La ciberseguridad, el gran reto para las compañías en la era digital

ESTRATEGIA/ El 56% de las empresas no tiene un plan definido de ciberseguridad, según un informe de Minsait. Banca, telecomunicaciones, seguros y energía son los sectores más avanzados en este sentido.

SITUACIÓN

Apenas la mitad de las empresas cuenta con un **nivel** de madurez **razonable** en materia de **ciberseguridad**. Las diferencias entre sectores son aún amplias.

Jesús de las Casas. Madrid

La pandemia ha acelerado la digitalización global, ha generalizado el teletrabajo y ha incentivado la migración de aplicaciones hacia la nube. Sin embargo, esto ha multiplicado las brechas de ciberseguridad en las empresas. Como resultado de esta mayor exposición y del incremento de las amenazas, las compañías se han visto obligadas a revisar sus estrategias de ciberseguridad. Sin embargo, muchas no han reaccionado aún a este nuevo escenario.

En concreto, el 90% de las empresas no dispone de profesionales especializados en ciberseguridad, un 82% no tiene actualizados sus registros de activos digitales a proteger, un 73% no ha implementado mecanismos de concienciación para sus empleados y apenas el 55% cuenta con un Centro de Operaciones de Ciberseguridad dirigido a detectar y responder a ciberataques. Éstas son las principales conclusiones de la presentación del tercer *Informe sobre madurez digital en ciberseguridad*, elaborado por Minsait y SIA, compañías pertenecientes a Indra.

Mauricio Skrycky

Luis Álvarez Satorre, consejero delegado de SIA durante la presentación del informe.

LUIS ÁLVAREZ SATORRE
Consejero delegado de SIA

"La mitad de las empresas da aún a la ciberseguridad un tratamiento meramente táctico"

DANIEL ZAPICO
CISO global de Globalia

"Hay que definir cuáles son los activos a proteger y las potenciales amenazas para buscar un equilibrio"

ROBERTO BARATTA
Vicepresidente ejecutivo de seguridad de Abanca

"Hay una inflación tremenda en el sector en cuanto a talento, que aún es muy joven"

SANTIAGO RODRÍGUEZ
Director Centro de Seguridad de la Información GISS

"Los ataques de 'phishing' han aumentado en gran medida con motivo de la pandemia"

CARLOS BELDARRAIN
Director de desarrollo de servicios de Minsait

"La guerra por el talento afecta a todo el ámbito de la tecnología y también la ciberseguridad"

ROSA KARIGER
CISO global de Iberdrola

"Hay que traducir en clave de negocio el conocimiento de la tecnología y sus riesgos"

CRISTINA GLEZ. PITARCH
Directora de Google Cloud Security en EMEA

"La duda no es si las empresas recibirán un ataque o no, sino cuándo va a ocurrir"

Visión estratégica

"La relevancia de la ciberseguridad está creciendo, pero aún tenemos un amplio camino por recorrer", recalcó Luis Álvarez Satorre, CEO de SIA. Los datos extraídos reflejan que en muchas organizaciones subyace una falta de visión estratégica. "La mitad de las empresas no ha incorporado aún la ciberseguridad a sus agendas y le dan un tratamiento meramente táctico", añadió. Así, se centran en la adquisición de herramientas y dejan a un lado aspectos decisivos como la cultura, los procesos y las personas.

A partir de entrevistas personales a responsables de un centenar de grandes empresas y organismos españoles y europeos, además de expertos en ciberseguridad, el estudio concluye que el 56% de las compañías carece de una estrategia de ciberseguridad bien definida y está lejos de cumplir con el modelo de Organización Digitalmente Protegida. De esta forma, su viabilidad se ve comprometida en la actual era digital.

No obstante, el informe destaca que "hay una gran divergencia en cuanto a las inversiones realizadas y el grado de madurez digital en los diferentes sectores", como puntualizó Álvarez Satorre. Las empresas del sector bancario, las telecomunicaciones, los seguros y la energía sobresalen por su alto grado de avance, inversión en nuevas tecnologías y búsqueda de respuestas innovadoras a los retos de ciberseguridad.

La escasez de talento especializado es una de las dificultades para las organizaciones, que demandan cada vez más expertos en la materia. "La guerra por el talento afecta a todo el ámbito de la tecnología y también la ciberseguridad. Apenas el 10% cuenta con los profesionales necesarios para la puesta en marcha de su protección", recalcó Carlos Beldarrain, director de desarrollo de servicios de Minsait.

Asimismo, el 68% de las compañías aún no dispone de la figura del CISO –*chief information security officer*–, como responsable ejecutivo de la seguridad de la información y de su vinculación con los objetivos de negocio. Beldarrain aseveró que "llama mucho la atención que solo el 37% de las compañías disponga de mecanismos para concienciar a sus empleados de la importancia de la ciberseguridad".

Por su parte, Luis Álvarez Satorre agregó que "apenas el 20% contempla la ciberseguridad desde el principio a la hora de lanzar un servicio nuevo, y menos del 10% la utiliza como un elemento diferencial para proteger a sus clientes". A modo de recomendaciones, el consejero delegado de SIA aconsejó que las compañías "identifiquen los riesgos, protejan sus activos críticos, detecten con celeridad cualquier amenaza, se encuentren preparadas para responder con diligencia y, posteriormente, se recuperen con el menor impacto en el negocio".

Talento

Desde el punto de vista de las empresas, "hay una inflación tremenda en el sector en cuanto a talento: es difícil conseguirlo porque es muy joven y está aún por desarrollar, y como consecuencia acabamos pagando mucho por un talento justito", explicó Roberto Baratta, vicepresidente ejecutivo de prevención de pérdida, continuidad de negocio y seguridad de Abanca. Baratta subrayó que "no sólo es responsabilidad de la administración y de las universidades desarrollar ese talento, sino también de las compañías".

Rosa Kariger, *chief information security officer global* de Iberdrola, manifestó que "necesitamos socios porque el talento es escaso. Podemos subcontratar ciertas cosas, pero es necesario contar con alguien dentro del negocio que conozca perfectamente los procesos y los riesgos y sea capaz de transmitirlo a la alta dirección". Esta combinación entre socios especializados y el conocimiento interno del negocio se traduce en una visión integral.

En la misma línea, "la clave es hacer una evaluación de los riesgos: hay que definir cuáles son los principales activos que debes proteger y cuál es el impacto de una potencial amenaza para buscar un equilibrio", coincidió Daniel Zapico, *chief information security officer global* de Globalia. Así, la figura del CISO tiene el cometido de trasladar esta visión a las altas esferas.

En cuanto al origen de los riesgos, el informe señala que el 90% de los ciberataques emplea técnicas de ingeniería social para romper las defensas de las empresas. Durante la pandemia, los ataques de *phishing* se dispararon hasta un 6.000%. "Mucha gente ha tenido que relacionarse con las administraciones por vía telemática y los *hackers* han aprovechado para hacer ingeniería social e inyectar *malware*", dijo Santiago Rodríguez, director del Centro de Seguridad de la Información GISS (Gerencia de Informática de la Seguridad Social).

Por último, Cristina González Pitarch, directora de Google Cloud Security en EMEA, advirtió que "el hecho de que las defensas de una empresa no se hayan visto comprometidas aún no demuestra necesariamente que tenga una buena seguridad". En materia de ciberseguridad, concluyó que "la duda no es si recibirás un ataque o no, sino cuándo va a ocurrir".