ES DIFÍCIL ABANDONAR LOS VIEJOS HÁBITOS:

cómo los desafíos de personas, procesos y tecnología afectan a los equipos de ciberseguridad en México

UN DOCUMENTO TÉCNICO DE TENABLE ELABORADO CON BASE EN UN ESTUDIO COMISIONADO DE 825 PROFESIONALES DE TI Y CIBERSEGURIDAD, INCLUYENDO 101 ENCUESTADOS MEXICANOS, QUE FORRESTER CONSULTING REALIZÓ EN 2023

Índice

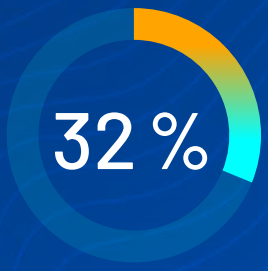
Introducción

Para reducir el riesgo cibernético, las organizaciones de todas partes del mundo se ven limitadas por problemas relacionados con las personas, los procesos y la tecnología. En conjunto, estos desafíos hacen que sea sumamente difícil para las organizaciones poner en práctica la ciberseguridad preventiva de manera eficaz, incluso a medida que la superficie de ataque se vuelve cada vez más compleja. Para colocar parches proactivos a las vulnerabilidades del software, muchas organizaciones siguen teniendo problemas con los aspectos básicos. Abordar de forma preventiva los errores de configuración del sistema también sigue suponiendo un desafío. Para complicar aún más las cosas, las organizaciones se enfrentan al desafío de obtener un panorama preciso de su superficie de ataque, incluyendo visibilidad hacia activos desconocidos, recursos en la nube, debilidades de código y sistemas de derechos de usuarios.

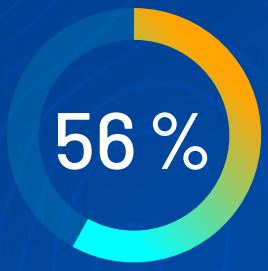
Cualquiera de las áreas de exposición mencionadas anteriormente representa múltiples posibles vías que un atacante puede explotar para poner en riesgo una organización. En un estudio comisionado de 825 líderes de ciberseguridad y TI que realizó Forrester Consulting en nombre de Tenable en 2023, incluyendo 101 encuestados mexicanos, nos propusimos comprender cómo los siguientes desafíos relacionados con personas, procesos y tecnología que enfrentan los equipos modernos de ciberseguridad y TI se interponen en el camino de las prácticas eficaces de reducción de riesgos:

DESAFÍOS RELACIONADOS CON LAS PERSONAS

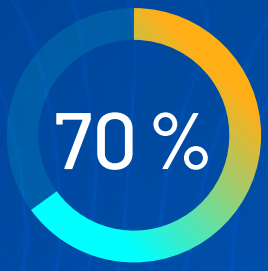
Los equipos de ciberseguridad y TI frecuentemente se encuentran aislados en silos y su desempeño se evalúa mediante criterios y objetivos separados y contradictorios. Las actitudes internas hacen que la coordinación entre los equipos de TI y de seguridad sea difícil y requiera mucho tiempo.



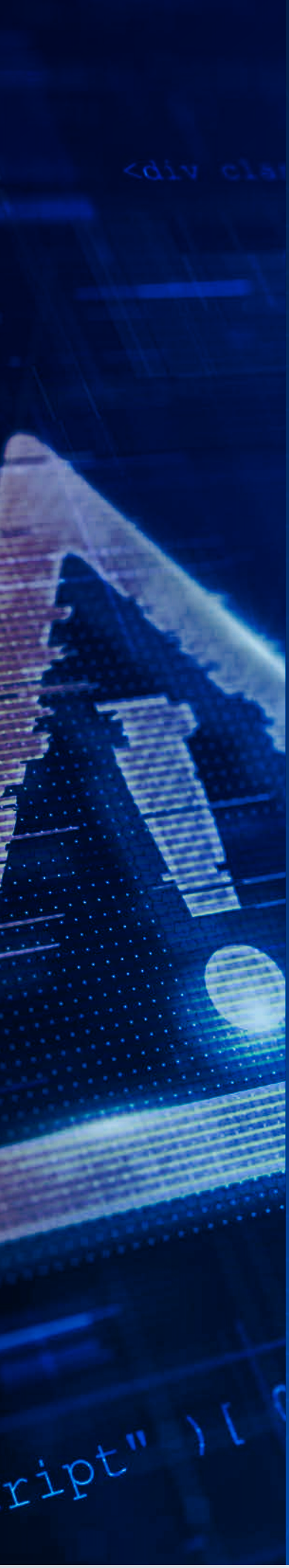
El 32 % considera que la coordinación entre los equipos de TI y de ciberseguridad es difícil y requiere mucho tiempo.



Casi seis de cada 10 encuestados (56 %) afirman que el equipo de ciberseguridad está demasiado ocupado luchando contra incidentes críticos para adoptar un abordaje preventivo con el fin de reducir la exposición de su organización.

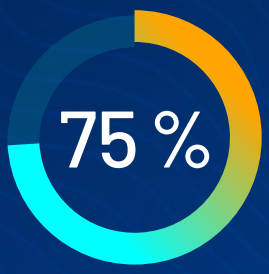


Más de dos tercios (70 %) afirman que el área de TI está más preocupada por el tiempo de actividad que por la colocación de parches o la corrección.



DESAFÍOS RELACIONADOS CON LAS PERSONAS (CONTINUACIÓN)

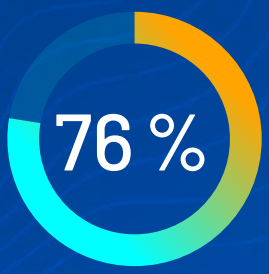
Se necesitan recursos humanos considerables para gestionar las numerosas herramientas que se necesitan para practicar la ciberseguridad preventiva y para crear informes de riesgos útiles a partir de estas fuentes de datos dispares.



Tres de cada cuatro encuestados (75 %) tienen 25 o más empleados destinados a la implementación, el soporte, el mantenimiento y/o las relaciones con los proveedores de las herramientas de ciberseguridad preventiva que utilizan.

En promedio, las organizaciones dedican 16 horas al mes a elaborar informes de seguridad para los líderes de negocios.

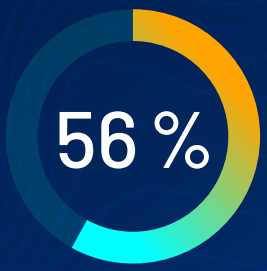
En los dos últimos años, observamos que la organización promedio estaba preparada para defenderse de forma preventiva del 57 % de los ataques cibernéticos que sufría. Sin embargo, tener únicamente esta cobertura las hace vulnerables al 43 % de estos ataques, que tuvieron que mitigar de forma reactiva en lugar de detenerlos por completo.



Tres de cada cuatro encuestados (76 %) consideran que su organización tendría más éxito en la defensa contra los ataques cibernéticos si dedicara más recursos a la ciberseguridad preventiva.

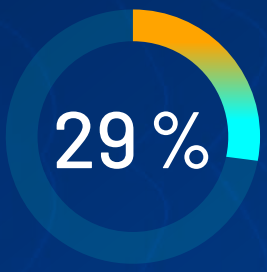
DESAFÍOS RELACIONADOS CON LOS PROCESOS

Los atacantes evalúan constantemente los entornos, pero, en la mayoría de las organizaciones, las reuniones sobre los sistemas críticos para el negocio se celebran una vez al mes (¡en el mejor de los casos!).

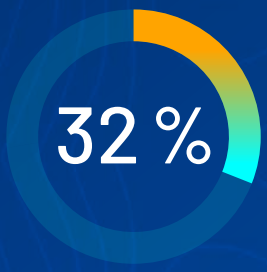


En la mayoría de las organizaciones (56 %), los líderes de TI y seguridad se reúnen cada mes con los líderes de negocios para debatir qué sistemas son críticos para el negocio. Más del 29 % de las organizaciones solo se reúnen una vez al año (o menos). Teniendo en cuenta que los atacantes evalúan constantemente el entorno, creemos que es fundamental mantener reuniones y comunicaciones más frecuentes sobre la criticidad de los sistemas para el negocio a fin de reducir el riesgo.

Los intereses de negocio en conflicto frecuentemente implican que la ciberseguridad no se consulta con la suficiente antelación - si es que se la consulta - en la implementación de los servicios en la nube.

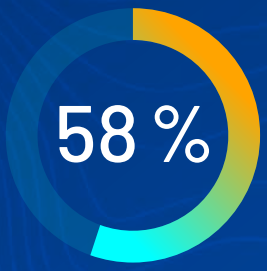


Casi un tercio de los encuestados (29 %) afirma que no se consulta al equipo de ciberseguridad con suficiente anticipación en el proceso de elección e implementación de servicios en la nube.



El 32 % señala que sus equipos de negocios e ingeniería compran e implementan servicios en la nube sin informar al equipo de ciberseguridad.

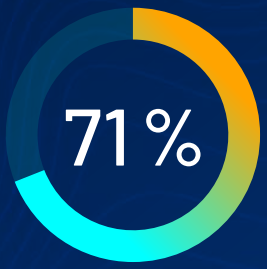
Los problemas de higiene de los datos impiden una priorización eficaz.



Casi seis de cada 10 encuestados (58 %) señalan que la falta de higiene de los datos les impide extraer datos de calidad de los sistemas de gestión de privilegios y accesos de los usuarios, así como también de los sistemas de gestión de vulnerabilidades. La ciberseguridad preventiva requiere la capacidad de evaluar las vulnerabilidades en contexto con los datos de los usuarios, para que los empleados de TI y ciberseguridad puedan tomar las decisiones de priorización adecuadas sobre qué sistemas o clases de usuarios y activos corregir primero.

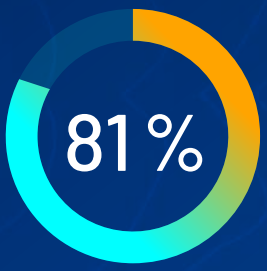
DESAFÍOS RELACIONADOS CON LA TECNOLOGÍA

Una mezcolanza de herramientas de ciberseguridad preventiva hace que sea difícil para los líderes de ciberseguridad y TI obtener información significativa sobre la profundidad y la amplitud de su exposición.

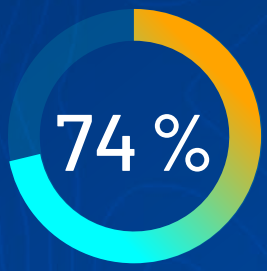


Casi tres cuartas partes de los encuestados (71 %) utilizaron 10 o más herramientas de ciberseguridad preventiva en los últimos 12 a 24 meses.

Los profesionales que utilizan herramientas aisladas en silos no pueden determinar las relaciones entre usuarios, sistemas y software, y las distintas métricas de medición entre todas las herramientas dificultan la evaluación precisa del riesgo.

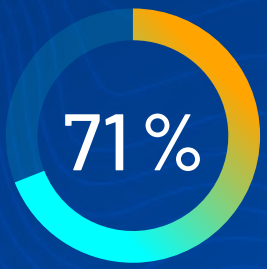


Si bien la mayoría de los encuestados (81 %) afirma tener en cuenta la identidad del usuario y los privilegios de acceso al priorizar las vulnerabilidades para su corrección, más de la mitad señala que su organización carece de una forma eficaz de integrar dichos datos en sus prácticas preventivas de ciberseguridad y gestión de exposición.



Casi tres de cada cuatro encuestados (74 %) aseguran que sus sistemas aislados en silos constituyen una barrera para obtener datos de los usuarios.

Tres de cada cuatro de las herramientas de ciberseguridad que se utilizan con más frecuencia son reactivas, no preventivas, lo que dificulta la ejecución de prácticas de ciberseguridad proactivas.



Casi siete de cada 10 organizaciones (71 %) utilizaron 10 o más herramientas de ciberseguridad preventiva en los últimos dos años.

¿Qué hace que la ciberseguridad preventiva sea tan difícil?

En una época en la que los programas de ciberseguridad se enfrentan a niveles de escrutinio sin precedentes por parte de los organismos gubernamentales y la comunidad de inversionistas, muchas organizaciones afirman que afrontan desafíos para informar y comunicar sobre el riesgo. La naturaleza de aislamiento en silos de las miles de soluciones puntuales que ofrecen los proveedores de ciberseguridad hace casi imposible comprender en toda su profundidad y amplitud la exposición de una organización.

La complejidad de la infraestructura de TI - con su dependencia de varios sistemas en la nube, múltiples herramientas de gestión de identidades y privilegios y diversos activos orientados a la web - conlleva múltiples oportunidades de errores de configuración y omisiones de activos.

¿En cuál de las siguientes áreas es mayor su exposición al riesgo?

Área	Encuestados
Infraestructura en la nube pública	33 %
Infraestructura en multinube/híbrida	23 %
Internet de las cosas (IoT)	20 %
Infraestructura en la nube privada	11 %
Herramientas de gestión de contenedores en la nube	11 %
Tecnología operativa/sistema de control industrial (ICS)/Control de supervisión y adquisición de datos (SCADA)	2 %
Infraestructura local	1 %-

BASE: 825 ENCUESTADOS QUE PARTICIPAN EN EL ESTABLECIMIENTO, LA GESTIÓN Y/O LA IMPLEMENTACIÓN DE ESTRATEGIAS, PRESUPUESTOS Y/O MÉTRICAS DE DESEMPEÑO DE CIBERSEGURIDAD/SEGURIDAD, INCLUYENDO 101 DE MÉXICO.

La mayoría de los encuestados (77 %) considera que la infraestructura en la nube (específicamente la nube pública, multinube y/o la nube híbrida) es la mayor fuente de exposición en su organización.

Abordar las áreas de riesgo requiere no solo visibilidad hacia toda la superficie de ataque, sino también la capacidad de analizar con eficacia los hallazgos en su contexto. Sin embargo, los líderes de ciberseguridad y TI se enfrentan al desafío de obtener información de la mezcolanza de herramientas de ciberseguridad preventiva en uso. Casi siete de cada 10 encuestados (71 %) utilizaron 10 o más herramientas de ciberseguridad preventiva en los últimos 12 a 24 meses.

¿Cuál de las siguientes herramientas o tecnologías utiliza su organización como parte de su estrategia de ciberseguridad?

Herramientas/tecnologías	Encuestados
Gestión de identidades y privilegios de usuario	86 %
Cifrado de contraseñas	82 %
Software antivirus/antimalware	76 %
Firewalls	74 %
Seguridad en la nube	60 %
Seguridad de la comunicación y la colaboración (por ejemplo, seguridad del correo electrónico, prevención de pérdida de datos, cifrado)	60 %
Detección y respuesta en puntos de conexión (EDR)/detección y respuesta ampliadas (XDR)	55 %
Gestión de vulnerabilidades	55 %
Servicios de seguridad gestionados (por ejemplo, proveedor de servicios de seguridad gestionados [MSSP], detección y respuesta gestionadas [MDR])	44 %
Seguridad de aplicaciones web	38 %

NOTA: SE PERMITIERON RESPUESTAS MÚLTIPLES BASE: 825 ENCUESTADOS QUE PARTICIPAN EN EL ESTABLECIMIENTO, LA GESTIÓN Y/O LA IMPLEMENTACIÓN DE ESTRATEGIAS, PRESUPUESTOS Y/O MÉTRICAS DE DESEMPEÑO DE CIBERSEGURIDAD/SEGURIDAD, INCLUYENDO 101 DE MÉXICO.

Se requieren muchos recursos para gestionar todas estas herramientas aisladas en silos. Tres de cada cuatro encuestados (75 %) (México Q7-Línea de países 314) tienen 25 o más empleados destinados a la implementación, el soporte, el mantenimiento y/o las relaciones con los proveedores de las herramientas de ciberseguridad preventiva en uso.

Para empeorar las cosas, los profesionales de ciberseguridad y TI tienen que procesar demasiados datos de demasiadas fuentes dispares.

¿Cuál de las siguientes opciones utiliza su organización para identificar la exposición global al riesgo?

Fuente de datos	Encuestados
Fuentes de inteligencia de amenazas	64 %
Hallazgos en la nube	60 %
Hallazgos de evaluaciones de preparación para incidentes	57 %
Resultados de pruebas de penetración	43 %
Revelaciones de vulnerabilidades	43 %
Hallazgos de la superficie de ataque externa	43 %
Perfiles y privilegios de los usuarios	33 %
Hallazgos de tecnología operativa	28 %
Inventarios de activos	28 %

NOTA: SE PERMITIERON RESPUESTAS MÚLTIPLES BASE: 825 ENCUESTADOS QUE PARTICIPAN EN EL ESTABLECIMIENTO, LA GESTIÓN Y/O LA IMPLEMENTACIÓN DE ESTRATEGIAS, PRESUPUESTOS Y/O MÉTRICAS DE DESEMPEÑO DE CIBERSEGURIDAD/SEGURIDAD, INCLUYENDO 101 DE MÉXICO.

Combinar todo esto es complicado e implica otra mezcla de herramientas aisladas en silos, desde sofisticadas plataformas de administración de eventos e información de seguridad (SIEM) y de inteligencia de negocios hasta la tradicional hoja de cálculo con varias pestañas.

¿Cuál de las siguientes opciones utiliza su organización para recopilar y analizar datos con el fin de cuantificar la exposición global al riesgo?

Método/herramienta	Encuestados
Herramientas de administración de eventos e información de seguridad (SIEM)	76 %
Plataformas de inteligencia de negocios	72 %
Herramientas de agregación	54 %
Lago de datos interno de nuestra organización	43 %
Hojas de cálculo con varias pestañas	30 %

NOTA: SE PERMITIERON RESPUESTAS MÚLTIPLES BASE: 825 ENCUESTADOS QUE PARTICIPAN EN EL ESTABLECIMIENTO, LA GESTIÓN Y/O LA IMPLEMENTACIÓN DE ESTRATEGIAS, PRESUPUESTOS Y/O MÉTRICAS DE DESEMPEÑO DE CIBERSEGURIDAD/SEGURIDAD, INCLUYENDO 101 DE MÉXICO.

Recopilar todos estos datos requiere mucho tiempo. En promedio, lleva 16 horas al mes elaborar informes para los líderes de negocios sobre la salud de su infraestructura de seguridad.

Mientras que los atacantes evalúan constantemente los entornos, en la mayoría de las organizaciones, las reuniones sobre los sistemas críticos para el negocio se celebran una vez al mes (¡en el mejor de los casos!). Una ligera mayoría (56 %) afirma que se reúne todos los meses con los líderes de negocios para debatir qué sistemas son críticos para el negocio, mientras que el 26 % celebra este tipo de reuniones solo una vez al año y el 3 % afirma que nunca las mantiene.

Si no se comprende bien la criticidad para el negocio de los sistemas en uso, ¿cómo pueden las organizaciones priorizar con eficacia sus esfuerzos de corrección con el fin de reducir su exposición con el tiempo?

La ciberseguridad preventiva precisa contexto y visibilidad

Las organizaciones se enfrentan al desafío de priorizar sus respuestas al alcance total de las exposiciones en su superficie de ataque. Este se extiende mucho más allá de las vulnerabilidades tradicionales en el software de negocios y TI e incluye errores de configuración en la infraestructura y los servicios en la nube; errores de configuración en las herramientas que se utilizan para administrar los privilegios y el acceso de los usuarios; fallas en el código de las aplicaciones web y fallas en el software de tecnología operativa (TO).

¿Cuáles de las siguientes situaciones considera su organización que son exposiciones y/o vulnerabilidades?

Situación	Encuestados
Errores de configuración en la infraestructura y servicios en la nube que se utilizan a lo largo de toda mi organización	77 %
Fallas en algún software de negocios o de TI que se utiliza a lo largo de mi organización	67 %
Errores de configuración en las herramientas que utiliza mi organización para gestionar los privilegios y el acceso de los usuarios	55 %
Fallas en algún software de tecnología operativa que se utiliza a lo largo de mi organización	40 %

NOTA: SE PERMITIERON RESPUESTAS MÚLTIPLES BASE: 825 ENCUESTADOS QUE PARTICIPAN EN EL ESTABLECIMIENTO, LA GESTIÓN Y/O LA IMPLEMENTACIÓN DE ESTRATEGIAS, PRESUPUESTOS Y/O MÉTRICAS DE DESEMPEÑO DE CIBERSEGURIDAD/SEGURIDAD, INCLUYENDO 101 DE MÉXICO.

Para empeorar aún más las cosas, las organizaciones carecen de un método estandarizado para priorizar la corrección de vulnerabilidades en los activos de TI tradicionales.

Los encuestados recurren a otra mezcolanza, esta vez de metodologías y marcos, para intentar comprender qué vulnerabilidades representan el mayor riesgo para la organización.

¿Cuál de los siguientes métodos utiliza su organización para priorizar la corrección de vulnerabilidades de los activos de TI tradicionales?

Método/marco	Encuestados
Puntuaciones del sistema de puntuación de vulnerabilidades comunes (CVSS)	67 %
Documentos de Intercambio de Vulnerabilidad y Explotabilidad (VEX)	63 %
Marco de tácticas, técnicas y conocimientos comunes de adversarios (ATT&CK) de MITRE	51 %
EPSS	49 %
Categorización de vulnerabilidades específica de las partes interesadas (SSVC)	46 %
Puntuación específica del proveedor	27 %

NOTA: SE PERMITIERON RESPUESTAS MÚLTIPLES BASE: 825 ENCUESTADOS QUE PARTICIPAN EN EL ESTABLECIMIENTO, LA GESTIÓN Y/O LA IMPLEMENTACIÓN DE ESTRATEGIAS, PRESUPUESTOS Y/O MÉTRICAS DE DESEMPEÑO DE CIBERSEGURIDAD/SEGURIDAD, INCLUYENDO 101 DE MÉXICO.

Si bien la mayoría de los encuestados (81 %) afirma tener en cuenta la identidad del usuario y los privilegios de acceso al priorizar las vulnerabilidades para su corrección, más de la mitad señala que su organización carece de una forma eficaz de integrar dichos datos en sus prácticas de gestión de vulnerabilidades. Casi tres de cada cuatro encuestados (74 %) aseguran que sus sistemas aislados en silos constituyen una barrera para obtener datos de los usuarios.

También hay problemas con la falta de higiene en lo que respecta a los datos de usuario y los sistemas de gestión de vulnerabilidades, que el 58 % de los encuestados menciona como algo que les dificulta la extracción de datos de calidad para ayudar a tomar decisiones de priorización.

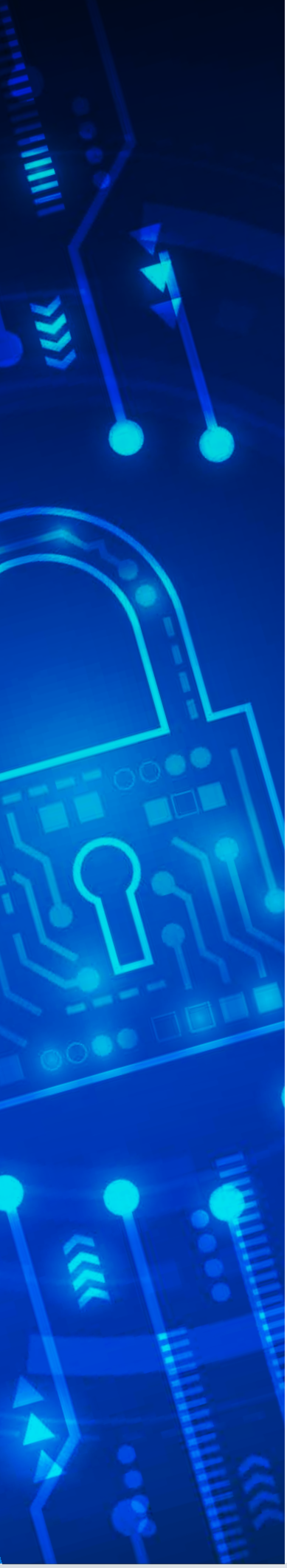
Para empeorar las cosas, los procesos y las actitudes internos pueden generar conflictos. Por ejemplo, más de dos tercios (70 %) de todos los encuestados (profesionales de TI y seguridad) afirman que el área de TI está más preocupada por el tiempo de actividad que por la colocación de parches o la corrección.

Además, el 32 % de todos los encuestados considera que la coordinación entre los equipos de TI y de ciberseguridad es difícil y requiere mucho tiempo.

Estos problemas no son nuevos. Aunque la aplicación de una higiene cibernética básica se considera desde hace tiempo una forma clave para reducir la exposición, continúa siendo un desafío para las organizaciones con su actual combinación de herramientas aisladas en silos.

Mientras tanto, la superficie de ataque aumenta exponencialmente cada año. La infraestructura digital moderna comprende varios sistemas en la nube, múltiples herramientas de gestión de identidades y privilegios, diversos activos orientados a la web, junto con sistemas y software de tecnología operativa (TO) e Internet de las cosas (IoT). El entorno de TI actual conlleva múltiples oportunidades de errores de configuración y omisión de activos.

La falta de una visión unificada y contextual de los usuarios, los sistemas y el software hace que los equipos de seguridad no puedan evaluar eficazmente lo que ocurre a lo largo de la superficie de ataque. Además, los intereses de negocios suelen favorecer la velocidad y el tiempo de actividad en detrimento de la seguridad.



Recomendaciones

Las organizaciones mexicanas pueden empezar a tomar medidas para reducir el riesgo dando 10 pasos para afrontar los desafíos relacionados con las personas, los procesos y la tecnología que se interponen en su camino.

PERSONAS

1. **Replantearse la forma de medir el rendimiento de sus equipos de TI y ciberseguridad** puede contribuir considerablemente a resolver conflictos internos y silos de la organización. ¿Existen contradicciones inherentes en la forma de recompensar a cada equipo? Considere la posibilidad de crear y utilizar métricas de puntuación e indicadores clave de rendimiento (KPI) que estén estrechamente alineados con el riesgo cibernético. Haga que todos los miembros de la organización cumplan con estas mismas métricas, independientemente de si trabajan en sus equipos de ciberseguridad, TI, ingeniería, DevOps, gestión de identidades y acceso o en la nube.
2. **Reduzca el número de herramientas aisladas en silo que estén en uso para que los equipos que tienen la responsabilidad de gestionar todas estas soluciones dispares**, y que pasan horas todos los meses elaborando informes a partir de ellas, puedan concentrarse en el análisis constante y la corrección preventiva en toda la profundidad y amplitud de la superficie de ataque. Destinar más recursos a la práctica de la ciberseguridad preventiva es el primer paso para reducir el riesgo cibernético. Cuando evalúe una nueva herramienta, tenga en cuenta el tiempo que tarda en generar valor; toda nueva herramienta tiene una curva de aprendizaje que reduce la productividad.

PROCESO

3. **Trate a la ciberseguridad como un verdadero socio de negocios**, e incorpórela en las etapas más tempranas posibles cuando considere la compra y la implementación de nuevas soluciones. Permita que el área de ciberseguridad participe en la elaboración de la estrategia de negocios. El sector de ciberseguridad debe colaborar estrechamente con los líderes de negocios para determinar cómo incorporar las métricas de los riesgos cibernéticos a todos los procesos de toma de decisiones. La seguridad es un deporte en equipo: no corresponde solo al área de ciberseguridad. La seguridad debe incorporarse a todos los procesos de negocios y estar en manos de todos los miembros de la organización. La ciberseguridad y la gestión de riesgos pueden proporcionar marcos y gobierno, pero son las áreas de negocio las que, en última instancia, toman las decisiones sobre los niveles de riesgo aceptables.
4. **Intente agrupar y analizar hallazgos de ciberseguridad dispares para conseguir una comprensión contextual de qué vulnerabilidades y errores de configuración plantean el mayor riesgo para su organización.** Implemente un abordaje claro y estandarizado para priorizar las iniciativas de corrección e incentivar a los equipos de TI para que la corrección sea una prioridad, con métricas que se comprendan claramente y que puedan rastrearse con el tiempo. Si la colocación de parches no es posible (por ejemplo, en entornos TO, o si un parche no se ha puesto a disposición), considere la posibilidad de establecer algún tipo de control compensatorio para reducir la exposición.

5. **Incorpore la seguridad de terceros como parte del programa general de ciberseguridad.** Implemente un proceso mediante el cual se evalúe el acceso a los datos por parte de terceros y, simultáneamente, se realicen evaluaciones constantes del entorno de los activos no gestionados que se conectan a la red corporativa.
6. **Invierta en la mejora de la higiene de los datos a lo largo de toda la organización.** Su ciberseguridad es tan buena como sus datos. La calidad de sus datos puede contribuir al éxito o al fracaso de todos los demás esfuerzos de ciberseguridad. La calidad de los datos es más fundamental que nunca con la llegada de las herramientas de inteligencia artificial generativa. Como afirma el dicho: "basura entra, basura sale".
7. **Implemente KPI para dar seguimiento a sus procesos y cuantificar la eficacia de estos.**

TECNOLOGÍA

8. **Audite su mezcla actual de herramientas.** ¿Puede agregar y analizar de forma rápida y eficaz los resultados de toda la profundidad y amplitud de su superficie de ataque, incluyendo la gestión de vulnerabilidades, la seguridad de aplicaciones web, la seguridad en la nube, la seguridad de identidades, el análisis de ruta de ataque y la gestión de superficie de ataque? Si le resulta difícil obtener una evaluación precisa y contextual de toda la profundidad y amplitud de su superficie de ataque en un momento dado, es posible que haya llegado el momento de asumir un nuevo abordaje.
9. **Vuelva a evaluar todas sus herramientas de ciberseguridad aisladas en silos y las funciones que desempeñan.** ¿Cuáles se utilizan principalmente en respuestas reactivas ante incidentes y cuáles lo ayudan a poner en práctica la ciberseguridad preventiva de forma cotidiana? ¿Las herramientas están creando silos internos que impiden una comunicación y coordinación eficaces entre TI y ciberseguridad? Las herramientas preventivas y de respuesta ante incidentes también deberían integrarse entre sí; cada una puede enriquecer a la otra con un contexto importante.
10. **Audite el valor de la información que recopila.** ¿Puede determinar rápidamente las relaciones entre usuarios, sistemas y software en toda su organización, de modo que pueda identificar y abordar de forma realista su exposición? O bien, ¿sus sistemas aislados en silos forman una barrera que le impide integrar eficazmente esos datos en sus prácticas de gestión de exposición? A medida que introduce más datos procedentes de diversas fuentes (nube, sistemas de TO, herramientas de gestión de identidades y acceso, escáneres de aplicaciones web y herramientas de gestión de superficie de ataque), corre el riesgo de sufrir una sobrecarga de datos. La higiene de los datos es fundamental, pero no es la única pieza del rompecabezas que hay que tener en cuenta. También debe considerar detenidamente la plataforma que utiliza y si puede ayudarle a encontrar algunas agujas críticas en el proverbial pajar, cuando este se expande exponencialmente cada año.

La ruta hacia la gestión de exposición

Proteger los entornos de TI complejos y dinámicos actuales exige reunir la gestión de vulnerabilidades, la seguridad de aplicaciones web, la seguridad en la nube, la seguridad de identidades, el análisis de ruta de ataque y la gestión de superficie de ataque externa para ayudarle a comprender toda la amplitud y profundidad de sus exposiciones. La complejidad de la superficie de ataque moderna es la razón principal del surgimiento de programas de gestión de exposición. Los equipos de seguridad se enfrentan al desafío de mantenerse al tanto de la afluencia constante de datos procedentes de la serie de soluciones puntuales que utilizan para gestionar las vulnerabilidades, las aplicaciones web, los sistemas de identidades y los activos en la nube. Además, se enfrentan al desafío de analizar de forma eficaz todos esos datos para tomar decisiones informadas y proactivas sobre qué exposiciones representan el mayor riesgo para la organización. La implementación de un programa de gestión de exposición permite a los profesionales de la seguridad asignar mejor el tiempo y los recursos para poder enfocarse en la toma de acciones preventivas que reduzcan legítimamente el riesgo cibernético de una organización.

La adopción de un programa de gestión de exposición implica cambios en las personas y en los procesos. Requiere que los equipos de seguridad den tanta importancia a los esfuerzos proactivos como la que actualmente dan a los esfuerzos reactivos de respuesta ante incidentes. Requiere que los profesionales de seguridad y de TI consideren cómo las estructuras organizativas aisladas en silos, y la infinidad de herramientas de seguridad que se utilizan en apoyo de esos silos, están obstaculizando su capacidad para ver lo que ve un atacante. También requiere una forma para que los profesionales de seguridad analicen los datos procedentes de herramientas dispares que les permita extraer información significativa que puedan aplicar a sus objetivos de reducción de riesgos.

La gestión de exposición permite que su organización comprenda el riesgo cibernético para poder tomar decisiones de negocios más eficaces. La gestión de exposición, que se desarrolló sobre la base de la gestión de vulnerabilidades basada en el riesgo, adopta una visión más amplia de la superficie de ataque moderna y aplica contexto tanto técnico como de negocios para identificar con mayor precisión y comunicar con mayor exactitud el riesgo cibernético, lo que permite tomar mejores decisiones de negocios.

ACERCA DE TENABLE

Tenable® es la empresa de Exposure Management. Aproximadamente 43 000 organizaciones de todo el mundo confían en la ayuda de Tenable para comprender el riesgo cibernético y reducirlo. Como creador de Nessus®, Tenable amplió su conocimiento sobre vulnerabilidades para ofrecer la primera plataforma del mundo para ver y proteger los activos digitales en cualquier plataforma de cómputo. Entre los clientes de Tenable, se incluye aproximadamente al 60 % de las compañías de la lista Fortune 500, aproximadamente el 40 % de las compañías de la lista Global 2000 y grandes instituciones gubernamentales.

Para obtener más información, visite **es-la.tenable.com**.