Desafíos de ciberseguridad para los próximos años: una visión integral

Macarena López Medel[1]

La convergencia entre el derecho y la tecnología adquiere una relevancia creciente, dada la complejidad y evolución constante del entorno digital, así como la creciente incidencia de delitos informáticos. En este contexto, los abogados especializados en tecnología desempeñan un rol esencial para garantizar que las normativas se implementen de manera efectiva y conforme a los principios legales, al tiempo que brindan apoyo para enfrentar los desafíos cada vez más complejos que el entorno digital presenta a las empresas y organismos públicos.

En cuanto a los principales retos en ciberseguridad que se perfilan para los próximos años, la industria identifica estrategias claves para abordar las amenazas cibernéticas. Entre ellas destacan la implementación de arquitecturas *Zero Trust*, la protección de los entornos en la nube, el fortalecimiento de la resiliencia en ciberseguridad y la mejora de la ciberagilidad. No obstante, estos desafíos no solo implican la adopción de tecnologías avanzadas, sino también un cambio de mentalidad organizacional, donde la seguridad se perciba como un proceso continuo de adaptación y mejora. Así, para mitigar riesgos y garantizar la continuidad y protección de los activos digitales, resulta esencial no solo la preparación y capacidad de respuesta ante incidentes cibernéticos, sino también la resiliencia frente a los ciberataques.

Uno de los enfoques clave es la *arquitectura Zero Trust* (Confianza Cero, un nuevo paradigma de seguridad), un modelo de seguridad basado en la premisa de que no se debe confiar en ninguna entidad, independientemente de su ubicación. A diferencia de los enfoques tradicionales, *Zero Trust* asume que las amenazas pueden encontrarse en cualquier parte de la red, incluso dentro de la infraestructura corporativa. Este modelo se fundamenta en la verificación continua y el acceso mínimo. Cada solicitud de acceso debe ser rigurosamente verificada, evaluando la identidad del usuario, el contexto de la solicitud y el comportamiento del dispositivo. Asimismo, los usuarios solo pueden acceder a los recursos estrictamente necesarios para el desarrollo de sus labores, lo que limita el alcance de posibles daños en caso de un ataque.

Este enfoque resulta especialmente relevante en entornos laborales y tecnológicos distribuidos, como el trabajo remoto, que requieren cambios significativos en la infraestructura de seguridad y suponen desafíos en términos de inversión, capacitación y adaptación de los sistemas existentes.

Por otro lado, la creciente adopción de la computación en la nube ha generado nuevos retos de seguridad, como el control y la visibilidad de los datos, los riesgos derivados de configuraciones incorrectas y la protección de los datos al migrar servicios a la nube. Este proceso amplía el perímetro digital de las organizaciones, incrementando el riesgo de sufrir ciberataques. Para garantizar la seguridad en estos

[1] Gerente Legal TI, Privacidad y Ciberseguridad Falabella

entornos, las organizaciones deberán implementar estrategias de protección específicas, como la integración de herramientas de seguridad avanzadas adaptadas a la naturaleza de la nube.

Otro concepto clave es la resiliencia en ciberseguridad (prepararse para lo inesperado) que se refiere a la capacidad de las organizaciones para anticipar, resistir, recuperarse y adaptarse a los incidentes cibernéticos. Este enfoque no se limita a prevenir ataques, sino que también se centra en la rapidez y eficacia con que una organización puede recuperarse tras un ataque. Para ello, se requiere una planificación detallada, simulaciones periódicas, redundancia en los sistemas y copias de seguridad, protocolos claros de comunicación interna y externa en situaciones de crisis. Asimismo, se requiere un proceso constante de aprendizaje a partir de los incidentes y de mejora continua de los procedimientos de seguridad.

Finalmente, nos encontramos con la *ciberagilidad* que se perfila como un aspecto esencial en el futuro de la ciberseguridad. Esta capacidad de adaptación rápida a un entorno de amenazas dinámico se traduce en la habilidad de una organización para ajustar sus estrategias y medidas de seguridad en tiempo real. Los aspectos clave de la ciberagilidad incluyen monitoreo continuo, automatización de respuestas ante incidentes de seguridad para reducir los tiempos de reacción y una colaboración estrecha entre los equipos de seguridad, los abogados especializados en tecnología y los equipos de TI, fomentando una cultura de comunicación constante y trabajo conjunto.

En conclusión, en un entorno digital en rápida evolución, los próximos años exigirán un enfoque integral y proactivo para afrontar los complejos desafíos que la ciberseguridad presenta. La sinergia entre tecnología, normativas legales y capacidades organizacionales será fundamental para garantizar la protección y continuidad de los activos digitales, así como para fortalecer la confianza en el ecosistema digital global.