CincoDías

Publicación	Cinco Días General	Fecha	21/11/2019
Soporte	Prensa Escrita	País	España
Circulación	29 266	Página	1
Difusión	20 314	Tamaño	16,42 cm² (2,7%)
Audiencia	38 000	V.Publicitario	1472 EUR (1667 USD)

Desayunos **CincoDías**

El reto de impulsar la innovación sin desproteger a la empresa

—P12-13

CincoDías

Publicación	Cinco Días General	Fecha	21/11/2019
Soporte	Prensa Escrita	País	España
Circulación	29 266	Página	12
Difusión	20 314	Tamaño	508,33 cm² (83,4%)
Audiencia	38 000	V.Publicitario	8445 EUR (9564 USD)

Desayunos **CincoDías**

El desafío de proteger la empresa e impulsar la innovación

"Los responsables de ciberseguridad se enfrentan a una gran complejidad en el día a día y su figura resulta vital en el negocio de las compañías"

CARMEN DUFUR, DIRECTORA DE LA UNIDAD DE CIBERSEGURIDAD DE CAPGEMINI ESPAÑA

"Tenemos el deber de proporcionar tecnología para lanzar productos y conseguir que los clientes estén más seguros e informados"

RUBÉN RUIZ, CISO DE OPENBANK

Detrás de la seguridad de los sistemas conectados a internet en las compañías se encuentra la figura del CISO (responsable de ciberseguridad), quien, además de salvaguardar los datos, cada vez adquiere más peso en los procesos de innovación

CINCO DÍAS
MADRID

Garantizar la seguridad de todos los sistemas conectados a internet es una de las mayores preocupaciones de las empresas en el proceso de digitalización que están atravesando. Detrás de las estrategias para evitar fugas de información está la figura del CISO (*chief information security officer*), que está ganando cada vez más peso en el impulso a la innovación y transformación del modelo de negocio.

Precisamente, según un estudio elaborado recientemente por Capgemini junto a IDC, se refleja que los CISO están involucrados en el 90% de las decisiones empresariales importantes de la empresa, pero solo el 25% de los altos directivos los considera propulsores de la transformación digital.

"Ahora las compañías están en un proceso de transformación digital importante. Según el estudio, el siguiente paso es aumentar la proactividad y el liderazgo del CISO dentro de la compañía. Detectamos que la transformación está basada en cinco pilares tecnológicos; entre ellos, están entrando con fuerza el *cloud*, el *blockchain* y la inteligencia artificial. Los responsables de ciberseguridad se enfrentan a una gran complejidad en el día a día y su figura resulta vital en cuanto al negocio de las compañías". Así lo destacó Carmen Dufur, directora de la unidad de ciberseguridad de Capgemini España, en un desayuno organizado por **CincoDías** junto a Capgemini, en el que participaron Carlos Asún (CISO de la división industrial de Técnicas Reunidas), Rafael Hernández (responsable de los servicios y proyectos de seguridad y CISO de Cepsa), Rubén Ruiz (CISO de Openbank), Agustín Valencia (responsable global de ciberseguridad OT de Iberdrola), Andrés Peral (CISO de Mapfre), Virginia Rodríguez (delegada de *digital security* en Madrid de CaixaBank) y María Gutiérrez (responsable de producción de ciberseguridad de Capgemini España).

Y es que la función del CISO dentro de las compañías ha evolucionado en la última década. Además de garantizar la seguridad de la empresa y diseñar la estrategia para prevenir ataques, los profesionales de ciberseguridad participan en la generación de valor dentro del negocio de la firma.

"Para mí, el CISO tiene que entender la realidad de la organización y saber transmitir los riesgos adaptados al momento en el que se encuentra. En ese sentido, debe ser proactivo y exponer los planes de acción de forma clara. Están apareciendo nuevos actores y nuevas tácticas, y con la complejidad de los sistemas que tenemos, hay que hacer mucho trabajo de entrenamiento para entender el caso de la empresa y preparar los sistemas", señala Virginia Rodríguez.

Más allá de trabajar en la inexpugnabilidad de los sistemas digitales, los expertos coinciden en señalar que el CISO debe llegar a todos los departamentos de la empresa para potenciar la creatividad y preservando la seguridad. "El CISO tiene que saber proteger la cultura del negocio y la confidencialidad y disponibilidad de la información, además de la parte *core*. Adicionalmente a esto, tiene que saber convencer a las diferentes áreas del negocio para que lo involucren en sus proyectos y sea propulsor de cambios tecnológicos, de ciberseguridad y de innovación", apunta Carlos Asún.

En la misma línea, el CISO de Mapfre, Andrés Peral, destaca que los responsables de ciberseguridad en las compañías se están convirtiendo en asesores de la alta dirección, ya que la seguridad es una de las palancas para crear valor añadido en la estrategia de negocio. "Todas las compañías nos estamos transformando de una forma u otra y los consejeros delegados, presidentes y consejos de administración ven que la seguridad afecta a las compañías y se preguntan: ¿en qué estado se encuentra mi compañía? Ahí nace un nuevo papel, y es el de asesor de los consejos de administración y altos cargos sobre los riesgos que podemos y debemos asumir y cuáles no. En ese sentido, hacemos de habilitadores para que las nuevas tecnologías se integren en todas las áreas de la compañía con un riesgo controlado".

De pie: Virginia Rodríguez (CaixaBank), Rubén Ruiz (Openbank), Andrés Peral (Mapfre), Rafael Hernández (Cepsa), Carmen Dufur (Capgemini España) y Agustín Valencia (Iberdrola). Sentados: Carlos Asún (Técnicas Reunidas) y María Gutiérrez (Capgemini España). FOTOS: PABLO MONGE

El CISO tiene que entender la realidad de la organización y saber transmitir los riesgos

VIRGINIA RODRÍGUEZ

Tradicionalmente, el papel del CISO se basaba en analizar los proyectos en función de los posibles riesgos en la seguridad y aprobarlos o desecharlos. Su trabajo se veía como una especie de barrera, pero en los últimos tiempos esa imagen se ha derribado en favor de la proactividad. Ahora, los responsables de ciberseguridad se convierten en un apoyo de la alta dirección que impulsan los proyectos, ayudan a buscar soluciones y participan en el diseño de nuevos productos.

De hecho, según el citado estudio de Capgemini, el 75% de los líderes empresariales

CincoDías

Publicación	Cinco Días General	Fecha	21/11/2019
Soporte	Prensa Escrita	País	España
Circulación	29 266	Página	13
Difusión	20 314	Tamaño	493,05 cm² (80,9%)
Audiencia	38 000	V.Publicitario	8264 EUR (9359 USD)

"Ya no vale el concepto clásico de tener un perímetro y olvidarse del resto, hay que entender todo el proceso"

AGUSTÍN VALENCIA, RESPONSABLE GLOBAL DE CIBERSEGURIDAD OT DE IBERDROLA

"El responsable de ciberseguridad tiene que saber convencer a las diferentes áreas del negocio para que lo involucren en sus proyectos"

CARLOS ASÚN, CISO DE LA DIVISIÓN INDUSTRIAL DE TÉCNICAS REUNIDAS

"El equipo de España es referencia en ciberseguridad. Mucha gente forma parte de los comités donde se toman decisiones importantes"

MARÍA GUTIÉRREZ, RESPONSABLE DE PRODUCCIÓN DE CIBERSEGURIDAD DE CAPGEMINI ESPAÑA

"Cada organización tiene una forma distinta de describir los problemas, pero colaboramos globalmente de forma desinteresada"

RAFAEL HERNÁNDEZ, RESPONSABLE DE LOS SERVICIOS Y PROYECTOS DE SEGURIDAD Y CISO DE CEPSA

"Lo crucial es diseñar una estrategia de resiliencia bien implantada en la organización para disponer de la habilidad de actuar rápido"

ANDRÉS PERAL, CISO DE MAPFRE

"Con la complejidad de las herramientas tecnológicas, el CISO ha de ser proactivo y exponer los planes de acción de forma clara"

VIRGINIA RODRÍGUEZ, DELEGADA DE 'DIGITAL SECURITY' EN MADRID DE CAIXABANK

consultados considera que la influencia del responsable de ciberseguridad ha mejorado en los últimos tres años. "El rol del CISO había estado muy centrado en poner murallas. Se está viendo un cambio y ahora tenemos que salir fuera y no solo apoyar, sino ayudar a lanzar productos. Nosotros ayudamos a que la organización y los clientes estén seguros. Tenemos el deber de proporcionar tecnología para crear el producto. Pero también colaborar para lanzar campañas y conseguir que los clientes estén más seguros e informados", valora Rubén Ruiz.

Entre los proyectos en los que el CISO de Openbank ha participado directamente, señala la creación de una aplicación para gestionar las contraseñas digitales del cliente o en el diseño de campañas de prevención destinadas a los usuarios para evitar que sean víctimas de *phishing*.

"El acceso a la dirección es definitivo. Como estamos en multinacionales, te das cuenta de que ni las organizaciones ni las personas son las mismas en cada parte del mundo. La tecnología hay que adaptarla según el uso y costumbres. El mundo evoluciona y de pronto tenemos un esquema híbrido en el que ya no vale el concepto clásico de tener mi perímetro y olvidarse de los demás, hay que entender todo el proceso. Esto nos lleva a que estamos creando comunidades de información. Hay que añadirle un componente de dificultad del riesgo que evoluciona a una velocidad tremenda y además la legislación no suele ir a la misma velocidad", considera Agustín Valencia.

"Todos debemos ser conscientes de que parte de nuestro trabajo lo debemos hacer de forma segura. Más allá de la propia empresa también incluye a todas las partes de la cadena de valor. En ese sentido, la colaboración con proveedores es clave para mantener vías de comunicación sobre incidentes y medidas de seguridad. También con los propios clientes. Tienen que estar seguros para que no afecte al negocio. La seguridad es cosa de todos, es fundamental y vital", añade el CISO de Mapfre, Andrés Peral.

Perfiles preparados

Las compañías españolas, según apunta el panel de expertos, cuentan con grandes equipos de responsables de ciberseguridad, a pesar de que no existe una titulación específica de formación. No obstante, animan al impulso de la figura del CISO ya que, ante la carencia de titulación propia, achacan un déficit de perfiles capacitados para el puesto.

"Trabajamos a diario con gente de todas partes del mundo y el equipo de España es referencia en ciberseguridad. Eso acaba calando en el resto de la sociedad. Mucha gente forma parte de los comités donde se toman las decisiones importantes y después traslada ese conocimiento. Ahora planteamos un nuevo enfoque sobre cómo abordar el mapa de seguridad en la red y cómo garantizar que la organización está *securizada*", detalla María Gutiérrez, responsable de producción de ciberseguridad de Capgemini España.

Igualmente, Rafael Hernández apunta a que el conocimiento de los CISO se refuerza gracias a la colaboración los responsables de ciberseguridad de distintas compañías ya que está ayudando a desarrollar la profesión. "Hay muy buenos profesionales y sobradamente capacitados para dar respuesta a nivel de formación de personas. Al final, la relación entre los CISO de las compañías es de confianza. No entiendo la seguridad si no hay confianza. Nos conocemos todos desde hace mucho tiempo y compartimos muchos aspectos en materia de seguridad. Cada organización tiene una forma distinta de describir los problemas, pero colaboramos desinteresadamente de forma global.

Los clientes deben estar seguros para que no afecte al negocio, es algo fundamental

ANDRÉS PERAL

Somos bastante permeables entre nosotros a nivel personal y profesional", explica.

Prevenir los ataques

Según afirman los expertos, cada día las empresas son objeto de intentos de ataques externos. Más allá de reforzar los sistemas para que desde fuera nadie pueda acceder a información sensible, dicen que lo más importante es dotarse de una estrategia, de un modo de actuar para reaccionar rápidamente y, en caso de ser víctima de un ataque, disponer de un protocolo para solucionarlo.

"Los ataques o incidencias siempre van a existir y siempre va a haber un nivel de riesgo. Lo crucial es diseñar una estrategia de resiliencia bien implantada en la organización y perfectamente documentada para que, si en el momento en el que somos atacados no hemos podido detenerlo, al menos disponer de la habilidad para levantarnos lo más rápido posible del golpe recibido", expresa Carlos Asún.

"Al otro lado de la frontera hay gente que busca hacer el mal, que maneja más dinero y tiene mayor potencial. En 2018, el negocio de la ciberseguridad y el cibercrimen fue más rentable que el narcotráfico. Es un dato muy importante. Tenemos que ser humildes y saber en lo que trabajamos. Tenemos que tener un perfil bajo, de colaboración, asumir que somos uno más e intentar ayudar a la parte del negocio", concluye Rafael Hernández.

Mejora de la percepción del CISO

- **Aprovechar el acceso a los altos directivos.** Según los datos manejados por Capgemini, la percepción de la importancia del CISO en los procesos de creatividad e innovación de las empresas ha mejorado, pero todavía falta que adquiera relevancia. "El acceso a la dirección es definitivo. Tenemos que tener claro que en algunas empresas es posible que el acceso del CISO al comité de dirección se limite a media hora en todo el año, por lo que hay que tratar bien ese mensaje", advierte Agustín Valencia.

- **Cambio de modelo.** Debido a la transformación digital en la que se encuentran inmersas todas las compañías, los expertos que participaron en el evento apostaron por modelos de trabajo flexibles que salgan del nicho de trabajo tradicional, en el que el CISO permanecía anclado a un departamento. "Nos empodera y nos ayuda a trabajar en equipo; todos los temas son complejos y, en ese sentido, me gusta que sea colaborativo", valora Virginia Rodríguez.

- **Evaluación de ciberseguridad.** La importancia de la ciberseguridad de las compañías ha trascendido a la parte puramente del negocio y se ha convertido en uno de los elementos que tienen en cuenta las agencias de rating para conceder una calificación a la empresa. Así lo indica Andrés Peral, quien considera que "ahora hay índices de sostenibilidad que incluyen temas de ciberseguridad, como el Dow Jones, para conceder el rating a las compañías. Eso demuestra que es algo que estamos aportando al negocio y estamos siendo importantes".

- **Estigmatización del hacker.** Por otro lado, los ocho expertos inciden en la estigmatización que tienen los denominados hacker informáticos debido a que habitualmente se los relaciona con los delincuentes en la red. No obstante, señalan que en ocasiones los hacker son profesionales que tratan de dar la vuelta al sistema para intentar ver fallos, lo que en última instancia permite reforzar la seguridad. "Hay que quitar la palabra de 'hacker' como algo malo. El malo es el pirata o el delincuente informático. Hacker es el que piensa cómo el sistema puede fallar. La parte mala es hacer eso con ánimo de lucro", señala Agustín Valencia.