IDG RESEARCH SERVICES

Security Day:
"Follow the Sun"

# Estado de la Seguridad en España en 2018

DIAMOND

LOGICALIS Business and technology working as one

RSA

FORCEPOINT

Akamai NETALLIANCE PARTNER Telefónica

GOLD

KASPERSKY lab

SOPHOS

vmware

SILVER

CITRIX

hp intel

# Índice


| | | |
|---|---|---|
| | Introducción | 3 |
| I. | Fase expansiva: los presupuestos de seguridad crecen | 4 |
| II. | El CISO gana presencia en las empresas | 6 |
| III. | El ciclo de seguridad está anclado en la prevención | 8 |
| IV. | Dónde no se invierte lo suficiente | 14 |
| V. | Mirando hacia el futuro | 17 |
| VI. | Conclusiones | 19 |
| VII. | Ficha técnica | 21 |
| VIII. | Partners de seguridad | 22 |

# Informe sobre seguridad en España en 2018

En este informe ejecutivo, IDG Research Services presenta los resultados principales de la encuesta "Security Day 2018" llevada a cabo a los 127 responsables de seguridad que participaron en el evento que tuvo lugar en nuestro país.

La concienciación sobre la ciberseguridad es más elevada que nunca. En palabras de Warren Buffet, los ciberataques representan la mayor amenaza para la humanidad, por encima de las armas nucleares. Las pequeñas empresas que ponían la seguridad en un segundo plano, pensando que eran objetivos poco atractivos para un atacante, han visto cómo en los últimos años han pagado el precio de ataques como el ransomware.

Son cada vez más las empresas que, sin importar su tamaño, crean el puesto específico de CISO para la seguridad. Su reto en las pymes es la falta de cultura de ciberseguridad mientras que en la gran empresa es la escasa integración con el negocio.

Las organizaciones se dan cuenta de que no es suficiente con concentrarse en prevenir ataques, tienen que estar preparadas para detectarlos a tiempo y responder con agilidad. Esta capacidad sobrepasa el ámbito tecnológico y deja claro que la seguridad no puede relegarse a una persona, sino que es responsabilidad de toda la organización. Por ello, el CISO necesita tener una posición de influencia y visibilidad.

**El CISO tendrá que entender y adoptar nuevas tecnologías** que aparecen a un ritmo vertiginoso. Por ejemplo, la inteligencia artificial encierra la principal promesa y amenaza a la seguridad. Como promesa permite liberar a su equipo de muchas tareas manuales y concentrarse en la toma de decisiones. Pero no puede ignorarse que al mismo tiempo es un arma utilizada por los propios atacantes a los que les dota de armas adicionales.

Aunque estamos en una fase de expansión en lo que se refiere a presupuestos de seguridad, las empresas tienen que elegir bien dónde dirigen sus esfuerzos y recursos. Para ello, es necesario elevar la perspectiva de seguridad por encima de la tecnología y basar las decisiones en un entendimiento de las implicaciones para el negocio.

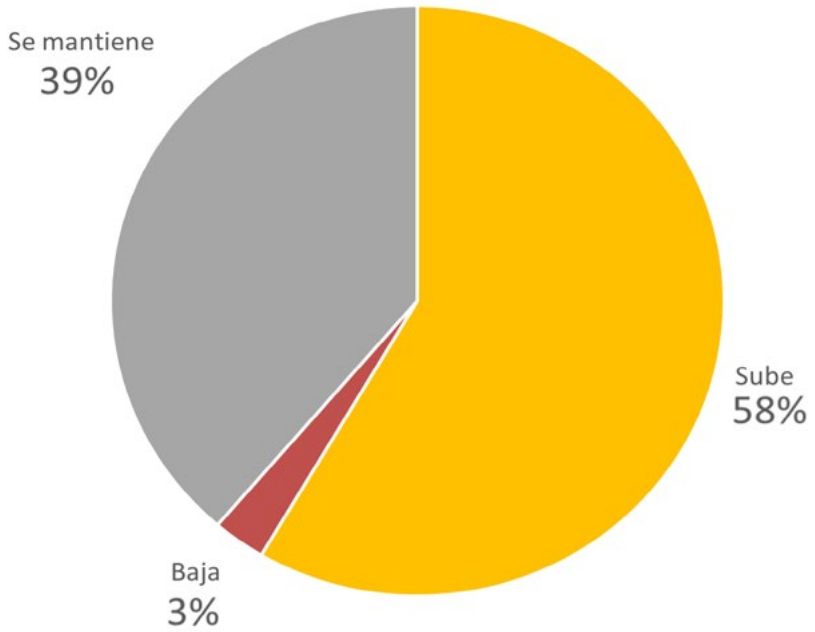
# I. FASE EXPANSIVA: LOS PRESUPUESTOS DE SEGURIDAD CRECEN

La seguridad sigue ganando relevancia dentro de las organizaciones: el aumento de los presupuestos de seguridad es un fenómeno global, pero en España se produce con gran contundencia: aumenta en un 58% de las empresas encuestadas y solo disminuye en un 3%. Los motivos de esta fase expansiva hay que buscarlos en tres aspectos que se están produciendo de forma simultánea: mayor impacto en el negocio, mayor sensibilización y una regulación que se ha vuelto mucho más exigente.

- **Los ataques impactan al negocio más que a las operaciones.** El componente digital de los negocios está creciendo. En consecuencia, una brecha tiene relevancia ya no solo para las operaciones (ej. una parada), sino para la seguridad del propio cliente que puede ver sus datos comprometidos. Por ello, el impacto afecta a la confianza del cliente y por tanto a la generación de ingresos.

- **La sensibilidad a la seguridad va más allá del departamento de TI.** La amplia cobertura mediática de casos de ransomware como WannaCry, ha concienciado a la organización que ha visto cómo no solo se creaban brechas, sino que la propia empresa recibía un chanta-

**Presupuestos en ciberseguridad de 2018 frente a 2017**




*Fuente: IDG Research Services. Estudio de Seguridad 2018*

je. La seguridad empieza a percibirse como algo que concierne a todos, no solamente al departamento de tecnología de la organización.

- **La regulación está diseñada para proteger el negocio digital.** La regulación está pensada no solo a corto plazo sino mirando a un futuro digital para el que hay que prepararse ahora. Es deliberadamente imprecisa para que cada empresa encuentre su camino de operar de forma segura. Lo que no es impreciso son las multas de hasta un 4% de la facturación a nivel de grupo que impone GDPR. Esto consigue reforzar el caso de negocio para que aumenten los recursos dedicados a la seguridad.

El **58%** de las empresas incrementarán sus presupuestos en seguridad.

**Ataques como WannaCry han concienciado a todos los niveles de las organizaciones**

## II. EL CISO GANA PRESENCIA EN LAS EMPRESAS

Un aspecto que refleja la importancia de la seguridad entre las empresas españolas es que hoy la figura del CISO es prácticamente omnipresente en las grandes organizaciones y entra cada vez más en las medianas y pequeñas. Lo importante no es solo la decisión de crear el cargo de CISO, sino la de dónde se le ubica en la organización. Estas dinámicas se pueden ver por separado.

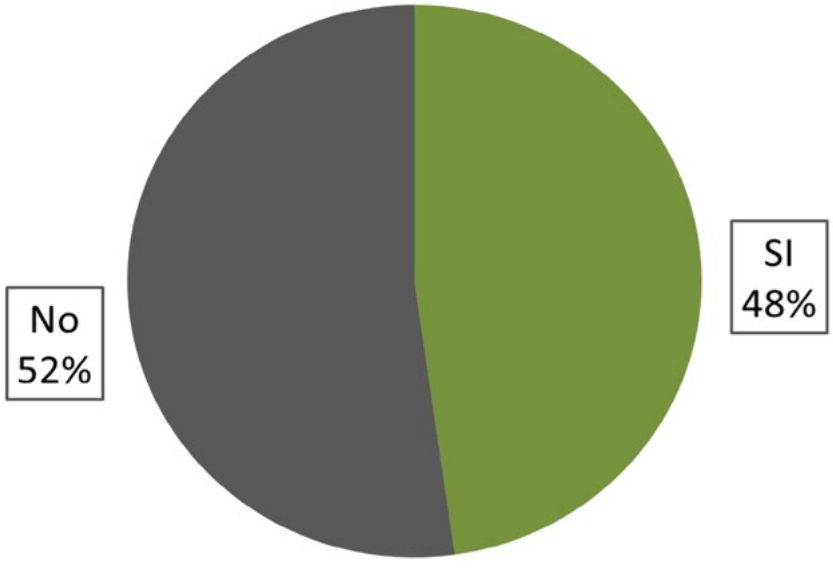
- **El CISO se extiende a la mediana y pequeña empresa.** Se trata sin duda de un reflejo de que los ciberataques a empresas de menor tamaño están aumentando. La ciberseguridad no puede quedarse al margen de su estrategia de negocio. De acuerdo con el Ponemon Institute, la proporción de empresas pequeñas que han experimentado ataques ha pasado del 55% en 2016, a un porcentaje del 61% en 2017.

- **EL CISO gana visibilidad en la estructura organizativa.** El CISO ya está presente en el 84% de las grandes empresas y además adquiere mayor peso en la organización. Dentro de las grandes compañías se percibe una tendencia a romper la dependencia tradicional del CISO con el área de sistemas. Se está abriendo paso dentro del área de gestión de riesgos, llegando incluso a reportar al director financiero. En algunos casos, tiene interlocución directa con el CEO. En definitiva, la ubicación del CISO es un reflejo de la importancia estratégica que otorga la organización a la seguridad.

El **61%** de las pymes sufrió algún tipo de ataque en 2017.

**La ciberseguridad no puede quedarse al margen de la estrategia de negocio**

**Presencia del CISO**




*Fuente: IDG Research Services. Estudio de Seguridad 2018*

N = 127

RSA

# ¿Puede hacer esto tu SIEM?

## Detecta de forma instantánea el alcance completo de un ataque

### Con RSA NetWitness® Platform

Learn more at rsa.com/en-us/products/threat-detection-response

## III. EL CICLO DE SEGURIDAD ESTÁ ANCLADO EN LA PREVENCIÓN, PERO SE ACERCA UN CAMBIO

Hemos visto que en conjunto crece el presupuesto de seguridad. Ahora sus responsables tienen que plantearse cómo reparten ese presupuesto, teniendo en cuenta que crecen también las necesidades.

Si consideramos las tres fases del ciclo de seguridad, (prevención, detección y respuesta), el enfoque que prevalece es el preventivo. De acuerdo con este estudio, un 58% de las empresas participantes consideran prioritario desarrollar un enfoque preventivo, mientras que la mejora de la capacidad de detección y repuesta baja hasta el 47%.

La prevención, aunque necesaria, no puede garantizar la seguridad al 100%. Un ataque inteligente y sofisticado, terminará encontrando la forma de traspasar las defensas. Los ciberdelincuentes innovan a un ritmo vertiginoso. La pregunta ya no es si conseguirán entrar en la empresa, sino que cuando lo hagan, cuánto tiempo llevará su detección para articular una respuesta.

En relación con la detección, existen dos motivos para dedicarle más recursos: la lentitud en la detección de un ataque y su complejidad.

- **El tiempo de detección es demasiado largo, permitiendo al atacante causar el perjuicio.** Los datos de Ponemon Institute de 2017 indican que el tiempo promedio de detección de una brecha es de 206 días. Es preocupante que este tiempo ha empeorado con respecto al año anterior. **El problema principal de la detección está en que hay una diferencia de orden de magnitud entre los tiempos de un ataque y los tiempos de detección.** Una vez que se ha realizado una brecha, extraer datos de clientes puede llevar minutos u horas; extraer datos críticos, días o incluso semanas. Sin embargo, detectar un ataque, hemos visto que lleva en promedio entre 6 y 7 meses. Esta discrepancia no es sostenible en una economía digital.

- **La detección de un ataque es compleja y necesita recursos,** dado que requiere interpretar información de muchas fuentes, y detectar patrones anómalos. Además, hay que contar con la posibilidad de falsos positivos, que puedan producir fatiga en el equipo y en toda la organización. Por tanto, la detección requiere una madurez a través de un aprendizaje, para lo que es recomendable

El **58%** de las empresas considera clave desarrollar la prevención mientras que el **47%** prefiere mejorar la detección y repuesta

# Kaspersky® Threat Management & Defense

## Minimice el riesgo de ciberseguridad en la transformación digital.

Combinación única de tecnologías y servicios basada en la implementación de una estrategia de seguridad adaptativa, que permite:

- PREVENIR y reducir el número de amenazas complejas y ataques dirigidos
- DETECTAR e identificar las actividades sospechosas (ataques dirigidos)
- RESPONDER ante las brechas de seguridad e investigar los ataques
- PREDECIR dónde y cómo se producirán los próximos ataques

ponerla en marcha cuanto antes y si es posible, apoyarla en métodos de inteligencia artificial.

**206**
días es el tiempo medio de detección de una brecha

Una vez detectado el ataque es necesaria una capacidad de respuesta ágil por parte de todos los departamentos de la organización para mitigar los daños que puedan ocasionarse. Esto va a requerir de un plan predefinido previamente, a lo que se le une el ser tremendamente transparente con el cliente y los datos que hayan podido verse afectados.

- **Una respuesta adecuada va a implicar a toda la organización.** Partimos de que si el período de detección ha sido largo, las opciones de respuesta disponibles son limitadas, ya que el daño está hecho. Aun así, la capacidad de respuesta sigue siendo esencial, por ejemplo, para evitar una fuga de clientes y limitar las consecuencias adversas para el negocio. El reto se encuentra en que una respuesta adecuada sobrepasa el ámbito del equipo de seguridad. Aquí la capacidad de influencia del CISO y su posición en la organización tienen especial relevancia.

El **51%**
de empresas considera que necesita mejorar su cumplimiento con GDPR

- **La capacidad de respuesta requiere un plan predefinido.** Tras una brecha será necesario activar un plan de contingencia establecido de antemano. Para diseñarlo y ejecutarlo es necesario comenzar por un análisis exhaustivo de escenarios y definir un equipo que pueda movilizarse cuando tenga lugar la incidencia. Este equipo es necesariamente multidisciplinar y puede abarcar por ejemplo la atención al cliente, Marketing, operaciones, legal y Recursos Humanos. Un ejemplo de falta de planificación fue el caso de Equifax, donde los recursos dedicados a la atención al ciudadano fueron improvisados e insuficientes, además de que inicialmente se les exigía un pago para verificar si sus datos habían sido comprometidos.

- **La respuesta debe incluir la comunicación a los clientes, que tiene que ser ágil.** En concreto, GDPR da 72 horas desde la detección de una brecha para notificarla a los clientes y al regulador. También hay que tener en cuenta la comunicación tanto a la dirección de la empresa como a los partners u otros agentes que puedan ver-

LOGICALIS
Business and technology working as one

IBM Platinum Business Partner

# La protección de datos personales que exige GDPR

¿Qué empresa no está interesada en mejorar su nivel de seguridad y cumplir con la nueva normativa? Evite sanciones, pérdidas de imagen y disminución de su negocio.

Logicalis Spain ya está acompañando a sus clientes hacia la seguridad necesaria: analizada y unificada para cumplir con GDPR

Con **IBM Guardium e IBM Security:**
- Monitorice los accesos (quién, cómo, desde dónde)
- Garantice la securización y el cifrado de sus datos.

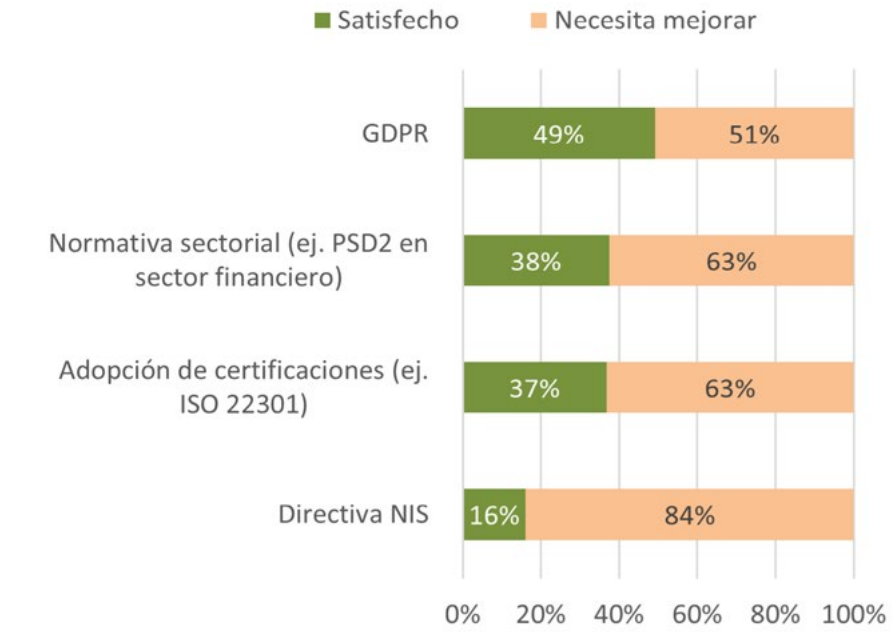
Descárguese la guía gratuita y descubra cómo IBM y Logicalis pueden ayudarle

Web
www.es.logicalis.com

Teléfono
91 766 90 69

Email
marketing-es@es.logicalis.com

## En relación con su organización, ¿en cuál de los siguientes aspectos regulatorios están más avanzados?




*Fuente: IDG Research Services. Estudio de Seguridad 2018*

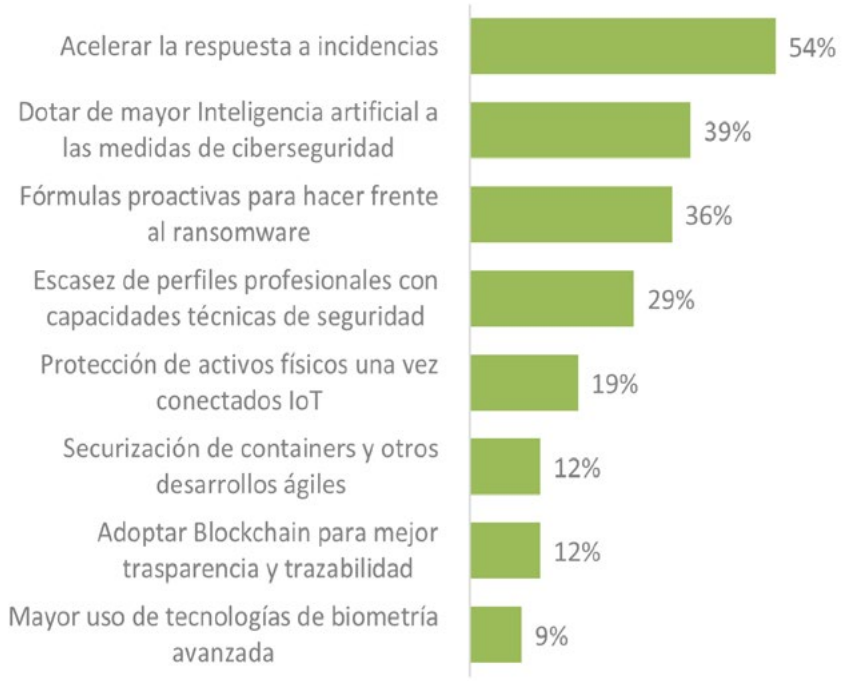
El **39%** de empresas dotará de mayor inteligencia artificial a las medidas de ciberseguridad desplegadas

se afectados. El denominador común de la respuesta es que tiene que ser ágil; no puede hacerse esperar.

En definitiva, los tres elementos del ciclo tienen que cubrirse. Si no hay prevención, los recursos de seguridad estarían continuamente comprometidos resolviendo brechas. Si no hay detección, la reacción se produce cuando ya se ha producido el daño. Si no hay respuesta adecuada, el negocio puede verse seriamente afectado, además de incidir en un posible incumplimiento normativo tras la entrada en vigor de la nueva normativa Europea.

En este equilibrio de fuerzas se está observando un desplazamiento desde la prevención hacia la detección y respuesta, algo que no solo ocurre en nuestro país, sino en todo el mundo. De hecho, para los próximos 3 años, un 54% de las empresas que fueron encuestadas va a invertir en soluciones y sistemas que les permitan acelerar su respuesta ante la aparición de incidencias de seguridad. De los encuestados, un 39% de las organizaciones se plantea adoptar medidas de ciberseguridad que contemplen el uso de tecnologías de inteligencia artificial con el fin de ofrecer una mejor respuesta ante los incidentes. En definitiva, aplicar fórmulas proactivas para

**¿Cuáles de las siguientes tendencias tendrán mayor impacto en su estrategia de ciberseguridad en los próximos 3 años?**




*Fuente: IDG Research Services. Estudio de Seguridad 2018*

hacer frente a las nuevas amenazas como pueda ser el ransomware.IV. DÓNDE NO SE INVIERTE LO SUFICIENTE

En este informe también queremos destacar los aspectos que no reciben suficiente atención y sin embargo, tienen gran relevancia para la seguridad. Esta situación se refleja en el gráfico siguiente, donde se aprecia la baja prioridad que reciben.

### Se presta más atención a la tecnología que al empleado

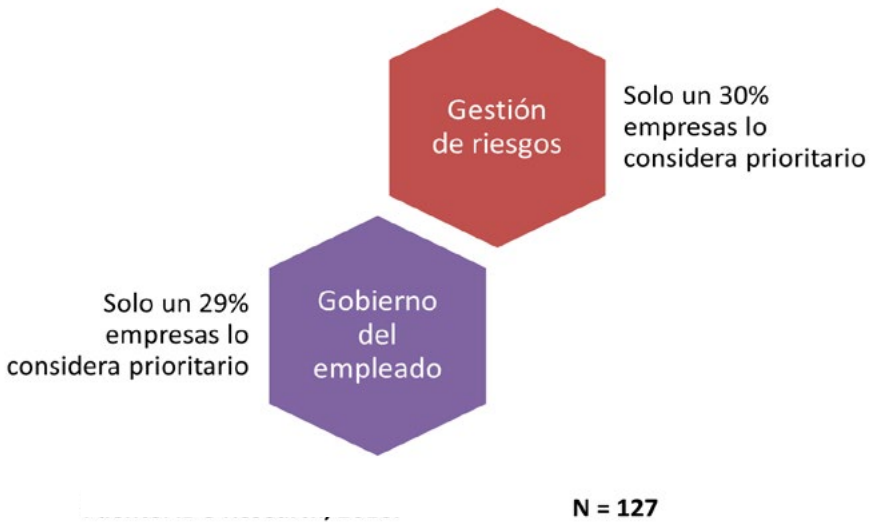
El empleado es el eslabón más débil de la seguridad de la organización y pieza esencial de la misma, tal y como se comentó en una de las mesas redondas del IDG Security Day de 2018.

De hecho, Ponemon Institute destaca que el 56% de las empresas reconocen un riesgo de robo de datos por parte de sus empleados, en particular aquellos que van a abandonarla o los que acaban de incorporarse.

El gobierno del empleado es también una exigencia regulatoria. El reglamento GDPR establece que se debe informar al cliente del uso que se hace de su información. Ello implica que la empresa debe saber en primer lugar quién accede a la información y qué uso hace de la misma.

Un ejemplo de lo crítico que puede llegar a ser el empleado para la seguridad lo podemos ver en un caso reciente: Elon Musk (fundador de Tesla y otras iniciativas) enviaba una carta a toda su plantilla alertando de la posibilidad de que un empleado malintencionado había realizado  acciones de sabotaje. Su preocupación es que se pueda llegar a comprometer código. No solo les ha pedido estar en alerta,

**Dónde se invierte lo suficiente**




*Fuente: IDG Research Services. Estudio de Seguridad 2018*

# Forcepoint presenta la primera solución Risk-Adaptive Protection de la industria, llamada Dynamic Data Protection.

Desarrollada para afrontar la avalancha de amenazas complejas y sofisticadas que aquejan hoy a las empresas, Risk-Adaptive Protection de Forcepoint evalúa constantemente el riesgo y ofrece automáticamente una ejecución proporcional que puede elevarse o reducirse. Esta capacidad es posible a través del poder del análisis de comportamientos centrado en los usuarios, el cual entiende las interacciones que tienen con los datos, las máquinas y las cuentas. El contexto inteligente acelera la toma de decisiones y los controles de seguridad específicos para cambiar el riesgo en las redes empresariales. Con la primera capacidad de ejecución automática que se adapta de manera dinámica, los analistas de seguridad pueden centrarse en actividades de alto valor y eliminar la acumulación de alertas de las herramientas de seguridad tradicionales, reduciendo el tiempo necesario para detectar y mitigar el riesgo de días o meses, a segundos.

La analítica del comportamiento humano finalmente ofrece protección efectiva de datos.

Con la analítica del comportamiento centrada en los usuarios, Forcepoint Dynamic Data Protection aplica la calificación anónima de los comportamientos, la cual se actualiza continuamente con la finalidad de establecer una base de comportamiento “normal” de cada usuario final, en las redes corporativas o no gestionadas. Los sistemas inteligentes de Forcepoint, informados por la evaluación del riesgo individual, aplican entonces una serie de contramedidas de seguridad para afrontar el riesgo identificado. Por ejemplo, Forcepoint Dynamic Data Protection permite la monitorización y el acceso a los datos, dar acceso a las descargas aunque cifrándolas, o bloquear totalmente el acceso a archivos sensibles, dependiendo del contexto de las interacciones individuales con los datos corporativos y la calificación de riesgo resultante.

La capacidad de una organización para adaptar la política de ejecución al riesgo más critico de manera automática, puede marcar la diferencia en el objetivo de proteger los datos críticos de los clientes, la propiedad intelectual e, incluso, el propio éxito de una misión.

FORCEPOINT

sino informar de cualquier situación o comportamiento que les resulte anómalo.

En este estudio se ha detectado una preocupación creciente por el dispositivo, especialmente por el endpoint, por parte de un 49% de las empresas. Sin embargo, esto no se traduce en la prioridad de un gobierno robusto del empleado, señalada solamente por un 29% de las mismas que fueron encuestadas.

### Las decisiones de seguridad no parten de un análisis de riesgos

Las empresas están en un contexto de amenazas crecientes pero de presupuestos limitados aunque crezcan. Ello implica que hay que asignar los recursos de seguridad allí donde sean más necesarios. Uno de los criterios de más peso para esta decisión es el análisis de riesgo, tanto interno como para el cliente. Sin embargo, solo un 30% de las empresas encuestadas lo considera prioritario.

También aquí el reglamento GDPR deja claro que la seguridad ya no se organiza sobre una lista predeterminada de acciones (como en el caso de la LOPD). Cada empresa debe crear su propia lista en función de un análisis de riesgo e impacto.

Las decisiones sobre seguridad muchas veces conllevan situaciones de compromiso, como el coste de proteger frente al coste del impacto. Un ejemplo es el lanzamiento de un nuevo producto o aplicación; cuanto antes se realice, mayor es la ventaja competitiva y la capacidad de generar ingresos. Pero, a su vez, es necesario un testing de seguridad que puede retrasar la comercialización del producto.

Las empresas tienen que tener muy claro cuáles son sus riesgos, el impacto de una brecha, y el coste de evitarla. Una vez realizado dicho análisis, tienen que tener clara la propensión al riesgo de su organización. En función de esto tendrán que decidir qué riesgos asumen, lo que conlleva tomar decisiones de compromiso. Sin un análisis previo las decisiones de seguridad de la organización estarán muy condicionadas por la urgencia de resolver la situación.

# V. MIRANDO HACIA EL FUTURO

En este apartado destacamos las prioridades de empresas participantes, tanto en innovación como en inversión para los próximos 3 años. Estas se muestran en el gráfico de abajo. Los porcentajes hacen referencia a las empresas que lo indican como prioridad elevada.

### Resolver la seguridad de las nuevas aplicaciones y DevOps

La seguridad en los nuevos desarrollos es un aspecto todavía no resuelto. Representa una prioridad alta para el 45% de las empresas del estudio. Teniendo en cuenta que no todas están adoptando DevOps, esto refleja que la seguridad se considera prioritaria antes incluso de ser adoptada.

La práctica habitual del testing de seguridad ha sido llevarlo a cabo una vez entregada la aplicación. Sin embargo, si los resultados son desfavorables se puede ralentizar o parar un desarrollo. En estos casos, se cancelan las ventajas que ofrece DevOps. Por eso, se están integrando los ciclos de pruebas de seguridad dentro de cada iteración. Para que esta integración no destruya la agilidad, es necesario evitar el componente manual e introducir automatización en las pruebas de seguridad.

### Introducir inteligencia artificial/machine learning:

La inteligencia artificial representa una tendencia de inversión en los próximos 3 años para el 39% de las empresas participantes. En conjunto, las nuevas generaciones de malware y ciberataques son cada

**Innovación y prioridades futuras**


*Fuente: IDG Research Services. Estudio de Seguridad 2018*

vez más difíciles de detectar con los protocolos de ciberseguridad convencionales. Es aquí donde Machine Learning facilita la detección y respuesta, ya que aprende de los datos de ataques anteriores y automatiza la respuesta.

La inteligencia artificial no debe considerarse una panacea. En primer lugar, se tiene que producir el aprendizaje inteligente de forma efectiva. Pero además, hay que tener en cuenta que los atacantes también usan machine learning y utilizarán la estrategia de confundir a los modelos. La denominada ''Adversarial AI'' se basa en estudiar los modelos de aprendizaje, así como posibles sesgos, para confundirlos o eludir su detección.

**El 29%**
de las empresas considera crítica la seguridad en IoT

### Fórmulas proactivas para hacer frente al ransomware:

La respuesta al ransomware es muy importante para el 36% de los participantes. A pesar de la gran repercusión mediática de ataques como WannaCry o el caso de Uber, la capacidad del ransomware de causar perjuicio ha sido muy superior a la de generar ingresos para los atacantes.

En el caso de WannaCry, la estimación sobre los ingresos obtenidos fue 143.000 dólares (Elliptic). Cada vez son más las empresas que se niegan a pagar el rescate, ya que estiman que ya han sufrido el daño, y no confían en criminales. Por ello, a pesar del elevado volumen de ransomware en 2017, los atacantes ya están buscando otros modelos de negocio más rentables e incluso variantes de esta amenaza. Un ejemplo son los ataques de cryptojacking/cryptomining de creciente popularidad.

### Integrar la seguridad de IoT

La seguridad en IoT se torna crítica para el 29% de empresas. Gestionar el mundo físico que nos rodea incrustando sensores en activos, productos e incluso en personas conlleva nuevos retos difíciles de ignorar. El enfoque de la seguridad debe abarcar tanto la seguridad lógica como la física de los objetos sensorizados. Basta pensar en un vehículo autónomo para entenderlo. Aquí la seguridad abarca a la propia conducción del vehículo, entrando en el ámbito de la seguridad vial.

Otro reto que habrá que considerar es cuando los objetos comiencen a comunicarse entre sí de forma descentralizada en modelos ''peer to peer''. En este escenario, poder controlar la seguridad va a requerir la colaboración del ecosistema de fabricantes que haya detrás de esos objetos. La industria dista mucho de estar abordando esto en la actualidad. Una forma de hacerlo sería trabajar sobre APIs abiertas, lo cual permitiría a las empresas superar fragmentación actual para tener una visión integrada.

# VI. CONCLUSIONES

### Entender la seguridad en un contexto de gestión de riesgos.

No existe todavía una cultura de seguridad basada en el riesgo de negocio. Sin embargo, el verdadero reto es la desconexión entre la alta dirección y el equipo de seguridad. La dirección se preocupa de aspectos como desventajas competitivas, la pérdida de propiedad intelectual, o el coste de las multas, mientras que el equipo de seguridad mantiene una visión de riesgo ligada a la tecnología y los activos de su compañía.

Es necesario que el análisis de riesgos abarque criterios tanto de tecnología como de negocio y que ambas perspectivas se encuentren. En este punto, la seguridad no puede tratarse como un absoluto, sino como una decisión de negocio en la que se asumen ciertos riesgos.

### Empoderamiento del CISO como cargo integrado en el negocio

El CISO no puede limitar su interlocución a la función de "semáforo", que actúa al final para dar su aprobación o consentimiento, o bien, para frenar un determinado proyecto. Su función debe ser la de integrarse en los proyectos, bien contribuyendo a las pruebas de seguridad, o bien entrando desde el diseño. De este modo, la seguridad entra por defecto de forma nativa en la actividad del negocio.

Está claro que la seguridad no es la responsabilidad de una persona, ni la de un equipo. Es necesario crear una cultura de seguridad que abarque a los hábitos de toda la organización, y para ello, el CISO necesita una posición que le otorgue visibilidad e influencia sobre las demás áreas y directivas.

### El ciclo de seguridad debe desplazarse hacia la detección y respuesta

El enfoque basado en la prevención que prevalece no solo en España, sino también en el mundo, no es suficiente. Hay una concienciación de que no se puede garantizar la seguridad al 100%. Sin embar-

go todavía existe un amplio margen de mejora en torno a la detección y respuesta.

Para que ambas funcionen es necesario que participen otros departamentos, como Recursos Humanos (gobierno del empleado), Marketing o servicio al cliente (respuesta de negocio en caso de una brecha). La seguridad ya no depende ni de una tecnología, ni de un departamento. Es necesario un enfoque que involucre a todos los actores.

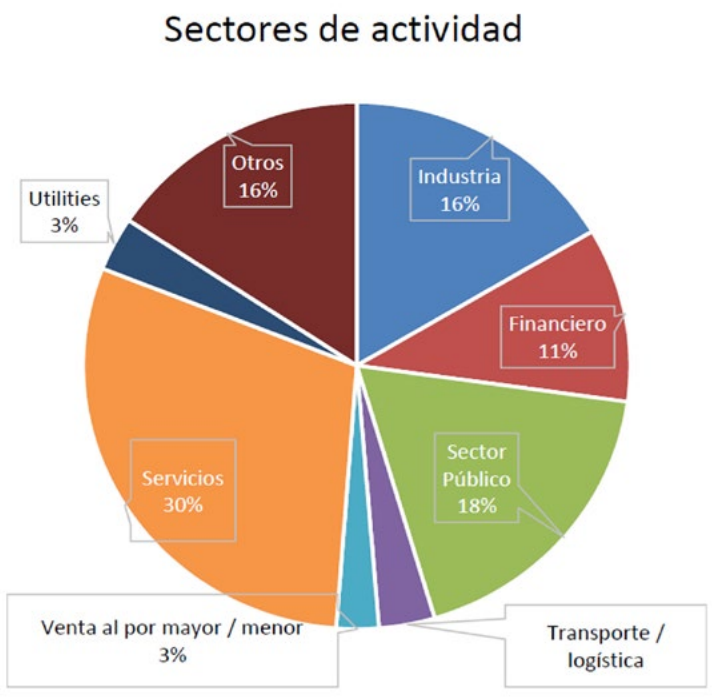
### Automatización inteligente: la respuesta al imperativo de agilidad

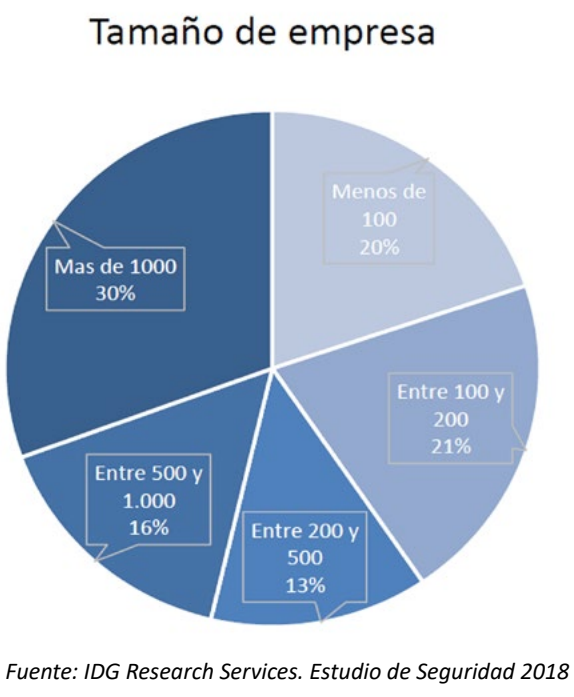
La seguridad se encuentra ante un imperativo de agilidad. Esto no solamente aplica a la detección y respuesta, sino también al desarrollo de aplicaciones y a las operaciones. Es decir, la seguridad no puede ser un freno para la actividad del negocio. Por tanto, no puede apoyarse en acciones manuales lentas que además están sujetas a cometer errores.

La automatización inteligente representa el camino hacia el futuro ya que libera tiempo de los profesionales de seguridad y hace más eficiente y ágil la detección y respuesta. Además, contribuye a resolver la escasez de personal cualificado.

No obstante, las limitaciones de la inteligencia artificial seguirán haciendo necesaria la intervención humana, en particular en el caso de amenazas complejas o de decisiones de compromiso. El futuro de la seguridad se apoyará sin duda alguna, en la colaboración entre personas y tecnología.

## Demografía de las empresas participantes



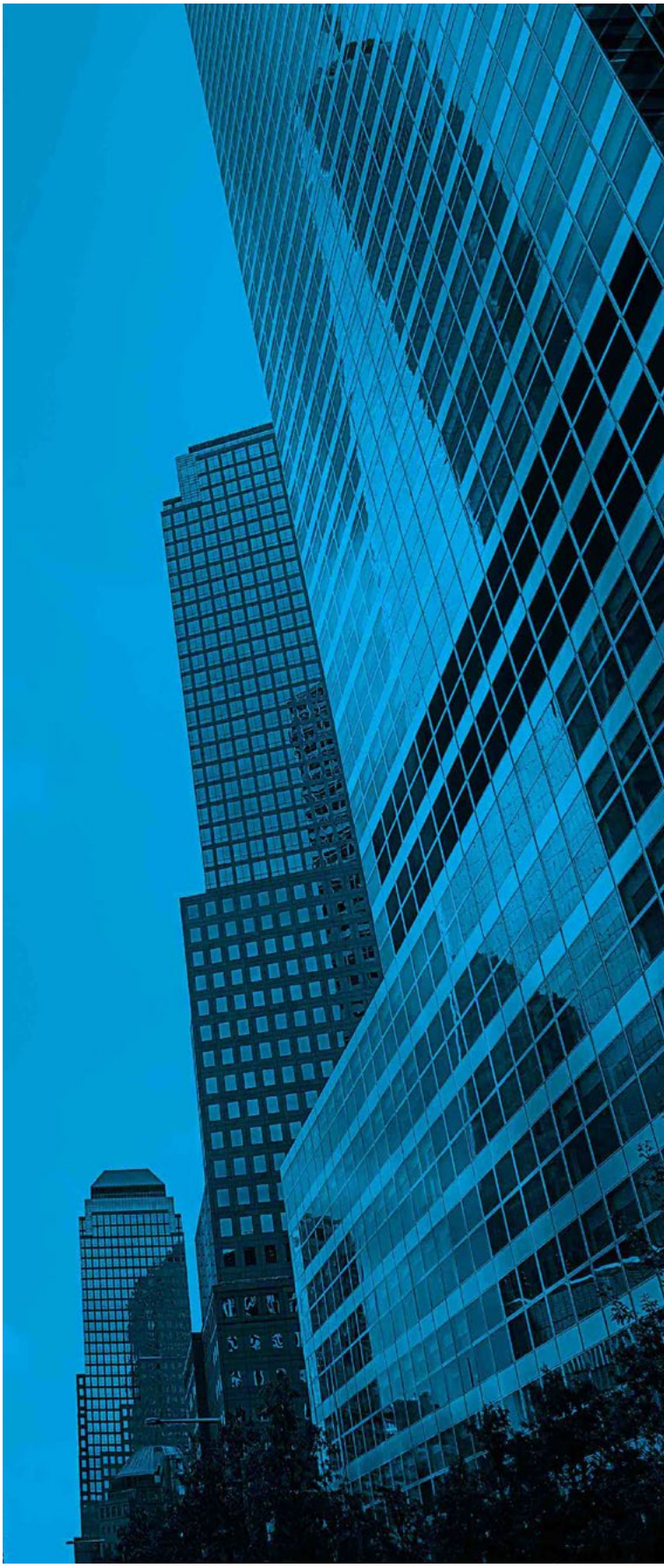

*Fuente: IDG Research Services. Estudio de Seguridad 2018*

## VII. FICHA TÉCNICA

Este estudio se ha llevado a cabo mediante una encuesta online durante el pasado mes de junio de 2018. El cuestionario fue autoadministrado y representa el universo de empresas que asistieron al evento de IDG Security Day de 2018.

El número total de encuestas completadas fue de 127. Su desglose, según tamaño de empresa y sector de actividad, puede verse en los gráficos de la página anterior, permitiendo extraer conclusiones sobre el estado de la seguridad en el que se encuentran las organizaciones de nuestro país.

La automatización inteligente contribuye de manera eficiente a resolver la escasez de personal cualificado



# Partners de seguridad


GDPR: es la hora de ponerlo en práctica 23

Cómo lo hice 24

Detección y respuesta a incidentes 25

El CIO debe dar forma a la transformación digital 26

“Cibersecurity made simple” 28

La protección de las aplicaciones y los datos 29

Cómo contactar con los expertos 30

# GDPR: es la hora de ponerlo en práctica

David Angulo, BDM Consultant de Logicalis, afirma que ''es el momento de dejar la teoría a un lado y poner en práctica las demandas de una normativa transversal que afecta a todas las organizaciones, especialmente a las europeas''.

Desde hace un mes escaso, el nuevo Reglamento General de Protección de Datos (GDPR, por sus siglas inglesas) es ya una realidad. Y más que lecciones teóricas, que ya han sido promulgadas en gran cantidad durante los dos últimos años, lo que necesitan las empresas es poner en práctica la protección y la privacidad de datos de los usuarios si no quieren tener que enfrentarse a las sanciones que reserva la normativa. Por ello, David Angulo, BDM Consultant de Logicalis, intervino en el evento IDG Security Day ejemplarizando sobre cómo pueden llevarse a cabo estas demandas de manera sencilla y eficaz.


> "Nuestra plataforma ofrece una protección global y horizontal"

En el imaginario, Angulo ha colocado a un cliente, procedente de un proyecto de fusión de distintas compañías y para el cual es muy difícil encontrar un modelo de clasificación de datos; saber cuáles son sensibles y cuáles no y establecer una estrategia de seguridad en torno a ese panorama. ''Nosotros ayudamos a aplicar políticas de seguridad, métodos de protección, cifrado o capas de monitorización para que en caso de que haya comportamientos anómalos, poder actuar''. Y lo hacen de la mano de IBM y de su plataforma Guardium que, según el directivo, puede cubrir gran parte del montante de artículos de GDPR.

La solución distingue tres procesos. Por una parte, es elemental el descubrimiento y clasificación de los datos. Se trata de definir una búsqueda y unos patrones para encontrar cualquier parámetro y más adelante escoger las bases de datos necesarias y poder vincularlas a las políticas de seguridad. El segundo paso es escanear las vulnerabilidades de las diferentes bases de datos para, por último, monitorizar y auditar el acceso a los datos sensibles. ''Además, Guardium no solo cubre GDPR sino que da cobertura a otras normativas y ámbitos legales'', destacaba Angulo.

Para completar el ciclo de seguridad y dar una visión más holística, esta plataforma se complementa con QRadar SIEM que avisa a Guardium si hay alguna infección para establecer las políticas de seguridad adecuadas.

# “Cómo lo hice”

El CISO de Forcepoint habla sobre la preparación a GDPR: ‘‘Hay que alinear a las partes interesadas para luego ejecutar’’, afirma.

*Fabiano Finamore,*
Country Manager, Forcepoint.

No es inusual ver al CISO, Jefe de Recursos Humanos, CIO y el Consejo Jurídico Principal reunidos en la sala del consejo. Sin embargo, no es el elenco de personajes que se esperaría para resolver un desafío relacionado con la protección de datos. Esto es lo que hace al Reglamento General de Protección de Datos (GDPR), la última ley de privacidad de datos de la UE, que sea único.

El primero de su tipo, el GDPR comprende iniciativas diseñadas para proteger los datos de los ciudadanos de la UE de una amplia gama de ‘‘delincuentes’’, desde vendedores entusiastas, hasta ciberdelincuentes sin escrúpulos.

Al final, nuestro equipo de liderazgo necesitaría alinearse con la terminología legal y de seguridad, qué significaba la ley para Forcepoint y cómo se aplicaría la tecnología de seguridad para la protección de los datos personales.

Es importante imaginar cómo una acción necesaria en un lado del negocio, podría afectar a otro.

Por ejemplo, aprendí que necesitábamos hacer una distinción clara entre la recolección de datos y la monitorización. Si vamos a hacer ciertos tipos de monitoreo, el área legal necesita estar segura de que no violará la ley, y los recursos humanos deben ser capaces de transmitirlo a los empleados en general. GDPR no proporciona una ruta prescriptiva para el cumplimiento. Una vez que tuvimos una comprensión compartida de los requisitos de la regulación y la alineación de cómo afectaría a nuestra compañía, necesitábamos encontrar las tecnologías correctas para que fuesen aplicadas. En Forcepoint, creamos un proceso de implementación de GDPR de tres pasos:

- Identificar dónde residen los datos personales y flujos
- Proteger datos personales y detectar amenazas
- Ajustar procesos

Cada compañía tendrá su propia versión de planificación sobre GDPR y experimentará problemas que podríamos haber conocido o no. Aquí es donde usted y sus colegas pueden construir sobre su base de entendimiento mutuo y trabajar a través de estos problemas a medida que surjan.

A menudo, la gente me pregunta: ‘‘¿Cómo sabes si estás alineado al cien por cien con GDPR?’’ La verdadera respuesta es que nadie puede estar completamente seguro.

Lo que sí podemos hacer es mantenernos comunicados, anticipar dónde el GDPR puede afectar al negocio, e implementar la tecnología adecuada que nos permita proteger todas las áreas de la organización, de forma proactiva, frente a los incidentes de datos de cualquier tipo.

# RSA, detección y respuesta a incidentes basada en el negocio

La historia demuestra que cualquier compañía es vulnerable y aquellas que mantengan únicamente un enfoque preventivo se verán abocadas a desaparecer. Por lo tanto, parece razonable que en 2018 las inversiones se centren, por un lado, en mejorar y aumentar las capacidades de detección y respuesta y, por otro, en la implantación de plataformas GRC. En ambas áreas, RSA tiene una propuesta de valor única en el mercado que permite abordar todas las fases de proyectos.


La detección, gestión y respuesta de incidentes es una tarea que recae en los centros de operaciones de seguridad (SoC) durante la mayor parte del tiempo. RSA Netwitness Platform es la solución orientada a los analistas que trabajan en los SoC y al responsable de seguridad. La plataforma permite, a cualquier empresa con un SoC, cubrir todo el ciclo de vida del incidente: desde la detección temprana, pasando por la fase de investigación y terminando por el cierre del incidente, reporting y la aplicación de las contramedidas. El objetivo de negocio de un SoC es que el incidente tenga el menor impacto posible en la organización y para ello los analistas deben tener capacidades de detección temprana del incidente al mismo tiempo que automatizan todas las actividades repetitivas. De esta forma, los analistas son capaces de gestionar más incidentes, aportando valor en aquellas fases en las que realmente la automatización no es válida.

Por otro lado, típicamente los SoC han trabajado con plataformas SIEM, las cuáles han cumplido su cometido de forma sobresaliente, sin embargo, en el mundo en el que vivimos no es suficiente y el resultado es que los SIEM tradicionales han pasado a tener miles de alertas sin ningún contexto de negocio. En este sentido, RSA Netwitness Platform permite obtener esta información de la plataforma de gestión de riesgos RSA Archer, la cual es líder en los cuatro cuadrantes mágicos de Gartner.

RSA Archer, además de ser la pieza que conecta el mundo técnico con el mundo del negocio, permite a este último tener una visión unificada y global de todos los riesgos de la compañía. Es capaz de cubrir todos los dominios actuales de la gestión de riesgos, siendo la cuantificación del ciber-riesgo la última novedad anunciada.

Un ejemplo de esta evolución es la empresa "Los Angeles World Airports", que gestiona el 4º aeropuerto más concurrido del mundo (2º de USA) entro otros. El programa se centró en las áreas de gestión de riesgo operacional y business resiliency bajo la plataforma RSA Archer, de tal forma que en una única plataforma tienen implementadas ambas áreas. La integración con RSA Netwitness Platform les permitió realizar una respuesta a los incidentes mucho más eficientes al mismo tiempo que mejoraban sus tiempos de respuesta.

Para más información sobre cómo lo hicieron, haz click **aquí**.

# El CIO debe dar forma a la transformación digital de las organizaciones

*Fari Ebrahimi, CIO de Akamai*

La función del CIO es crear valor empresarial a través de la tecnología. Como CIO de una empresa pionera como Akamai, quiero aprovechar la tecnología digital más reciente y revisar los procesos integrales a fin de posibilitar la transformación empresarial. Para ello tengo la gran suerte de poder contar con nuestras propias aplicaciones en el terreno del rendimiento web, distribución de contenido multimedia y la seguridad en la nube.

Nuestro objetivo principal es garantizar que la compañía ofrezca la mejor experiencia posible para sus empleados, partners y clientes. Queremos optimizar la relación con el cliente de forma integral, dando lugar a un proceso digital seguro, flexible y móvil, además de fácil de usar y disponible en cualquier lugar y en todo momento.

## Concentración de esfuerzos

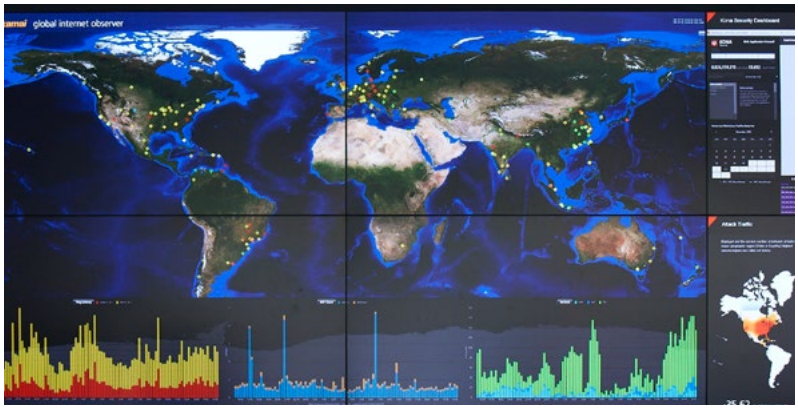
Para ofrecer las mejores experiencias digitales, seguimos perfeccionando nuestros procesos y soluciones de forma integral. Nos focalizamos en la simplificación y en aprovechar oportunidades para automatizar completamente los procesos. Lo que puede resultar todo un desafío es la alineación de la visión y el establecimiento de prioridades frente a las diversas tecnologías innovadoras que no dejan de surgir: ¿qué adoptar, qué transmitir, qué tener en cuenta para el futuro?

Buscamos nuevas oportunidades para ayudar estratégicamente a nuestros clientes. Actualmente estamos focalizados en el acceso móvil de Zero Trust a aplicaciones y por otro lado, dotamos a nuestros empleados con los conocimientos y contenidos necesarios relacionados con las tecnologías emergentes, como la inteligencia artificial (IA), para que ofrezcan la mejor experiencia al cliente.

## Nuevas tecnologías

A medida que la IA y el aprendizaje sigan desarrollándose y estableciéndose aún más en la conciencia colectiva, el impacto que ejerzan en las actividades de cualquier CIO será

mayor. Además de aligerar las rutinas de trabajo, estas tecnologías, desarrollarán asistentes digitales para apoyar el manejo de tareas complejas. El CIO debe estimular este uso de asistentes digitales para identificar las tendencias y perspectivas, garantizando una mayor eficiencia y productividad en la organización.




Esto afectará a la forma en que se trabaja, pero también cambiará radicalmente el concepto que se tiene de la experiencia global del cliente, así como su gestión. La IA forma parte de nuestra plataforma inteligente para mejorar nuestros servicios e impulsar los beneficios en nuestra oferta de seguridad. Estas tecnologías emergentes afectarán a la ciberseguridad y privacidad, ya que, al utilizar el aprendizaje automático, los departamentos de seguridad responderán con mayor rapidez y eficiencia a las ciberamenazas. Estas tecnologías seguramente produzcan importantes cambios en la forma en que las empresas evalúan y gestionan sus estrategias globales.

### Prioridad a la protección de datos

El panorama de los datos, en constante cambio, impacta en el papel del CIO respecto a la implementación de estrategias digitales, conforme más aplicaciones y servicios se alojan en la nube. Además, ahora hay más empresas que contratan a trabajadores móviles, remotos o subcontratados que necesitan un fácil acceso a los datos corporativos. Esto crea una nueva dinámica entre la seguridad de los datos y la facilidad de uso. El CIO debe garantizar que las aplicaciones y datos empresariales se protejan de forma óptima contra ataques externos sin que la seguridad suponga un obstáculo a la accesibilidad por las partes involucradas. En los próximos años, un perfecto traslado de los datos será una de las tareas básicas del CIO.

### CIO como agente del cambio

En general, el panorama empresarial está cambiando, y el CIO debe ser agente del cambio en su empresa, debemos aprovechar la tecnología digital más reciente para crear un funcionamiento seguro, eficiente y efectivo que proporcione al negocio un ahorro importante de tiempo y costes. Solo entonces aprovechará su papel decisivo y ofrecerá resultados reales.

# "Cybersecurity made simple"

Las redes actuales y las exigencias informáticas siguen haciéndose más complejas, pero la seguridad no tiene por qué serlo.


Desde la red a los endpoints y protección de servidores, nuestros productos están diseñados para eliminar las complicaciones. Sophos ofrece protección donde sea necesaria: equipos PC, portátiles, dispositivos móviles, escritorios virtuales y servidores, así como puertas de enlace de red, web o correo electrónico. La seguridad completa no se limita a detectar amenazas, sino que ayuda a gestionar todos los puntos que componen el ciclo de protección. Por eso, analistas del sector como Gartner nos consideran uno de los líderes en protección anti malware, protección de datos y de redes. Soluciones destacadas:

**Sophos Intercept X** es la protección para endpoints más completa del mundo. Combina prevención anti exploits sin firmas, aprendizaje automático para detección de malware y protección contra ransomware que permite una defensa inigualable contra las amenazas avanzadas.

**Sophos XG Firewall** es único porque permite que la función de seguridad sincronizada comparta información de seguridad con los endpoints de Sophos para identificar riesgos, mejorar la protección y responder ante incidencias. Sophos es el único proveedor que integra plenamente sus productos de firewall y endpoint para funcionar mejor de forma conjunta.

**Sophos SafeGuard** cifra contenido tan pronto como es creado. El cifrado siempre está activado, lo que permite una colaboración continua y segura. Un método de protección siempre activa que va allá donde vayan sus datos, al tiempo que ayuda en el cumplimiento del GDPR.

**Sophos Central** es la plataforma basada en la nube que permite gestionar la protección de endpoints, dispositivos móviles, cifrado, web, correo electrónico, servidores, redes inalámbricas y mucho más. Al utilizar la tecnología de administración sincronizada, se beneficia del intercambio de información de seguridad.

**Sophos PhishThreat.** Los criminales atacan constantemente a los usuarios con timos de ingeniería social, spam y suplantación de identidad. Más del 90 % de los ataques de ransomware se distribuyen a través del email. Sophos Phish Threat emula ataques de phishing para ayudarle a identificar los puntos débiles en materia de seguridad de su empresa.

**Más información**

**y descargas gratuitas:**

www.sophos.com/es-es

# La protección de las aplicaciones y los datos

La forma en que hacemos negocios está cambiando, pero ¿cómo afecta eso a la seguridad de TI? Con más nubes, más dispositivos y más aplicaciones cambiando nuestras prácticas de trabajo, es seguro decir que se trata de un mundo empresarial radicalmente cambiante.


Los riesgos de seguridad derivados de este cambio son altos y crecientes para las empresas en todas las industrias, por lo que proteger las aplicaciones y los datos es cada vez más importante.

La creciente frecuencia y el coste de los incidentes de seguridad, a pesar de la creciente proporción de presupuestos de TI que se gastan en seguridad, apunta a un defecto fundamental en los modelos de seguridad existentes que se centran únicamente en tratar las amenazas conocidas. Como indican las conclusiones del estudio realizado por IDG, esta ampliación los presupuestos en seguridad está liderada por las empresas de más de 500 empleados.

Pero también hay empresas más pequeñas que están demostrando su compromiso con la seguridad. Desde **VMware** presentamos un caso de éxito con uno de nuestros clientes: Alerce, matriz de un grupo internacional que desarrolla productos software para el sector del transporte y la logística. Alerce necesitaba unificar en una plataforma todas las herramientas para mejorar los tiempos de gestión y aprovisionamiento, pero sobre todo incrementar la seguridad de la plataforma SaaS a través de la micro-segmentación. VMware y Anadat, este último como partner integrador, plantearon la migración a una plataforma basada en la solución de virtualización de redes **NSX**.

Con NSX ya no necesitan esperar semanas para realizar las configuraciones de red, basta con tan solo unos minutos. Además, las capacidades de automatización y orquestación que ofrece la solución permiten eliminar el riesgo de errores de la configuración manual. Ahora disponen de una plataforma ágil y segura, capaz de garantizar en todo momento los requerimientos de rendimiento y disponibilidad, y totalmente integrada en su infraestructura.

# Cómo contactar y recibir asesoramiento de los expertos en seguridad

**Jose Manuel Medina**
*Director Área de Seguridad de Logicalis*

Teléfono: +34 91 766 90 69
josemanuel.medina@es.logicalis.com

**Roberto Llop**
*Regional Director RSA*

Teléfono: +34 639 201 085
roberto.llop@rsa.com

**Fabiano Finamore**
*Country Manager Forcepoint*

Teléfono: +34 661 23 37 88
ffinamore@forcepoint.com

**Jorge Muñoz**
*Sales Development Akamai*

Teléfono: +34 91 793 31 84
jmunoz@akamai.com

**Jose Manuel Delgado**
*Head of Sales Kaspersky*

Teléfono: +34 91 398 37 52
JoseManuel.Delgado@kaspersky.com


**Ricardo Maté**
*Country Manager Sophos*

Teléfono: +34 91 375 67 56
ricardo.mate@sophos.com

**VM WARE Spain S.L.**
*Rafael Botí, 26 2nd floor*
*28023 Madrid - Spain*

Tel +34 91 412 5039
madridreception@vmware.com

**Ana Alfaro**
*Directora de Marketing Citrix*

Teléfono: +34 91 414 98 00
ana.alfaro@citrix.com

**Melchor Sanz**
*Tech. Solutions Manager HP*

Teléfono: +34 91 215 29 00

## ACERCA DE
# IDG RESEARCH SERVICES

IDG Research Sevices es una plataforma inteligente de mercado que ofrece una amplia gama de servicios completos en el campo de la investigación TIC, con el objetivo de ayudar a las empresas a detectar nuevas oportunidades de negocio, conocer el grado de madurez de los clientes, y generar un pensamiento de liderazgo en su mercado.

IDG Research Services ha ayudado a los responsables de Marketing y negocio en la toma de decisiones empresariales más críticas desde el año 1987. Ofrece una visión personalizada del mercado para satisfacer las necesidades de los clientes. Con acceso directo a decisores de TI altamente cualificados, la plataforma aprovecha el potencial de las publicaciones de IDG Communications para poder llegar a las grandes audiencias de todo el mundo.

## ACERCA DE
# IDG COMMUNICATIONS

IDG Communications es la compañía de servicios de Marketing, datos y medios tecnológicos líder en el mundo con presencia en más de 147 países. IDG Communications influye en los compradores de tecnología más importantes del mundo, desde directivos y profesionales TIC, hasta usuarios domésticos de TI. A través de nuestros sitios web, eventos y publicaciones internacionales, IDG Communications proporciona los conocimientos que los compradores de tecnología necesitan para poner la tecnología a trabajar en su vida, tanto personal como profesional.

Calle Velázquez, 105 - 5ª planta - 28006 Madrid - Teléfono +34 91 349 66 00 - research@idg.es

# Estado de la seguridad en España en 2018

## Security Day: "Follow the Sun"

Calle Velázquez, 105 - 5ª planta
28006 Madrid
Teléfono +34 91 349 66 00
research@idg.es

IDG RESEARCH SERVICES

DIAMOND

LOGICALIS Business and technology working as one

RSA

FORCEPOINT

Akamai NETALLIANCE PARTNER Telefónica

GOLD

KASPERSKY lab

SOPHOS

vmware

SILVER

CITRIX

hp | intel