor Partner de Thycotic" en los Premios al Mejor Partner del año 2018 en España y Portugal, concedidos por el mayorista Ingecom. El galardón, entregado por Ingecom y el fabricante Thycotic, reconoce la labor hecha por **Secure&IT** en el transcurso de 2018. Este premio hace hincapié, no solo en volumen de ventas, sino también en el cierre de proyectos estratégicos para las compañías.

Francisco Valencia, director general de **Secure&IT** recibió el premio de manos de Carlos Ferro, *Regional Director, Southern Europe, Middle East & Africa* de Thycotic.

En la ceremonia de entrega de los galardones, que tuvo lugar en la fiesta anual de Ingecom, Cristina López, directora de Marketing de la compañía, señaló que estos galardones son especialmente importantes para Ingecom porque reconocen la buena labor realizada lo largo del año por los integradores y por parte de todos los que forman parte de "*la gran familia que es Ingecom*".

Juega seguro y aprende ciberseguridad

Los niños y niñas juegan cada vez menos en la calle o en el parque; los columpios y las pelotas han dejado paso al ordenador, el móvil o la tablet. Para los adultos es, incluso, tranquilizador. Solemos pensar que en su habitación están más seguros, sin peligros que les acechen, ya que están bajo supervisión y parece que no hay riesgos. Pero, ¿somos conscientes de a qué páginas web acceden? ¿Sabemos, realmente, qué hacen en Internet?

Según algunos estudios, casi el 50 por ciento de los niños españoles se ha enfrentado a alguna amenaza *online* (accediendo a contenido inapropiado o entrando en contacto con algún *malware*).

Los juegos en línea son uno de los pasatiempos favoritos de los más pequeños cuando utilizan Internet. En muchos casos, estos juegos son educativos y entretenidos, pero hay otros en los que pueden llegar a ser peligrosos. Hace un tiempo, conocíamos la denuncia de una madre que contó, en Facebook, que el avatar de su hija, de siete años, había sido violado por dos avatares masculinos en una plataforma de juegos *online* dirigidos a menores. Esto demuestra, que no podemos estar completamente seguros y que hay que permanecer informados y alerta.

Queremos ayudarte a que tus hijos jueguen seguro y, también, a que aprendan jugando. Y, para eso, debes saber qué tipo de juegos se pueden encontrar en Internet: educativos, de entretenimiento, comunidades virtuales, de apuestas, violentos e, incluso, sexuales.

Si te preguntas qué puedes hacer ante los riesgos, la respuesta ya te la hemos dado en otras ocasiones: en primer lugar, **utiliza el sentido común.** De la misma forma que estás atento a que las instalaciones de un parque estén en condiciones antes de que tus hijos jueguen en él; o te preocupa el contenido que puedan ver en televisión, debes saber qué hacen cuando navegan en la Red. Siéntate con ellos, averigua cuáles son sus inquietudes y aprende con ellos, a la vez que les enseñas qué deben evitar en Internet.

En nuestra guía práctica de Internet para padres y madres (disponible en nuestra página web **www.secureit.es**) te contamos cómo mantener la seguridad en los ordenadores y otros dispositivos móviles; qué hacer para que utilicen las redes sociales y otros servicios online de forma segura, y, sobre todo, a no ser tú (el adulto) quien cometa la imprudencia (por ejemplo, publicando todo tipo de información sobre tus hijos). Pero, vamos a darte unos consejos para que puedas transmitirles a tus hijos:

- **Cuéntales a qué riesgos se enfrentan:** para eso deberás estar bien informado a través de blogs y webs especializadas en la materia (te proponemos algunas en la guía para padres y madres).
- **Deben tener un buen comportamiento:** explícales que en el ciberespacio no podemos hacer lo que queramos y que, igual que en su vida diaria, hay unas normas de comportamiento que deben cumplir. Evita que sean ellos los que agredan a otros en el mundo *online*.
- **Controla cuánto tiempo pasan jugando:** igual que lo haces con el tiempo que pasan viendo la televisión o jugando en la calle.
- **Asegúrate de que juegan con personas conocidas:** para evitar problemas, asegúrate de

que conoces a las personas con las que juega (familiares o amigos de su entorno). Mejor que sean plataformas a las que no puedan acceder desconocidos.

- **Adviérteles que no deben compartir información personal:** no deben compartir información suya, ni del resto de la familia. Por supuesto, no deben enviar fotos a extraños (de ningún tipo, pero mucho menos si son comprometidas).

- **Enséñales a comunicarse contigo:** si en algún momento notan algo raro o se sienten acosados, agobiados o inseguros deben comunicártelo.

- **Bloquea todo tipo de juegos sexuales, violentos o de apuestas:** explícales que estos no son juegos para niños.

¿Quieres que aprendan jugando?

Te vamos a proponer algunos juegos que, además de entretenerles, les enseñan a navegar seguros en la Red:

- **Cyberscouts:** este juego que podrás encontrar en la web de la Oficina de Seguridad del Internauta (www.osi.es) está pensando tanto para niños, de más de 6 años, como para padres. Hay un área para los más pequeños y otra para adultos, con distintos niveles de dificultad. Aquí encontraréis retos en forma de juegos, preguntas y vídeos.

- **Hackers vs. Cibercrook:** también está disponible en www.osi.es y permite a los más pequeños aprender sobre ciberseguridad (contraseñas seguras, copias de seguridad, wifi públicas, etc.), a la vez que se divierten. Jugarán con el rol de Sergio, un chico que tendrá que proteger su casa de los ataques de Cybercrook.

- **Interland:** Google ha creado este juego *online* para concienciar y enseñar a los niños los aspectos más importantes de la ciberseguridad. En esta aventura, los más pequeños encontrarán cuatro mundos en los que se enfrentarán a diversos retos: ciberdelincuentes, acosadores, personas con las que comparten demasiada información o suplantadores de identidad, entre otros.

- **Hackend:** tú también puedes jugar y aprender. Por eso, te proponemos este juego para adultos, que encontrarás en la web de Incibe. En este caso, podrás ayudar a Max a resolver algunos episodios en los que la seguridad de su pyme se ha visto comprometida.

Si quieres conocer los peligros a los que se enfrentan tus hijos en el entorno digital y qué hacer para evitarlos, visita nuestro blog (www.secureit.es/blog) y encontrarás toda la información y consejos que necesitas.

Secure&IT

www.secureit.es