La ciberseguridad no es un producto, es un proceso con un coste recurrente, como la seguridad física

GIANLUCA D'ANTONIO,

Presidente de ISMS Forum

Su carrera se ha desarrollado en torno a la práctica de la ciberseguridad, en un recorrido que define como circular: empezó en consultoría, desde donde dio el salto al lado del usuario en grandes organizaciones, construyendo desde el principio la función de information security en empresas de distintos sectores, para, en la actualidad, compatibilizar la presidencia de ISMS Forum con el rol de partner en Deloitte España en la práctica de ciberseguridad.

¿Cómo surgió ISMS Forum?

En 2006, junto con otros socios fundadores, pusimos en marcha esta iniciativa. Uno de los objetivos era elevar el discurso sobre la ciberseguridad a la capa directiva y a la sociedad en general. Cuando empecé en este campo, en el año 2000, esta era una práctica eminentemente técnica, relacionada con los antivirus, los cortafuegos y poco más. Solo se hablaba de esto en foros muy técnicos y en lo que denominábamos *los calabozos de los departamentos de TI*.

> El CISO terminará saliendo del ámbito de TI, aunque hay mucha resistencia a permitir esa emancipación

Queríamos convertir la ciberseguridad en una práctica profesionalizada y con unos objetivos claros: la protección de los activos de información de las empresas, pero también del individuo y de la sociedad. Hemos evolucionado mucho en ese aspecto, pero todavía queda un camino por delante para que alcance el ámbito que le corresponde.

Otro de los objetivos era situarla en las escalas económicas o empresariales y evitar que se perciba como un área de resistencia al cambio, de control interno. Tenemos que cambiar esta percepción, que probablemente esté motivada por la forma en la que, en muchos casos, los responsables de ciberseguridad actúan. El enfoque "no se puede hacer esto" debería cambiarse por "sí, se puede hacer, pero con estos controles o con estas medidas".

Hay que situar la seguridad de la información como una función *cross*, al igual que ocurre con la tecnología. Ningún proceso de negocio puede subsistir sin tecnología; de la misma forma, no debería haber ninguno que no haya pasado a través de un análisis de los riesgos relacionados con el uso de estas tecnologías.

¿Qué os piden los CISO?

Tenemos un colectivo cada vez más numeroso de responsables de seguridad de la información; algunos son ya parte de la dirección de la empresa *(c-level)*, pero muchos de nuestros asociados están en este trámite. Quienes no tienen la visibilidad ni

el respaldo por parte de su organización nos piden, sobre todo, ayuda para construir la función dentro de la empresa y apalancarla sobre datos, informes, estadísticas, análisis…

Aquellos que ya cuentan con ese nivel de visibilidad también buscan formación, pero no solo de índole técnica. Por un lado, ya que su función debería ser transversal, necesitan entender al resto de las áreas de la empresa para ayudar en la gestión de los riesgos relacionados con el uso de las tecnologías. Además, quieren elevar el discurso, adquirir habilidades blandas —persuasión, comunicación, liderazgo, gestión de equipos y de proyectos complejos— sin olvidarse de las especificidades del rol: gestión de crisis, gestión del estrés, etc.

¿La ciberseguridad es tecnología?

Ahí hay visiones encontradas. Cada vez más, los analistas ven —a medio y largo plazo— que el responsable de ciberseguridad saldrá del ámbito de la tecnología, ya que la protección de los activos de información no tiene que ver solo con los sistemas de información. Sin embargo, en la práctica observamos que hay mucha resistencia a permitir esa emancipación.

Como asociación, la ciberseguridad es responsabilidad de toda la empresa. Aunque es el CISO quien impulsa la estrategia y lidera la función, es necesario que toda la organización se involucre y preste su apoyo, ya que el eslabón más débil suele ser cualquier usuario en su actuación cotidiana.

La previsión es que esta emancipación acabará consagrándose. Hay países en los que, en más del 50% de las organizaciones, la función de ciberseguridad todavía depende únicamente del CIO, sin embargo, en otras latitudes —y de acuerdo con las recomendaciones de los expertos— se prescribe cada vez más esta independencia de TI.

El CISO debe ser miembro de pleno derecho del comité de dirección y tener acceso a toda la capa directiva. Su presupuesto y sus recursos no pueden estar supeditados solo a la agenda tecnológica, ya que allí hay —y por eso los analistas recomiendan el cambio— conflictos en la agenda en cuanto a la priorización de las iniciativas.

¿Ayudaría el traducir a parámetros económicos lo que supone un incidente?

Estamos convencidos de ello. Ayudaría muchísimo. De hecho, una de las iniciativas que iniciamos el pasado año es un estudio econométrico sobre el coste de la *ciberinseguridad* comparándolo con el producto interior bruto del país. Está ya en su fase final de desarrollo y verá la luz en los próximos meses.

Los pocos estudios econométricos de este estilo que existen se han llevado a cabo en Alemania, Holanda, Países Bajos o Estados Unidos. A nivel macro, cada punto del PIB que se pierde —por fugas de información o robo de propiedad intelectual, por ejemplo— se puede traducir en puestos de trabajo que no se van a crear, en pérdida de competitividad con respecto a otros países…

La *security by design* no solo es lo más seguro, también es lo más eficiente desde el punto de vista económico

A nivel micro, una vez que tengamos estos datos por sectores, cada empresa podrá extrapolar su pérdida de acuerdo con su contribución al producto interior del sector.

Es cierto que hay empresas que ya hacen estos análisis econométricos, sobre todo las que han pasado por un incidente. Se suele calcular el daño

directo, que es el más evidente, pero también hay que tener en cuenta las horas perdidas por los empleados, el coste para la recuperación de los sistemas, y los efectos a medio y largo plazo relacionados con el daño reputacional, los costes legales (que se pueden dilatar), etc.

¿La respuesta es la seguridad desde el diseño?

Efectivamente, es parte de la estrategia. El Código de Buen Gobierno de la Ciberseguridad, que ha sido presentado en conjunto con el Foro Nacional de Ciberseguridad y la CNMV, establece en uno de sus trece principios la necesidad de impulsar una visión de la ciberseguridad embebida desde el principio en todos los procesos.

No es un paradigma novedoso; de hecho, se ha traspuesto de la directiva europea de Protección de Datos Personales, lo que pasa es que se suele tardar un tiempo en llevarlo a la práctica.

La única forma de enfocar la gestión de los riesgos es desde el principio: cuando una empresa hace un análisis de mercados y concluye que va a arrancar una nueva solución, un nuevo producto o servicio. Cuando empieza este análisis funcional, ya debería estar presente el punto de vista de los riesgos tecnológicos y de la ciberseguridad. No solo es lo más seguro, también es lo más eficiente desde el punto de vista económico.

Lo mismo ocurre en el *DevOps*, lo que se denomina *DevSecOps*. Es un cambio cultural que requiere tiempo. Los equipos de desarrollo tienen una tradición de *agile*: se trabaja por *sprints*, se pone en producción y es el usuario final quien lo testea, lo que supone unos riesgos enormes. Hay que cambiar el enfoque y embeber la ciberseguridad desde la fase más temprana del desarrollo.

Cuanto más conscientes se sea de esta necesidad, y a medida que la regulación haga cada vez más responsable a la alta dirección de su supervisión, esto acabará trasladándose a todos los equipos en todos los estamentos de una organización.

¿Cuál es el papel, actual y futuro, de la IA?

En ciberseguridad llevamos unos años hablando de inteligencia artificial. Las herramientas de SOAR y de XDR, de monitorización y respuesta, cada vez son más autónomas en la ejecución de casos de uso. Son capaces de detectar una amenaza y, de acuerdo con los procedimientos establecidos, tomar decisiones de forma autónoma. Esto acorta mucho los tiempos de respuesta, los lleva casi a cero, ya que un procesador puede ejecutar centenares o miles de estas operaciones de forma casi instantánea.

Desde el punto de vista de la respuesta, la inteligencia artificial alivia muchísimo lo que denominamos el *burnout* de los *security operation centers*. Además, las respuestas automatizadas, de acuerdo con un *playbook* definido, tienen un margen de error muy bajo. Se trata de tareas repetitivas o rutinarias, y ahí el elemento humano aporta poco.

En el otro lado de la barricada también se está aprovechando la IA para recopilar información de vulnerabilidades, producir código malicioso de una forma mucho más compleja, redactar correos de *phishing*… Por ejemplo, estamos observando un ataque de *phishing* basado en QR, y no sabemos si ha sido la máquina (la IA generativa) la que lo ha sugerido. Es algo nuevo que ha sido capaz de hacer un *bypass* a los sistemas actuales: al meter un código QR, el filtrado de correo no lo detecta porque el código en sí mismo no contiene ejecu-

Iniciativas de ISMS Forum

Entre las últimas iniciativas que hemos presentado me gustaría destacar:

- El Máster en Protección de Datos y Seguridad de la Información, que vamos a lanzar en colaboración con la Universidad Complutense de Madrid.
- El estudio econométrico sobre el coste de la ciberinseguridad, que presentaremos en la jornada internacional del 16 de noviembre.
- Los programas de formación y certificación diseñados para los CISO.
- El Código de Buen Gobierno de la Ciberseguridad, en el que hemos colaborado con el Departamento de Seguridad Nacional y con el Foro Nacional de Ciberseguridad.

No paramos de desarrollar iniciativas para apoyar la práctica de ciberseguridad de los profesionales y empresas que trabajan para proteger sus activos.

tables, ni enlaces… La inteligencia artificial en el lado de la empresa todavía no ha aprendido esto.
En los próximos años vamos a asistir casi a una competición entre el modo de utilizar la IA generativa para, por un lado, descubrir nuevos vectores de ataque (imaginarlos y diseñarlos) y, por otro, proporcionar la ayuda necesaria para aliviar el *burnout* en los equipos de seguridad.

¿Va a aliviar el problema del talento?
Claro. Los equipos no pueden crecer infinitamente. Además, no solo hay un problema de *recruiting*, sino también de organización. De hecho, en torno al 40% o el 60% de los niveles 1 de un SOC ya se están migrando a una respuesta basada en inteligencia artificial. Pero es que emplear a un profesional para que simplemente se dedique a mirar si un correo contiene un enlace y comprobarlo… Eso es quemarlo. Son tareas repetitivas de muy poco valor añadido. La inteligencia humana sí que es un bien escaso, y lo tenemos que aplicar allí donde más valor aporta.
Esto hay que explicarlo bien, porque muchas veces se genera la sensación de que van a sobrar personas. No es así. Hay tareas que hoy mismo no podemos llevar a cabo por falta de personal especializado. Por ejemplo, el desarrollo de la inteligencia artificial o el análisis de ciberinteligencias avanzadas, *reversing*, *forensic*… Esto, actualmente, está fuera del alcance de la IA y necesitamos personas para hacerlo.

¿Cómo se puede reducir el riesgo?
Esta es la pregunta del millón. Suelo explicar que la seguridad absoluta tiene coste infinito, y eso significa que es inasumible. Uno de los errores comunes por parte de nuestra práctica es querer tranquilizar a todo el mundo, generar una falsa expectativa de seguridad que no puede existir.
Se trata de gestionar el riesgo. Para ello, primero hay que conocerlo, entender qué puede pasar en la empresa y, entonces, diseñar una estrategia ajustada a la superficie de ataque, al tipo de negocio… Es imprescindible conocer muy bien el negocio, entender las amenazas que le pueden impactar, y, sobre esa base, diseñar una estrategia de mitigación del riesgo.
Ojo, *mitigación*. Eso significa que, de acuerdo con la dirección y con las áreas de negocio, cada uno tiene que decidir cuál es su *apetito de riesgo*, su postura de ciberseguridad. Hay que determinar hasta qué punto queremos invertir en seguridad y qué parte de riesgo decidimos —por el coste, o la probabilidad muy baja, o el impacto limitado— asumir. Esto es algo que hacen las empresas todos los días: hay riesgo financiero, de mercado, de competencia, legal… Todo el mundo acepta determinados riesgos, pero parece que el de la ciberseguridad no existe.

> **Asumir riesgos es algo que hacen las empresas todos los días, pero parece que el de la ciberseguridad no existe**

Con la experiencia se aprenden algunas reglas: el 30% de los controles de ciberseguridad, bien elegidos y priorizados, eliminan el 70% de los riesgos. A partir de aquí, cada uno elige cómo invertir en la banda superior para llegar hasta el 90% o el 95%, y aceptar ese 5% o 10%, que es algo que se asume también en el resto de los aspectos de la operativa de negocio.

¿Podrías darnos algunas recomendaciones?
Como aspectos importantes, primero, resulta clave que la dirección se involucre desde el principio. La ciberseguridad es responsabilidad de todos, no solo del CISO ni del equipo de seguridad, que son un recurso, un instrumento experto para diseñar una estrategia.
Segundo, la seguridad se consigue invirtiendo. Muchas veces se percibe la ciberseguridad como un gasto y no como lo que es: una inversión, porque ayuda a disminuir las pérdidas. Una vez que se tiene esta inversión, el siguiente paso es priorizarla de forma adecuada y, sobre todo, medir su rendimiento. Necesitamos KPI que la alta dirección pueda entender. Ahí tenemos un reto: definir indicadores alineados con la actividad de negocio; pocos, pero que utilicen parámetros tales como los ataques bloqueados, las pérdidas o los tiempos de interrupción que se han evitado en comparación con un *benchmark* del mercado, etc. Lógicamente, estos KPI deben derivar después en otros de índole técnica, que puedan ser interpretados por los equipos de TI y de seguridad.

Se trata de demostrar el valor
Esto es muy importante. En nuestros análisis de mercado estamos encontrando que la alta dirección de las empresas percibe que existe una sobreinversión en ciberseguridad. Esto probablemente se debe a un problema de comunicación. Desde hace años, la inversión media en ciberseguridad está en torno al 10% del presupuesto de TI de una compañía. Si esto no va acompañado de

La jungla digital

La tecnología es un elemento neutral. No es ni buena ni mala per se. Hay muchos ejemplos que pueden situarla a un lado u otro dependiendo de su uso. En este contexto, la ciberseguridad es un elemento clave para evitar que el concepto de *jungla digital* —donde reina la ley del más fuerte— se traslade a nuestra sociedad, cada vez más tecnológica. Para ello es necesario impulsar la práctica de la ciberseguridad y la regulación de una forma mucho más eficaz.

indicadores, de cuadros de mandos, de KPI claros y un relato entendible por la dirección, puede generar una enorme fatiga.

Hay que tener claro que la ciberseguridad no es un producto, es un proceso. Esto no es CAPEX, es OPEX: hay que mantener los sistemas todos los años, mejorarlos y, probablemente, de forma paulatina, incorporar nuevas tecnologías, como la inteligencia artificial, así como decomisar otras que ya no aportan valor. Pero esto hay que hacerlo todos los años porque estamos ante un proceso y un coste recurrentes, como la seguridad física.

Si la capa directiva percibe que hay una sobreinversión en seguridad, probablemente se deba a que no estamos siendo capaces de explicar lo que hacemos de la forma adecuada. El panorama de amenazas cambia y evoluciona continuamente aprovechando las nuevas tecnologías; esto mismo deben hacer las empresas para adecuar su seguridad a los nuevos escenarios de riesgo.

La prueba diabólica

Es lo que, en derecho, se denomina la *prueba diabólica*. Como CISO, lo estoy haciendo bien, disminuyo mi exposición a riesgos y, a diferencia de otras empresas de mi entorno, no tengo que enfrentar incidentes graves…; sin embargo, mi dirección está percibiendo que no hace falta la ciberseguridad porque no pasa nada. Por eso es tan importante que encontremos la forma de explicar que, de los millones de escaneos que cada empresa sufre a diario para buscar vulnerabilidades, no están encontrando nada en nuestra empresa y pasan a otra. Si el área de cíber no estuviera haciendo su trabajo, probablemente ya habrían entrado.

La gran pregunta no es cómo te atacarán o quién lo hará, sino cuándo sucederá. Las empresas tienen una superficie expuesta enorme y los criminales solo necesitan una pequeña brecha para entrar. Lo que sí estamos viendo es que las empresas que han invertido en resiliencia, en respuesta ante incidentes o en gestión de crisis también están expuestas a sufrir un incidente, pero son capaces de mitigar el impacto y limitarlo muchísimo, con una interrupción mínima de las operaciones y un tiempo de recuperación que se mide en días y no en semanas o meses. Estamos en tales casos ante una demostración del valor que suponen estas inversiones, y hay que dárselo a conocer a la dirección.

Las empresas que han invertido en cíber también están expuestas, pero son capaces de mitigar y limitar el impacto

Además, con la Directiva NIS2, cuando esté claramente definida la responsabilidad de los consejeros en estos escenarios, seguro que serán mucho más receptivos a estos temas.

Incentivar la inversión

Hace años, ISMS Forum presentó un Libro blanco de la ciberseguridad, donde apuntábamos la necesidad de un régimen de incentivos y no solo de sanciones, como el que establece la Ley de protección de datos. Más que estar con el bastón en la mano, si una empresa se certifica en ISO 27000, invierte en seguridad y lo puede demostrar, debería recibir un premio —incentivos fiscales, por ejemplo— con respecto a aquellas que no lo hacen.

Si la seguridad es un bien público, parte de este coste lo deberíamos sufragar los ciudadanos a través de impuestos, ya que todos nos beneficiamos.