Ciberseguridad y Auditoría Interna

Sonsoles Rubio

Presidenta del Instituto de Auditores Internos de España

IAI

auditoresinternos.es

En busca de la visión transversal

La ciberseguridad es un problema global y sistémico. El cibercrimen se ha convertido en un peligro permanente. Son numerosos los ejemplos de organizaciones —públicas o privadas, e incluso gobiernos— de todo el mundo que han sufrido robos de información, prolongadas indisponibilidades en sus sistemas, daños reputacionales o sabotajes de sus servicios online. Es importante abordar este riesgo desde diferentes departamentos, y el de auditoría interna tiene un papel fundamental.

En los últimos años los ciberataques se han multiplicado exponencialmente, alentados por la digitalización acelerada de las empresas. Ahora, a raíz de la pandemia, esa tendencia se ha acentuado aún más. Los ataques son cada vez más sofisticados y difíciles de prevenir y detectar. Se trata de un riesgo que preocupa, y mucho, tal y como pone de manifiesto el informe *Risk in Focus 2022*, elaborado por doce institutos de auditores internos europeos, incluido el de España. En este estudio se ha entrevistado a más de setecientos directores de auditoría interna, con el objetivo de conocer cuál será el mapa de riesgos de las organizaciones en un futuro cercano. Teniendo en cuenta este contexto, es importante destacar que el cibercrimen aparece, por cuarto año consecutivo, como el principal peligro al que tendrán que hacer frente las empresas europeas, no solo el próximo año, sino ya de manera permanente.

Esta posición en el *ranking* de riesgos no la determina solo el número de incidencias que se producen al año: también influye la naturaleza de las amenazas, que ha cambiado significativamente en términos de frecuencia, complejidad y objetivo. De hecho, los ataques cibernéticos son cada vez más sofisticados y dañinos. En poco tiempo, las tradicionales amenazas de seguridad —como virus, gusanos o troyanos— han evolucionado hacia ataques más complejos de denegación de servicios (DoS2), softwares maliciosos (*malware*) o las más recientes amenazas persistentes avanzadas (APT); o ataques dirigidos, que explotan diferentes tipos de vulnerabilidades —sirviéndose de técnicas como, por ejemplo, la ingeniería social—, lo que los convierte en más eficaces y dañinos.

grar. Dejando al margen el daño reputacional por la pérdida de confianza de los *stakeholders*, el mayor coste corresponde a la pérdida de negocio ocasionada por la fuga de clientes o por la propia paralización del negocio, como ocurre con los ataques de denegación de servicio (DoS) y con los de *ransomware*. A la luz de todo esto, la ciberseguridad no ha de verse como una cuestión cuya responsabilidad deba circunscribirse a los departamentos de sistemas, sino que es un aspecto cuya gestión ha de integrarse en la estrategia de la compañía. Para ello es necesario que

El papel de Auditoría Interna es clave para ayudar a identificar, evaluar y mitigar los riesgos

CAMBIO DE MENTALIDAD

Las consecuencias de estas acciones son incalculables. Un ciberataque puede tener un coste enorme para una compañía, cuya supervivencia puede llegar a peligrar. Dejando al margen el daño reputacional por la pérdida de confianza de los *stakeholders*, el mayor coste corresponde a la pérdida de negocio ocasionada por la fuga de clientes o por la propia paralización del negocio, como ocurre con los ataques de denegación de servicio (DoS) y con los de *ransomware*. A la luz de todo esto, la ciberseguridad no ha de verse como una cuestión cuya responsabilidad deba circunscribirse a los departamentos de sistemas, sino que es un aspecto cuya gestión ha de integrarse en la estrategia de la compañía. Para ello es necesario que exista un compromiso activo de la alta dirección de la empresa y una adecuada supervisión de los órganos de gobierno.

La implantación de medidas como los planes de continuidad, las pruebas de resistencia

y los ciberseguros ayuda a mitigar el riesgo, pero no lo elimina. Es necesaria una gestión proactiva de la ciberseguridad, con una identificación anticipada de los riesgos y una gestión continua de las ciberamenazas.

Aunque no es posible garantizar al cien por cien la seguridad corporativa (siempre estaremos expuestos en mayor o menor medida), sí que lo es proteger mejor nuestras organizaciones. Para ello, la anticipación es clave. Hay que ir por delante de los ataques, detectándolos y previniéndolos de forma anticipada. Además, se puede mitigar el daño si se reacciona de forma rápida y decidida ante cualquier intento de comprometer nuestro entorno.

Todo esto requiere continuidad y constancia, pero sobre todo es necesario un cambio de mentalidad. Las empresas deben efectuar un análisis detallado de la exposición a estos riesgos e implantar una estrategia de seguridad acorde a ella, así como a las necesidades, posibilidades y recursos de cada organización. El objetivo es construir un modelo de gestión de la seguridad y ciberresiliencia que, además de en las áreas clásicas de la seguridad de sistemas, tenga reflejo también en los procesos de negocio.

El área de auditoría interna debe enfocar sus esfuerzos de aseguramiento allí donde más lo necesite su organización. En las empresas menos maduras, debe concentrarse en los cimientos; es decir, en comprobar si la empresa está evaluando adecuadamente los riesgos y poniendo en práctica controles defensivos de carácter *soft* —concienciar a la organización del riesgo y las políticas correctas de uso— y *hard*. Entre estos últimos se incluye actualizar periódicamente los parches de software y configurar adecuadamente los *firewalls*, los privilegios de accesos y la autenticación mediante dos factores (2FA) para evitar que los ataques se propaguen.

Una vez afianzados los cimientos, el área de auditoría interna debe enfocarse en la capacidad de la empresa para responder y recuperarse. Si el personal no comprende bien los planes de continuidad de TI —o, peor aún, si no hay planes—, la organización está expuesta a riesgos innecesarios.

Este marco estratégico permitirá que las organizaciones comprendan el panorama de las ciberamenazas y los riesgos subyacentes, protejan los datos y activos, y estén mejor preparadas para reaccionar y responder frente a lo inesperado.

Auditoría Interna debe enfocarse en la capacidad de la empresa para responder y recuperarse

••• AUDITORÍA INTERNA Y CIBERSEGURIDAD

En este contexto, el papel del departamento de auditoría interna es clave para ayudar a identificar, evaluar y mitigar los riesgos. La ciberseguridad tiene que ser transversal a toda la organización, pues la amenaza está en constante evolución y es difícil de evaluar. Por ello, las organizaciones han de tener un adecuado marco de gobierno, con una clara asignación de roles y responsabilidades, y dotarse de medios y recursos que les permitan tanto prevenir y detectar cualquier ciberataque como reaccionar de forma inmediata ante él. Es también necesario que exista una adecuada cultura de ciberseguridad en la empresa, con programas de concienciación y formación dirigidos a toda la plantilla.

••• PUNTO DE VISTA INDEPENDIENTE

Es evidente que el riesgo para la ciberseguridad no es solo un problema de los departamentos de sistemas, sino que es de negocio. Por tanto, su gestión debe estar integrada en la estrategia de la compañía y gozar de la prioridad que su relevancia y las consecuencias —legales, financieras y reputacionales— que puede acarrear le conceden.

En este escenario, la perspectiva del área de auditoría interna nunca ha sido más necesaria. Su visión transversal del negocio y su obsesión por controlar los riesgos, contribuirá a que las empresas puedan identificar sus puntos débiles. Los consejos de administración y la alta dirección necesitan más que nunca ese punto de vista independiente. •••