Redefiniendo la estrategia para hacer frente a los ciberataques

A medida que las amenazas se vuelven más interconectadas, los incidentes se vuelven más costosos y más frecuentes.

Febrero, 2024

www.pwc.com/ve

Las compañías reportan incidentes que son cada vez más costosos

A medida que las amenazas se vuelven más interconectadas, los incidentes se vuelven más costosos y más frecuentes. A nivel global, de acuerdo a la 27° Encuesta Global Anual de PwC realizada a los CEO, los encuestados en Venezuela manifestaron que el cuarto mayor riesgo al que deberán hacer frente en los próximos 12 meses, es el de ciberseguridad (tercero a nivel global).

Nuestra encuesta también revela que para el 59% de las organizaciones en el país, los cambios tecnológicos impulsarán una transformación en la forma como el negocio crea, entrega y captura valor en los próximos tres (3) años.

Figura N° 1: Principales preocupaciones de los CEO en Venezuela

Las principales infracciones cibernéticas, (aquellas que le costaron a la empresa víctima más de 1 millón de dólares), aumentaron en un tercio durante el año pasado, según los hallazgos de la última encuesta Global Digital Trust Insights de PwC. Si bien no existen estadísticas precisas que aborden la situación actual de nuestro país en esta materia, los más recientes hechos noticiosos dan cuenta de que nos enfrentamos a un enemigo silencioso pero altamente dañino, y en constante crecimiento, capaz de afectar las principales operaciones del negoció, así como extorsionar por altas sumas de dinero a cambio de devolver el control de los principales datos de la organización.

Un factor detrás de esta tendencia es la creciente interconexión de los riesgos cibernéticos y su inadecuada gestión dentro de la organización. Lo que podría comenzar como un único incidente aislado, puede evolucionar rápidamente hacia una infiltración persistente y multifacética, en la que intrusos trabajan desde dentro de los sistemas de la empresa para extraer datos y filtrarlos, por ejemplo, o lanzar un ataque de ransomware.

En Venezuela, hay que considerar además, que buena parte de las infraestructuras tecnológicas han llegado a niveles de obsolescencia altos, y los años de desinversión en actualizaciones tecnológicas necesarias agregan nuevas brechas de seguridad que pueden ser aprovechadas por ciberatacantes.

Sin la adopción de un modelo de gestión de riesgos de ciberseguridad, resulta difícil responder a estas crecientes amenazas, lo cual podría producir, entre otros, los siguientes riesgos al negocio:

- Afectación directa o indirecta a la integridad, disponibilidad y/o confidencialidad de los datos de la organización.
- Modificación no autorizada de registros de información transaccional del negocio, como por ejemplo, el maestro de proveedores, lo cual puede derivar en la ejecución de operaciones irregulares que beneficien a los ciberatacantes.
- Ejecución de pagos o transferencias solicitados por terceros maliciosos, que aprovechan las debilidades de ciberseguridad o la falta de concientización en la materia por parte del personal de la organización.
- Indisponibilidad de las operaciones regulares de la organización, mediante la afectación directa o indirecta de los servicios críticos, o el secuestro de datos vitales para la operación del negocio.
- Daño permanente a la reputación del negocio.

El ransomware causa estragos en la operaciones del negocio

De acuerdo a los resultados de la encuesta Global Digital Trust Insights de PwC a nivel global, el 29% de las organizaciones les preocupa que su empresa se vea afectada por un evento de Ransomware en los próximos 12 meses. Si vemos el resultado de la región, nos encontramos que en latinoamérica este número se incrementa a 33% de las organizaciones.

Si analizamos la incidencia de ransomware en algunos sectores de la economía, se observa que para el sector financiero la preocupación se eleva al 44% de las organizaciones, 30% sector de tecnología, medios y telecomunicaciones, 29% retail y consumo, 27% el sector salud, y 24% el sector de industria y manufactura.

Las noticias en Venezuela dan cuenta de empresas que han sido afectadas por este tipo de amenazas en el último año, lo cual deja en evidencia la posibilidad de ver comprometidas las operaciones de la organización, con todas las consecuencias que esto trae consigo, como el daño a la reputación y las pérdidas financieras.

Por otro lado, los rescates y extorsiones reclamadas por los grupos de cibercriminales responsables de estos ataques superaron recientemente las seis cifras en los principales casos que se han hecho públicos.

En este sentido, la encuesta Global Digital Trust Insights de PwC da cuenta de la preocupación de los ejecutivos en Latinoamérica sobre las consecuencias de un incidente de ciberseguridad:

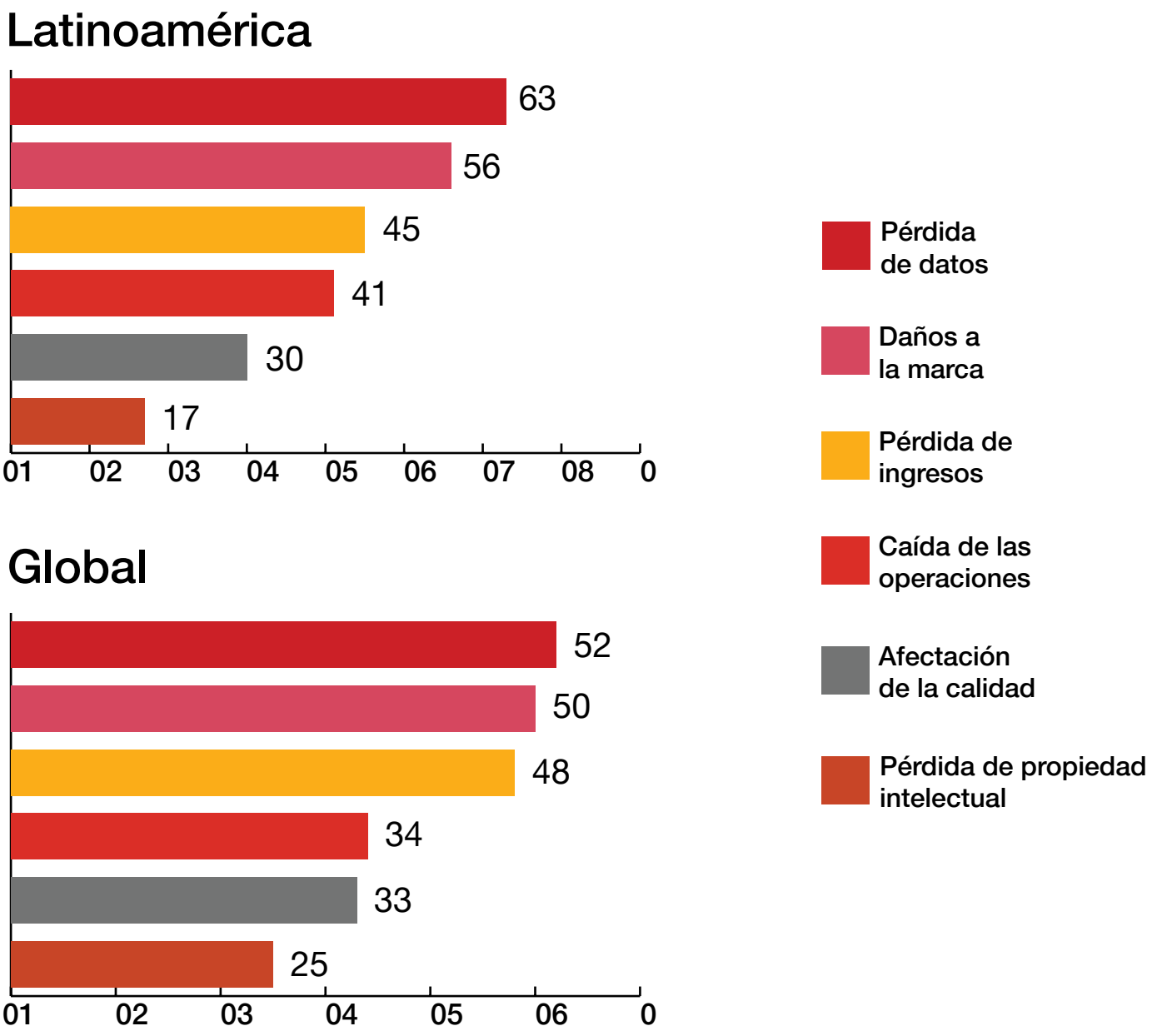


Figura N° 2: Preocupación de los ejecutivos en Latinoamérica sobre las consecuencias de un incidente de ciberseguridad

Dando respuesta a las ciber-amenazas

El liderazgo de la organización debe responder a estas crecientes amenazas con imaginación y con la determinación de romper los silos, haciendo uso de las buenas prácticas de gestión en materia de ciberseguridad. No se trata solo de “gastar” más en tecnología de protección, sino de hacer los ajustes necesarios para generar un ambiente de control, lo suficientemente robusto, que permita gestionar los riesgos hasta un nivel aceptable por la gerencia. En este sentido, desde PwC Venezuela podemos apoyar a su organización a hacer frente a los ciber-riesgos, considerando:

- Nuevas formas de gestionar el riesgo cibernético: mediante el uso de enfoques más sofisticados para el modelado de los riesgos cibernéticos, como el diagnóstico del nivel de madurez de la organización en materia de ciberseguridad, la preparación para hacer frente a ataques tipo ransomware, y la identificación de amenazas específicas para el sector, la visión y la estrategia de su empresa.

- Diseño del gobierno de ciberseguridad: Implementamos modelos de gobierno en materia de seguridad de la información y ciberseguridad, alineados con estándares internacionales que rigen la materia, como lo son la serie ISO 27000 y el marco de trabajo de ciberseguridad de Instituto Nacional de Estándares de Tecnología de Estados Unidos (NIST CSF por sus siglas en inglés).

- Uso de la tecnología para liberar a sus equipos de trabajo: liberamos a sus colaboradores de tareas tediosas que pueden ser gestionadas mediante el uso de tecnología y monitoreadas mediante un servicio gestionado de Inteligencia de Amenazas, que puede brindarle a su gente el tiempo y el espacio necesario para enfocarse en el día a día de su negocio y para reflexionar sobre nuevas formas de frustrar las amenazas cibernéticas.

- Dar la bienvenida a “Cyber” a la sala de juntas: hacemos que los riesgos y controles cibernéticos sean un tema básico en la sala de juntas, ayudando a que la función a cargo de los temas de ciberseguridad tenga voz sobre cómo la ciberseguridad encaja en las principales iniciativas estratégicas y cómo promueve el crecimiento del negocio.

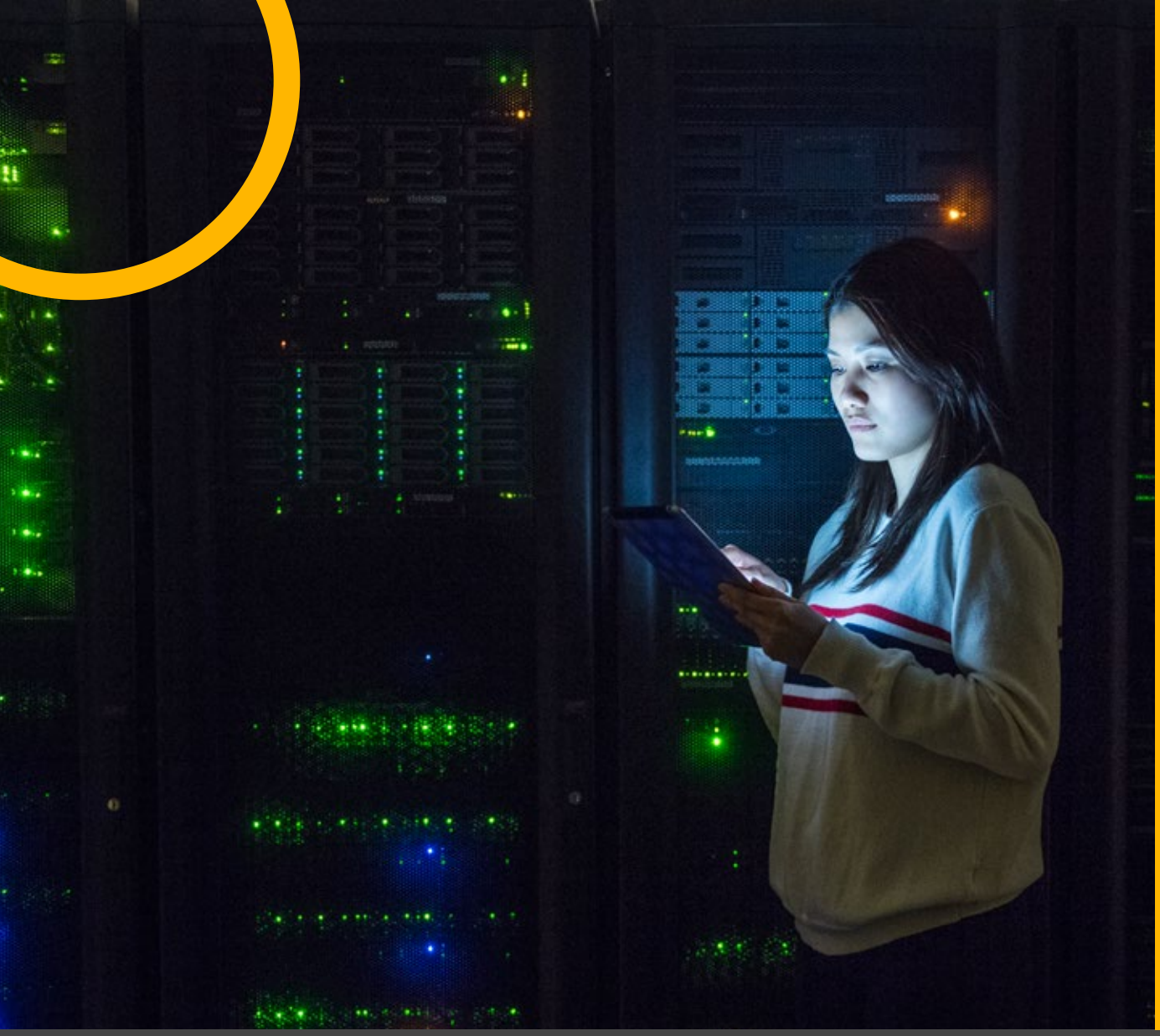
- Enmarcar la ciberseguridad como algo más que defensivo: proteger a la empresa contra amenazas (a los registros financieros, a la propiedad intelectual, a los datos de los clientes, a la marca misma) es más que jugar a la defensiva. Las innovaciones generadas por estos esfuerzos pueden ahorrar dinero y ayudar a que el negocio crezca. Describir la ciberseguridad como un esfuerzo que abarca a todo el negocio es una parte central del trabajo de la función de ciberseguridad hoy en día.

- Enseñar un nuevo idioma: hacemos de la ciberseguridad parte de los temas de conversación con los clientes, inversores y socios comerciales, de manera que estos también puedan informar de situaciones que pongan en riesgo a la organización e interactúen con los esquemas de protección. Utilizar vocabularios comunes puede ayudar a derribar las barreras de comunicación entre distintos grupos para hacer que un mensaje de concientización y protección sea eficaz .

- Capacitar y concientizar: diseñamos programas de concientización en materia de ciberseguridad para todos los colaboradores, estableciendo métricas que permitan medir la efectividad del programa.

En PwC Venezuela contamos con la capacidad y la experiencia para acompañarlos a lo largo del ciclo de vida de los incidentes de ciberseguridad. Desde la preparación de los cimientos y esquemas de gobierno y respuesta a situaciones que atenten contra la seguridad de la información, hasta el acompañamiento durante y después de los posibles incidentes que se puedan presentar.

Si desea obtener mayor información sobre este u otros temas relacionados, no dude en contactarnos



Contactos para servicios de ciberseguridad, privacidad y tecnología:

Edwin Orrico - Socio
Cybersecurity, Privacy & Forensics
edwin.orrico@pwc.com

Javier Rojas - Gerente
Cybersecurity, Privacy & Forensics
javier.rojas.r@pwc.com

www.pwc.com/ve

PwC Venezuela @pwcvenezuela @PwC_Venezuela PwC Venezuela