

CISO **EL HOMBRE QUE LO CIBERPROTEGE TODO**

¿SABES QUÉ ES UN
CISO? SE TRATA
DEL ACRÓNIMO DE
*CHIEF INFORMATION
SECURITY OFFICER*:
EL RESPONSABLE DE
CIBERSEGURIDAD DE
LA EMPRESA. UNA DE
LAS PROFESIONES
MÁS IMPORTANTES
HOY EN DÍA...



Imagina que unos ladrones intentan, a diario, a cualquier hora y centenares de veces, entrar en tu casa para robarte o atacarte. La tensión a la que estarías sometido sería máxima. Exactamente, así es la vida del director de seguridad informática -CISO, por sus siglas en inglés- de cualquier empresa. Él es el encargado de evitar que los ciber-criminales tengan éxito con los miles de ciberataques que

realizan 24 horas al día, 365 días al año. Basta con que sólo uno de ellos alcance su objetivo para hundir el prestigio de la empresa y costarle miles de millones de euros. Por eso, es uno de los perfiles más demandados y mejor valorados por las compañías, con unas retribuciones que oscilan entre los 50.000 y los 120.000 euros al año.

Bajo el acrónimo CISO, se encuentran profesionales muy variados, según el tipo de empresa a la que pertenecen, el sector en el que trabajan e, incluso, sus propios conocimientos. Hasta hace unos años su función quedaba diluida en diferentes áreas -explotación, producción, etc.-, dependiendo de la empresa. Incluso era visto como un mal menor, ya que su trabajo en pro de la seguridad suponía un retraso en el desarrollo y la comercialización del producto o servicio. Es más, aún hoy, cuando no sucede nada, su puesto es difícil de justificar, pero cuando ocurre algo... todas las miradas -y las culpas- recaen en él.

Todo ha empezado a cambiar en la última década, cuando los ciberataques protagonizan las noticias de los medios de comunicación. Unas noticias a las que hay que sumar unas normas más exigentes en materia de datos, como las de Basilea II, de 2004, que obliga a los bancos europeos a almacenarlos de forma más segura; el nuevo Reglamento General de Protección de Datos, en vigor desde 2016, pero que comenzará a ser aplicable en 2018 y que contempla multas de hasta 20 millones de euros o el 4% de la facturación global; o la directiva NIS, una norma de obligado cumplimiento que marca unas líneas genéricas en todos los países, como el deber de tener una estrategia nacional de ciberseguridad, estar equipados y preparados para dar respuesta a incidentes a gran escala o que en los colegios se curse una asignatura de ciberseguridad.

Pese a su importancia, a día de hoy, en España tan solo hay 60 CISOs profesionales que se identifican como tales, aunque muchos más ejercen bajo el nombre de ISO -así se denomina a quien está a cargo de la seguridad de la información-, CSO -el responsable de la seguridad corporativa-, BISO -encargado de la seguridad de la información de la empresa... Algo que choca con la gran cantidad de infraestructuras críticas que existen en España y que requieren de un Director de Seguridad Informática.

¿Cómo se llega a ser CISO? No existen titulaciones específicas, por lo que los ejecutivos que ostentan este cargo provienen de la ingeniería de seguridad y de perfiles de gestión empresarial, muy sensibilizados con el negocio. La pregunta que se hacen muchos es, ¿qué lugar debe ocupar en una empresa? ¿Cuál debe ser su responsabilidad frente al encargado de la seguridad física, del informático y del director general? ¿Debería estar más y mejor regulado su trabajo?



Gonzalo Asensio
MIEMBRO Y COLABORADOR DE
ISMS FORUM / CISO DE
BANKINTER @GON_AA

ASÍ ES EL CISO PERFECTO

TIENE SEIS 'SÚPER PODERES'

El 'súper CISO' es aquel que se lo pone muy, muy difícil a los cibercriminales. Para hacerles frente, necesita contar con una serie de habilidades propias de las más diversas profesiones: la precisión de un cirujano; el conocimiento legal de un abogado; los cálculos de un financiero; la destreza de un hacker... Atento a sus súper poderes.

ES UN EXCELENTE COMUNICADOR

Dentro de la compañía, el CISO se relaciona en diferentes niveles, a los que debe adaptar su discurso para hacerlo entendible. Por ejemplo, si lo hace con el Departamento de Tecnología, se dirigirá a ellos en un lenguaje técnico; mientras que si se dirige al Comité de Dirección, se centrará en los números.

TIENE CAPACIDAD DE CONVICCIÓN

Aún quedan ejecutivos que consideran que la seguridad es un 'stopper' -algo que frena la evolución de la empresa-, que no aporta valor y que supone haber caído en una paranoia. El CISO es el encargado de concienciar en materia de ciberseguridad a todos los trabajadores de una empresa, sin importar su cargo, y de convencer a los puestos directivos para invertir en ella. La clave es que nadie interprete unas buenas prácticas como un trabajo extra, sino como algo necesario para la compañía -como no dejar la puerta abierta-. Para ello, el CISO necesita empatizar y persuadir.

ES EXPERTO EN LEYES

Es uno de los aspectos más complejos para un CISO, ya que a sus conocimientos técnicos en ciberseguridad debe sumar aquellos relativos a las normativas que puedan afectar a esta faceta de la empresa. Así, debe estar al tanto de las leyes y directivas tanto estatales como europeas -o del país en el que opere o cotice-, para ajustarse a ellas y evitar a su compañía multas que, con el nuevo Reglamento General de Protección de Datos -que entra en vigor en 2018-, pueden alcanzar los 20 millones de euros.

TIENE OLFATO PARA LA GESTIÓN DEL RIESGO

Sus decisiones se apoyan, en gran parte, en su propia valoración del riesgo. Algo que no suele resultar sencillo, ya que su análisis debe acompañar al ritmo del negocio, del mercado, la cultura de la empresa, el presupuesto... y tiene que involucrar a todo el personal de la compañía, para que estén concienciados y remen en la misma dirección.

ENTIENDE EL NEGOCIO La clave es ser capaz de pedir, gastar y gestionar el presupuesto acorde al negocio. Esto exige conocimientos financieros y dominar conceptos como ROI -retorno de la inversión-, *Business Case* -documento que sirve para justificar una acción-, *Capex* -inversiones de capital que reportan un beneficio-, *Opex* -costes permanentes-, *KPIs* -métrica que sirve para identificar el rendimiento de una acción-, etc., algo útil para defender la inversión en ciberseguridad ante el Comité de Dirección.

CUENTA CON VISIÓN DE FUTURO

Es, probablemente, una de las habilidades más difíciles de conseguir. Además de identificar los problemas, debe plantear soluciones para que no lleguen a ocurrir. Para ello, lo más recomendable es definir una estrategia de seguridad a tres años donde se defina, al detalle, qué se hará, por qué y para qué durante el primer año; un 30 ó 40% de los cambios del segundo año; y las sensaciones, intuiciones y olfato para el tercero. Porque, siendo realistas, nadie sabe con absoluta certeza qué pasará dentro de tres años, pero quién se aproxime mucho... tendrá mucho de terreno ganado.

EL CISO TAMBIÉN SABE DE...

- **Seguridad en sistemas**, para ser capaz de simplificar los sistemas y programas que se usan; de esta forma se puede disponer de las mismas capacidades... pero con menos vulnerabilidades.
- **Gestión de identidades** digitales, para evitar que nadie las suplante.
- Conocimientos de **seguridad del perímetro** de la empresa y sus redes, a través de dispositivos como *Firewall* -cortafuegos-, *Sistemas de Detección de Intrusos* -IDS-, etc.
- **Seguridad en aplicaciones** que utiliza la empresa.
- **Análisis forense**, para ver qué ha pasado en un incidente y recabar pruebas.
- Conocer **cómo prevenir el fraude tecnológico** y las fugas de información.
- Saber de **seguridad en dispositivos móviles** -BYOD-, para evitar ataques a través de tablets y smartphones.
- **Seguridad en sistemas en la nube**, donde se almacena información.
- **Conocimientos de seguridad física**, ya que a través de ésta se puede evitar un ciberataque si, por ejemplo, alguien entra físicamente en la empresa para acceder a los servidores.



DÓNDE PUEDES FORMARTE PARA SER CISO

■ **Máster en Criminología y Ciberseguridad / Universidad Europea de Madrid**

917 407 272 / madrid.universidadeuropea.es
Se trata de un máster de un curso académico de duración -de octubre de 2017 a julio de 2018-, compatible con la actividad profesional. Además, incluye prácticas en empresas.

■ **Máster en Seguridad de la Información / IMF International Business School**

900 318 111 / www.imf-formacion.com
En septiembre comienza este máster a distancia, pensado para poder compatibilizarlo con la vida laboral. Cuesta 7.800 euros -con becas de hasta el 65%- y su duración va desde los seis hasta los 24 meses y está pensado para que, al finalizarlo, el alumno ya esté listo para trabajar como CISO.

■ **Máster online en Seguridad Informática / Universidad Internacional de La Rioja**

915 674 391 / unir.net
En este postgrado *online* -con exámenes presenciales-, que comienza el 26 de octubre -finaliza en junio de 2018-, se enseñan las principales técnicas de protección frente a ciberataques y amenazas.

■ **Máster universitario en Seguridad de las TIC / Universitat Oberta de Catalunya**

917 407 272 / www.uoc.edu
A partir del 20 de septiembre, el alumno estudiará vulnerabilidades, legislación y regulación, seguridad en redes, en bases de datos, análisis forense, programación de código seguro... para que, una vez finalice los estudios, sea el responsable de planear, coordinar y administrar los procesos de seguridad informática de una organización. El máster cuenta con una bolsa de trabajo exclusiva para alumnos. La matrícula ronda los 2.000 euros y hay descuentos disponibles.

■ **Certificaciones ISACA**

91 032 71 76 / isaca.org
Una alternativa a los másters son estos cursos de la asociación internacional ISACA, que certifican tu formación y conocimiento en determinados aspectos. Ofrecen cuatro diferentes, orientados a los profesionales de las Tecnologías de la Información -TI-: para los encargados de la plataforma tecnológica y sus sistemas de negocio; para los administradores de la seguridad de la información; para el gobierno empresarial de las TI; y para los que se dedican al análisis, evaluación y monitoreo de los riesgos.