Una cultura de ciberseguridad

basada en la gente, creadora de valor en las organizaciones

Carlos Bermúdez
Gerente de tecnología e informática del Consejo Colombiano de Seguridad (CCS)
Ingeniero de sistemas / Magíster en Transformación Digital / Certificado en Inteligencia Artificial (AI), computación en la nube, internet de las cosas (IoT), Blockchain y Ciberseguridad / Especialista en Dirección y Gerencia de Proyectos

En la era digital las organizaciones están cada vez más expuestas a los ciberataques. Esta es una preocupación creciente para las organizaciones en todo el mundo. Incluso, debido a la alta cantidad de datos que se manejan en línea, es fundamental tomar medidas para protegerse contra este fenómeno y evitar graves consecuencias para las organizaciones.

Según el reporte 'Reforzando la Resiliencia en Ciberseguridad' publicado recientemente por WTW Latam, hoy los ciberataques figuran como el riesgo más relevante, con pérdidas que podrían alcanzar a nivel global los 24 billones de dólares a 2027, lo que equivale al Producto Interno Bruto (PIB) de todo Estados Unidos (citado por La República, 2023).

De hecho, el Informe de Brecha de Habilidades de Ciberseguridad de 2022 realizado por Fortinet señaló que, tan solo en Latinoamérica, el 87 % de las empresas consultadas en esta región sufrió brechas de ciberseguridad en el periodo analizado (2022) y en el 63 % de los casos, las compañías sufrieron afectaciones económicas iguales o superiores al millón de dólares (Infobae, 2022).

Pero ¿qué son los ciberataques?

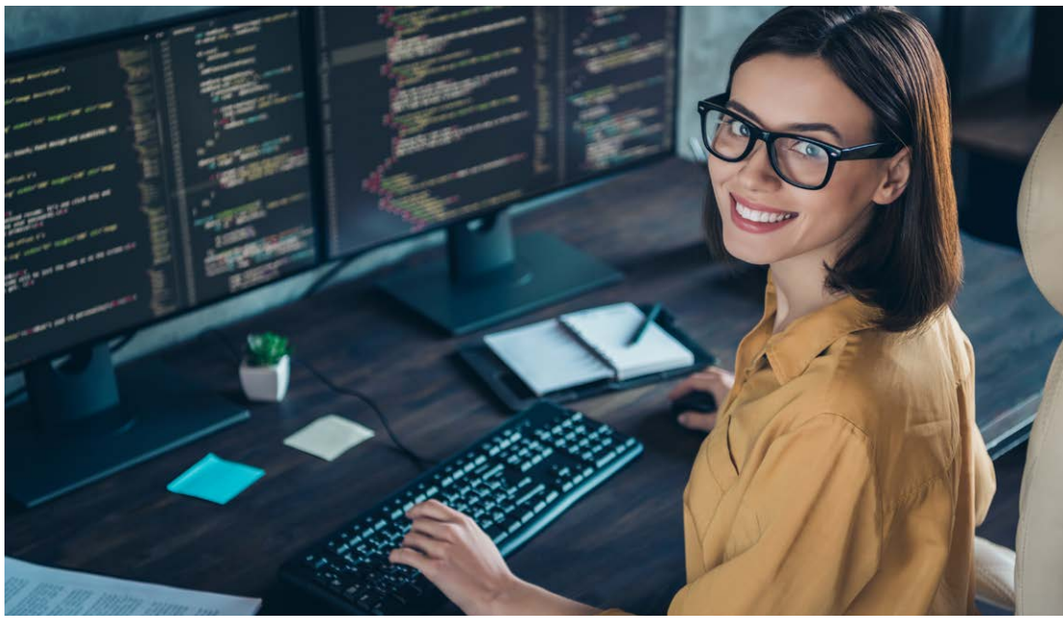
Se trata de ataques informáticos dirigidos a un sistema o red con el objetivo de dañarlo, robar información o interrumpir su funcionamiento. Los ciberataques pueden ser llevados a cabo por individuos, organizaciones delictivas o, incluso, por gobiernos. Las motivaciones pueden variar y se pueden clasificar en tres categorías principales: delictivas, políticas y personales.

Los atacantes con motivos delictivos buscan ganancias financieras a través del robo de dinero, la apropiación de datos o la interrupción del negocio. De igual manera, personas con motivaciones personales, como empleados actuales o antiguos colaboradores insatisfechos, pueden buscar acceder a información confidencial o perturbar el funcionamiento de una empresa. No obstante, su principal objetivo suele ser la obtención de compensaciones económicas. Entre tanto, los atacantes con motivaciones sociopolíticas buscan llamar la atención de sus causas.

De acuerdo con el informe de WTW, los ataques cibernéticos más frecuentes son el secuestro de datos *(ransomware),* acceso al servidor, correos maliciosos *(phishing),* robo de datos y recolección de credenciales (La República, 2023).

La ciberseguridad, por su parte, es la disciplina que se encarga de proteger los sistemas, redes, datos y aplicaciones de las organizaciones frente a los ataques cibernéticos. Por eso, resulta cada vez más importante en el contexto organizacional, ya que entidades, empresas e industrias de cualquier naturaleza, tamaño o sector dependen cada vez más de la tecnología para su funcionamiento. De esta manera, la ciberseguridad desempeña un papel fundamental en la preservación del valor y la continuidad de los negocios al salvaguardar los datos, que representan uno de los activos más preciados para las organizaciones. Esto contribuye a prevenir posibles pérdidas financieras, daños a la reputación e, incluso, la interrupción del negocio.

La ciberseguridad desempeña un papel crucial al resguardar la privacidad de clientes y empleados, lo cual contribuye a mantener y fortalecer la confianza en el negocio, generando beneficios tanto para la empresa como para sus partes interesadas.



Al prevenir posibles ataques cibernéticos y la consiguiente pérdida de datos confidenciales o información altamente sensible, la ciberseguridad contribuye a mantener la integridad de la empresa, protege frente a posibles demandas y litigios por fugas de datos y ayuda a proteger su posición en el mercado.

Otra de sus funciones importantes consiste en proteger la reputación de las organizaciones. La gestión efectiva de amenazas cibernéticas y la prevención de violaciones de seguridad ayudan a evitar incidentes que podrían dañar la imagen y la percepción pública de la empresa. Mantener una sólida reputación es esencial para atraer a clientes, inversionistas y socios comerciales y contribuye significativamente al éxito a largo plazo de la organización.

Por último, la ciberseguridad desempeña un papel esencial al salvaguardar las operaciones de las organizaciones frente a los ataques cibernéticos, lo que, a su vez, garantiza la continuidad del negocio. Esto asegura que la empresa pueda mantenerse en funcionamiento sin interrupciones significativas y, por lo tanto, sostener su capacidad de servir a sus clientes y cumplir sus compromisos comerciales.

Las organizaciones deben desarrollar políticas y procedimientos claros y concisos que sean fáciles de entender y seguir. Este tipo de lineamientos son necesarios para establecer normas y directrices, especialmente, en materia de ciberseguridad.

Además, la tecnología puede ayudar a las organizaciones a proteger su información y sus sistemas. Por ende, se deben implementar soluciones de ciberseguridad acordes al contexto, las necesidades y particularidades de cada empresa, institución o entidad. No obstante, a pesar de la disponibilidad de diversas soluciones tecnológicas en el mercado, junto con las considerables inversiones económicas que las organizaciones realizan, los ciberataques continúan siendo efectivos y comprometen la seguridad.

¿Cuál es la razón detrás de esta vulnerabilidad persistente?

La respuesta es más sencilla de lo que parece y compromete dos factores. El primero tiene que ver con las amenazas internas, las cuales son generadas por usuarios que tienen acceso autorizado y legítimo a los activos de una organización y abusan de ellos de forma deliberada o accidental. Este factor es el que, en la mayoría de los casos, genera vulnerabilidades frente a los ataques o permite el ingreso del

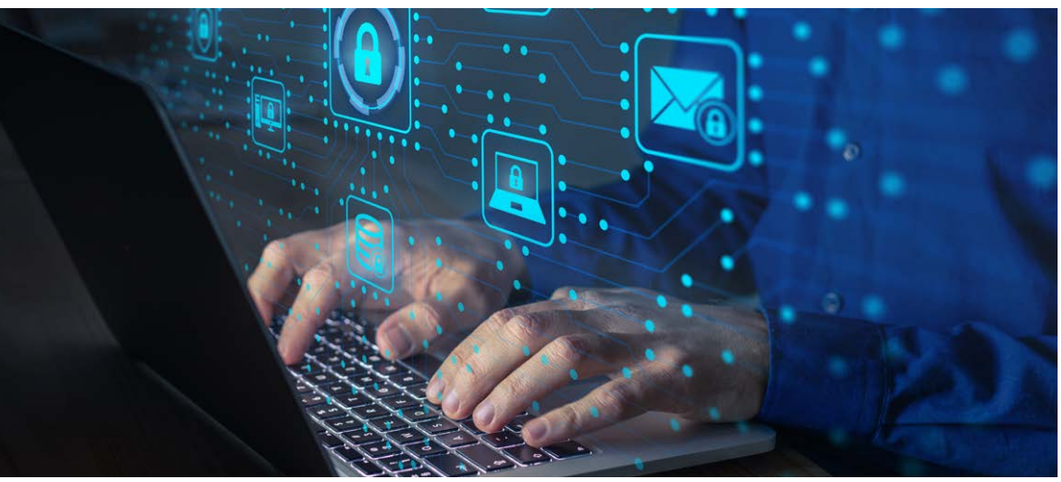
intruso a la organización. En otras palabras, todos y cada uno de los empleados y colaboradores de una organización son potencialmente atacantes o simplemente agentes portadores de la llave que da acceso a los atacantes. A este fenómeno se le conoce como "el eslabón débil de la cadena". Por consiguiente, es necesario fomentar un entorno en el que los trabajadores obtengan el conocimiento y la intuición para convertirse en la primera línea de defensa.

Una buena práctica en este ámbito es crear un programa integral de concientización en ciberseguridad dirigido a todos los empleados, independientemente de su nivel o función en la organización. Este programa puede incluir pruebas de conocimiento y herramientas de referencia fáciles de usar como guías, listas de verificación y recursos en línea que puedan ser consultados en busca de orientación sobre prácticas de seguridad. También se pueden implementar programas de reconocimientos especiales para aquellos empleados que demuestren un compromiso sobresaliente con la ciberseguridad.

El segundo factor se relaciona con la falta de adopción de una cultura organizacional de ciberseguridad que, además, debe estar centrada en las personas, criterio que puede aportar un mayor valor a las organizaciones. Para ello, es importante implementar estrategias con enfoque en la gente que tengan en cuenta su nivel de formación, responsabilidades, factores de riesgo, entre otras características.

Así mismo, resulta esencial que los trabajadores aprendan a comprender los riesgos cibernéticos de la mano de una alta dosis de comunicación, pedagogía y sensibilización frente a las medidas que pueden tomar para protegerse. Se recomienda hacer talleres y eventos de formación continua con los trabajadores, donde se puedan dar recomendaciones y políticas de uso de dispositivos personales en la red de la organización; también se pueden hacer simulaciones de ataques de *phishing* para evaluar la capacidad de los empleados para identificar correos electrónicos maliciosos. Esto les ayudará a desarrollar habilidades de detección de amenazas.

Una cultura de ciberseguridad basada en las personas ayuda a los empleados a identificar y reportar amenazas, lo que contribuye a reducir el riesgo de ataques. Por ende, es crucial invertir en comprender en profundidad los riesgos a los que se encuentran expuestos los datos y qué acciones o comportamientos realizan los usuarios de los sistemas, aplicaciones, redes y demás componentes tecnológicos de las organizaciones que generen la vulnerabilidad. La ciberseguridad debe ser una prioridad para toda la organización, no solo para el área de IT. Los directivos deben ponerse el sombrero de la prevención cibernética y transmitirlo a todos los equipos de trabajo, involucrando todos los niveles de la organización y permitiéndoles aportar sus ideas y recomendaciones.



Es importante tomar acciones de manera proactiva, oportuna y preventiva y no esperar a que las organizaciones sean noticia en las redes sociales o en los medios masivos por cuenta de un ataque cibernético. Los directivos, los mandos medios y, en general, todos los trabajadores deben abrazar una cultura de ciberseguridad sin prejuicios y sin miedo al cambio. Incluso, por qué no, permitirse desarrollar la ciberseguridad con un enfoque didáctico donde los empleados participen en actividades relacionadas con este tema a través de concursos y programas de incentivos. En lugar de castigar a aquellos que no sigan las políticas de seguridad informática, se debería recompensar a quienes sí las cumplan. Esto facilitará la comprensión, la adopción y la incorporación cotidiana de todos los aspectos relacionados este tema tan crítico.

Por último, pero ciertamente no menos importante, es esencial comprender que una vez que esta cultura se ha implementado, no se puede abandonar ni menospreciar. Más bien, debe convertirse en un proceso continuo y no limitarse a una iniciativa única. La ciberseguridad debe ser un compromiso constante que evolucione y se adapte a medida que cambian las amenazas y emergen nuevas tecnologías, manteniendo así la integridad de la organización a lo largo del tiempo.

Referencias

La República. (2023). Las pérdidas globales por ciberataques representarían hasta US$24 billones en 2027. *https://www.larepublica.co/globoeconomia/las-perdidas-globales-por-ciberataques-representarian-hasta-us-24-billones-en-2027-3723386*

Infobae. (2022). El 87 % de las empresas latinoamericanas fueron víctimas de ciberataques en el último año. *https://www.infobae.com/america/tecno/2022/04/29/el-87-de-las-empresas-latinoamericanas-fueron-victimas-de-ciberataques-en-el-ultimo-ano/*