TANIUM

CHIEF DISRUPTOR

Gestión de riesgos de la información: expectativas frente a realidad

Un *informe de perspectivas* de Tanium en asociación con Chief Disruptor.

INFORME DE PERSPECTIVAS

CONTENIDO

Introducción

La gestión de la información y la seguridad a menudo se mide en términos de costes generados, en lugar de los resultados empresariales logrados. Pero esto está cambiando, ya que las condiciones operativas inciertas para las empresas significan que el crecimiento comercial cada vez se vincula más a una comprensión precisa del riesgo. La transformación digital presenta nuevos desafíos para las organizaciones que desean obtener una visión más clara de sus activos de TI, riesgos tecnológicos y vulnerabilidades.

> **"La ciberseguridad es uno de los tres riesgos principales. Reconocemos eso como equipo de liderazgo y como empresa, por lo que se destacará muy significativamente en 2023".**
>
> **Director de Seguridad e Información**
> Negocio de empaquetado FTSE 100

Para abordar este desafío, los líderes sénior desarrollan nuevas estrategias para integrar la gestión de riesgos de la información en la estructura de su forma de hacer negocios. Ante este cambio, queríamos descubrir si todavía existen brechas entre la ideación de estas estrategias y la madurez real de su implementación.

En este informe, exploramos los factores contextuales que influyen en el nivel de madurez del sector de la información y la seguridad. A continuación, presentaremos las brechas a las que comúnmente se hace referencia entre la expectativa y la realidad cuando se trata de la gestión de riesgos de la información. El informe concluye con principios rectores para ayudar a cerrar la brecha de expectativas entre la estrategia y la implementación.

Reconocimientos

Los autores agradecen a los miembros sénior de la comunidad de Chief Disruptor que dedicaron su tiempo brindar entrevistas para este informe en el cuarto trimestre de 2022. Sus opiniones, algunas de las cuales se citan en las siguientes páginas, orientan la dirección de este informe. Estamos agradecidos por sus valiosas contribuciones e información.

Entrevistados

- Erik Gaston, vicepresidente de Compromiso Ejecutivo, Tanium
- Zac Warren, jefe asesor de seguridad, Tanium
- Barry Panayi, director de Datos e Información, John Lewis
- James Tomkins, arquitecto principal, Met Office
- Jon Roughley, director de Estrategia e Innovación de Datos, Experian
- Paul Curtis, director de Tecnología, Easyjet Holidays
- Matthew Wilmot, jefe de TI Empresarial y Seguridad de la Información del Grupo, Fraser Group
- Director de Seguridad e Información, departamento gubernamental
- Director de Seguridad e Información, negocio de empaquetado FTSE 100
- Gerente sénior, CERT, Vodafone
- Que Tran, director regional de Información, DP World
- Ketan Patel, director de Información del Grupo, WH Smith

SECCIÓN 1

El panorama actual

TI y su constante cambio

Nuestros entrevistados reconocieron que se ha dado una rápida evolución en la infraestructura de TI en los últimos años. El cambio de centros de datos locales a nubes públicas e híbridas es un disruptor clave. El cambio ha aportado ventajas operativas, como la velocidad de la comercialización, la escalabilidad y la capacidad de recopilar y almacenar más datos.

Desde el punto de vista de la seguridad, estos desarrollos necesitan un nuevo enfoque para la gestión de riesgos de la información. Con el almacenamiento físico en las instalaciones, los activos tecnológicos de una organización son tangibles y los activos de TI se pueden evaluar con enfoques tradicionales para la gestión de inventarios.

Y con la proliferación de software y soluciones en la nube, la complejidad del marco informático aumentó de manera exponencial. El cambio al trabajo remoto y el uso de dispositivos personales significa que el marco de una organización ya no está físicamente definido y los vectores de ataque se han expandido.

> "Tenemos empleados que quieren usar sus propios dispositivos, o que pueden querer trabajar en varias ubicaciones alrededor del mundo. Todos estos factores añaden más complejidad a la red".
>
> **Paul Curtis**
> Director de Tecnología, Easyjet Holiday

> "Ya no se trata de que un equipo altamente especializado mantenga la seguridad de un borde, ya que los vectores de ataque ahora incluyen el uso de WhatsApp o abrir un correo electrónico".
>
> **James Tomkins**
> Arquitecto principal, Met Office

A medida que las empresas se sustentan cada vez más estructuralmente en la tecnología, una filtración o un ataque se relaciona de manera directa con la capacidad de operar de una empresa, así como con la experiencia del cliente y el valor de marca.

> "El riesgo se hizo realidad hace unos tres años y tuvimos una gran filtración de datos muy pública. Afectó de gran manera nuestra reputación. Desde ese momento, decidimos aumentar de forma significativa nuestra inversión en gestión de riesgos y ciberseguridad".

Paul Curtis
Director de Tecnología, Easyjet Holiday

Los riesgos asociados con una gestión incorrecta de los activos de TI pueden provocar pérdidas significativas para una empresa. Por cada hora que un sitio web está inactivo, una empresa podría estar perdiendo ingresos importantes. Los cargos y sanciones asociados con una filtración también son notables. La cobertura negativa de la prensa y los debates en las redes sociales también pueden afectar los ingresos futuros. Con estos factores presentes, la justificación económica para invertir en herramientas, procesos y personal para ir más allá del cumplimiento hacia la resiliencia cibernética es obvia.

> "La seguridad se está convirtiendo en una prioridad cada año. Las historias sobre empresas que sufren filtraciones graves son más frecuentes. Como resultado, las soluciones de seguridad están ganando la carrera de la inversión debido a estos nuevos riesgos y sus resultados potencialmente catastróficos".

Barry Panayi
Director de Datos e Información, John Lewis

> "Lento es sinónimo de inactivo. Su sitio web no tiene por qué quedar inactivo para causar daños a su reputación. Si es lento, podría terminar con reseñas negativas en las redes sociales".

Erik Gaston
Vicepresidente de Compromiso Ejecutivo, Tanium

Muchos de nuestros entrevistados predijeron que la disolución de los límites organizativos continuará en 2023 y más allá. A medida que las empresas trabajan cada vez más en estrecha colaboración con los socios para superar desafíos cotidianos como el cambio climático, la disrupción de la cadena de suministro y las presiones inflacionarias, crece la necesidad de que las empresas compartan datos e información más allá de sus límites organizativos. Todo esto crea un argumento convincente para una mayor priorización e inversión en soluciones de seguridad y gestión de la información.

"Introdujimos protocolos estándar para la forma en que todas nuestras organizaciones asociadas entran en nuestra red y esto reduce los riesgos que asumimos. Esto es contrario a lo que hemos hecho históricamente, que era crear algo diferente para cada socio. Antes de que lo note, tendrá bajo su gestión muchos sistemas diferentes solo para administrar los datos que entran y salen", dice Paul Curtis, director de Tecnología de Easyjet Holidays

Un mandato del consejo de dirección

A medida que la información y la tecnología se convierten en componentes importantes de la capacidad de una organización para hacer negocios, el papel del director de Información evolucionó para reflejar la creciente importancia de este tema. A medida que TI converge con el negocio en general, el papel del director de Información (Chief Information Officer, CIO) está ahora en el foco.

> "La seguridad siempre se veía como algo aparte. Lo que veo en la mayoría de las empresas es que el papel del CIO está cambiando y ahora está más orientado al negocio. Ahí es donde vemos que la seguridad vuelve a emerger hasta su lugar legítimo, justo en medio".

Erik Gaston
Vicepresidente de Compromiso Ejecutivo, Tanium

A medida que la seguridad de la información y la tecnología de una organización se convierten en una prioridad principal para el consejo de dirección, los presupuestos de seguridad ahora son mayores. Para cumplir con esta prioridad, también se está desarrollando la función del director de Seguridad de la Información (Chief Information Security Officer, CISO). El CISO cada vez se alinea más estratégicamente con el CIO y el consejo de dirección para garantizar que se lleve a cabo una inversión eficaz en la gestión de la información y la seguridad.

> "Junto con el CIO, el CISO ahora tiene un puesto en la mesa del consejo de dirección y eso ha sido un desarrollo muy positivo".

Zac Warren
Jefe asesor de Seguridad, Tanium

Sin embargo, a medida que el CIO y el CISO buscan obtener una imagen clara para proporcionar un perfil de riesgo al consejo de dirección, pueden tener obstáculos por una falta de claridad y visibilidad en su parque informático. Muchos heredan amplios marcos informáticos con datos de infraestructuras heredadas, locales, en la nube y fuentes SaaS. Esto puede suponer un problema para el CIO y el CISO si desean articular el panorama de amenazas o demostrar un retorno de la inversión claro.

Convergencia de TI y seguridad

> "Intentamos alejarnos del antiguo enfoque donde todo tenía que pasar por varias medidas de seguridad. Se podría desarrollar una solución en ocho semanas, pero luego se gastaban de tres a seis meses esperando para obtener la aprobación de seguridad antes de que pueda ponerse dicha solución en marcha".

Paul Curtis
Director de Tecnología, Easyjet Holiday

Muchos de los entrevistados con los que hablamos recurren a modelos de SecOps en un intento por gestionar mejor el riesgo de la información y aumentar la visibilidad y la usabilidad de los activos de TI. SecOps implica una convergencia entre seguridad y operaciones de TI. Al permitir que la seguridad tenga un asiento en la mesa desde el mismísimo origen de un nuevo producto o servicio, las empresas pueden eliminar los bloqueos de seguridad más adelante.

> "Intentar diseñar sin involucrar al equipo de seguridad en ese proceso desde el principio muestra una falta de visión a futuro".

Barry Panayi
Director de Datos e Información, John Lewis

Si bien los esfuerzos por introducir o expandir SecOps son una evolución positiva, muchas organizaciones no pueden llevar a cabo completamente esta estrategia porque carecen de una comprensión fundacional de las herramientas, los procesos y las tecnologías que se usan en cada disciplina. Sin este nivel de comprensión, resulta difícil impulsar la eficiencia, la innovación y la eficacia entre las operaciones de TI y los equipos de seguridad.

"Reequipar la seguridad posteriormente suele ser más costoso y suele llevar más tiempo".

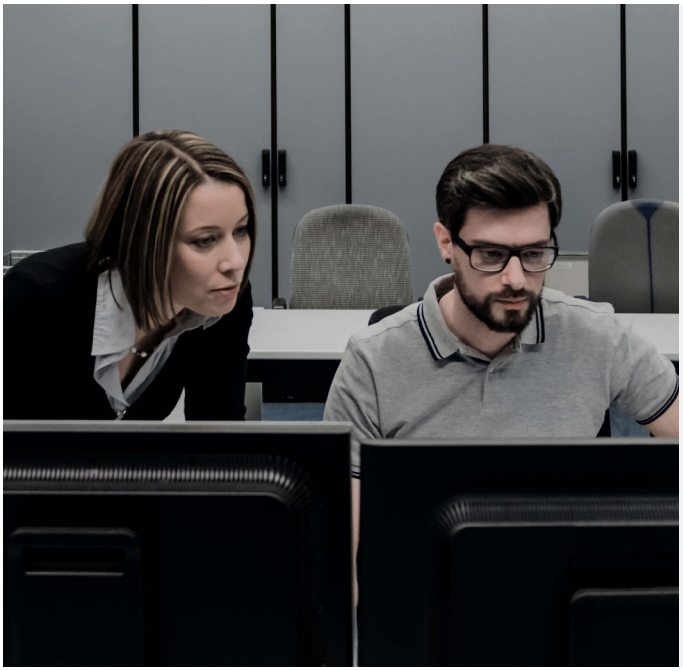
Que Tran
Director regional de Información, DP World

SECCIÓN 2

Expectativas frente a realidad

A medida que las organizaciones pasan de la estrategia a la implementación, a menudo surgen brechas en las expectativas. Gracias a entrevistas con expertos sénior en información y seguridad y líderes de una variedad de industrias, identificamos las ideas erróneas más comunes a las que se habían enfrentado los líderes durante su viaje para converger e innovar la seguridad y las operaciones de TI. En la siguiente sección de este informe, exponemos las expectativas y las realidades descritas por nuestros entrevistados. También establecemos una serie de principios que los líderes sénior pueden aplicar para ofrecer una mejor gestión del riesgo tecnológico.

"Muchas organizaciones pierden visibilidad porque heredan las arquitecturas y los entornos implementados por sus predecesores. Tomaron las mejores decisiones que pudieron con la tecnología, los procesos y las personas que tenían en ese momento, pero ahora nos damos cuenta de que existen brechas de seguridad", menciona Zac Warren, jefe asesor de Seguridad de Tanium.



> **"Siempre hay una brecha entre la aspiración y la implementación. Ese es un riesgo reconocido que debe gestionarse de manera adecuada".**
>
> **Director de Seguridad e Información**
> Negocio de empaquetado FTSE 100

Proliferación de herramientas frente a optimización de herramientas

La superficie de ataque ha crecido de forma exponencial debido a la expansión de la economía de la información y el desarrollo de pilas de tecnología cada vez más sofisticadas. En estos entornos complejos, las vulnerabilidades de seguridad pueden aparecer, reaparecer y multiplicarse de la noche a la mañana. Dado que las soluciones de firewall y VPN por sí solas son inadecuadas para proteger a las empresas modernas, la respuesta de muchas organizaciones fue adquirir una amplia gama de nuevas herramientas de ciberseguridad.

"Las capacidades de ciberseguridad son realmente muy buenas. En la falta de integración de las capacidades es donde está la brecha para muchas empresas", dice Erik Gasto, vicepresidente de Compromiso Ejecutivo de Tanium.

Aunque esto ha madurado la postura general de riesgo de seguridad, también ha aumentado la complejidad del complicado ecosistema de TI. Contrario a la intuición, un aumento en las herramientas para abordar las amenazas a la seguridad podría empeorar el problema si esas herramientas no se integran entre sí. Como tal, muchas organizaciones luchan contra cómo supervisar, gestionar y optimizar sus ecosistemas de información y seguridad existentes. Muchas organizaciones tienen funcionalidades duplicadas y aplicaciones infrautilizadas.

> "Utilizo las herramientas que ya están disponibles lo mejor posible antes de señalar las brechas".

Matthew Wilmot
Jefe de TI Empresarial y Seguridad de la Información del Grupo, Fraser Group

Para las organizaciones en esta posición, centrarse en la optimización de herramientas podría ser una estrategia más eficaz para sacar el máximo partido de las herramientas existentes. Esto comienza por obtener una visibilidad clara de los activos en uso e identificar formas de optimizar e integrar esas herramientas. Desde este punto de vista, las vulnerabilidades se pueden identificar y abordar de forma más eficaz y rápida.

> "Averigüe cómo utilizar completamente las herramientas que tiene disponibles. Elimine toda la interferencia, todo el software adicional y todas las cosas adicionales que no utiliza y luego vuelva a evaluar dónde están sus brechas. Para mí, se trata de simplificación".

Zac Warren
Jefe asesor de Seguridad, Tanium

Un panel único frente a múltiples paneles

> "Intentar obtener un panel único es increíblemente difícil, pero hay formas de crear lo que clasificamos como oráculos de la verdad".

Director de Seguridad e Información
Negocio de empaquetado FTSE 100

Un panel único es una estrategia de gestión que implica unificar los datos de varias fuentes y presentarlos como una visión única. A medida que las empresas tienen más datos y se vuelven dependientes de estos, los líderes sénior necesitan consolidar la información que entra y sale de su organización de diversas fuentes. Surgió la expectativa de que este flujo de información se puede gestionar a través de un único panel ejecutivo.

Gracias a nuestras entrevistas, descubrimos que lograr un panel único no siempre es eficaz para consolidar la información necesaria para responder a preguntas críticas para el negocio. Muchas empresas tienen demasiada información y demasiadas preguntas empresariales críticas que necesitan una respuesta rápida, lo que hace que un panel único no sea realista.

En su lugar, los líderes desarrollan múltiples paneles para abordar diversos problemas empresariales clave mediante la integración y la combinación de diferentes herramientas y la reducción de la información en un panel por problema empresarial. Al reunir datos de diferentes rincones de un entorno empresarial, los líderes cuentan con una imagen realista y obtienen una visión holística de los riesgos asociados con las aplicaciones y los datos críticos para el negocio.

> “Relacione directamente lo que está haciendo para resolver problemas empresariales. Luego, reduzca la información en planos de control que se relacionan de manera directa con la resolución de esos problemas empresariales. Eso es transformador. La transformación debe ser sencilla, no compleja”.

Erik Gaston
Vicepresidente de Compromiso Ejecutivo, Tanium

Cumplimiento frente a un enfoque basado en el riesgo

> “Enfoque su presupuesto porque nadie tiene un cheque en blanco cuando se trata de la seguridad y hay pocas personas con la experiencia para ello”.

Zac Warren
Jefe asesor de Seguridad, Tanium

Las organizaciones pueden protegerse contra numerosos riesgos mediante el cumplimiento.

Sin embargo, la expectativa de que cumplir con las normas equivale a ser ciberresistente es en gran medida incorrecto. El cumplimiento y la regulación a menudo se centran en áreas estrechas y fomentan un enfoque táctico que se limita a marcar casillas. Esto puede dejar sin control las vulnerabilidades y las brechas de seguridad.

> “Lo más importante son nuestros datos comercialmente sensibles y los datos de nuestros clientes. Para el resto, tenemos un nivel de seguridad diferente”.

Barry Panayi
Director de Datos e Información, John Lewis

Entre los expertos con los que hablamos, muchos estaban en proceso de cerrar la brecha entre el cumplimiento y un enfoque basado en el riesgo que previene y mitiga los riesgos.

Nuestros entrevistados solían mencionar la necesidad de llevar a cabo evaluaciones de riesgos para centrar sus recursos y experiencia en datos críticos en áreas de negocio de alta prioridad.

Una vez que esto se implemente, los datos pueden extraerse de múltiples fuentes, analizarse y protegerse en concordancia con una evaluación de riesgo. Esto proporciona una visión holística y ofrece la capacidad de afinar dinámicamente las aplicaciones y los datos críticos para el negocio, a medida que evolucionan las necesidades del negocio y el panorama de amenazas. Este enfoque también crea eficiencias y ayuda a demostrar las formas en que las medidas de seguridad pueden generar ingresos.

> “Comenzamos a analizar mucho más los controles graduados y el otorgamiento de derechos para entornos operativos y de investigación”.

James Tomkins
Arquitecto principal, Met Office

Pero para implementar de forma realista un enfoque basado en el riesgo, las empresas deben saber dónde se encuentran sus aplicaciones y datos críticos para el negocio. Deben tener visibilidad en sus ecosistemas de TI y procesos organizativos para evitar la expansión de herramientas e información.

Complejidad frente a simplicidad

> "Se han llevado a cabo esfuerzos significativos para simplificar el panorama de las políticas porque la seguridad a menudo se considera demasiado compleja".

James Tomkins
Arquitecto principal, Met Office

Muchas organizaciones aceptan que la complejidad añadida es inevitable en el recorrido de la infraestructura local a la nube pública. Sin embargo, dado que la transformación digital no muestra signos de desaceleración, las organizaciones reconocen que no pueden gestionar niveles de complejidad no controlados.

Siguiendo el ritmo y la escala de la transformación digital, las empresas reconocen que una complejidad excesiva les impide innovar y comprender sus vulnerabilidades. Para combatir esto, muchos de nuestros entrevistados se embarcaron en programas para simplificar sus ecosistemas de TI.

A medida que las empresas buscan implementar enfoques basados en el riesgo para la gestión de la información y la seguridad, es cada vez más claro que ser capaz de catalogar datos, activos e información de forma coherente y hacer un seguimiento de eso a través de la organización es un punto de partida clave.

> "Si no tiene esa visibilidad básica, no puede entender sus vulnerabilidades. Y para mí, esa es la mayor brecha que la mayoría de las organizaciones tienen entre las expectativas y la realidad".

Zac Warren
Jefe asesor de Seguridad, Tanium

"Tener observabilidad en la organización para ver lo que sucede es una prioridad para nosotros. A un plano empresarial significativo, queremos ver lo que sucede en el negocio a diario", dice James Tomkins, arquitecto principal de Met Office

> **"Estamos simplificando nuestro patrimonio general. Desde el punto de vista de la seguridad y los datos, es mucho más fácil gestionar un único conjunto de recursos que se pueden escalar, en lugar de muchos sistemas dispares. Esa simplificación realmente reduce la complejidad y hace que sea mucho más difícil que haya varios agujeros".**

Paul Curtis
Director de Tecnología, Easyjet Holiday

SECCIÓN TRES

Principios rectores para una mejor gestión del riesgo de la información

A medida que las organizaciones buscan superar las expectativas antiguas e implementar estrategias realistas para una gestión eficaz del riesgo de la información, pueden ayudar varios principios rectores. En la siguiente sección de este informe, resumimos los consejos más citados compartidos por los líderes sénior de información, datos y tecnología entrevistados para este informe.

Higiene de TI

> "La higiene de TI es realmente el elemento fundamental. Una vez que la implemente, podrá avanzar más hacia la gestión de riesgos, el cambio cultural y, en última instancia, la resiliencia cibernética".

Director de Seguridad e Información
Negocio de empaquetado FTSE 100

Las empresas que deseen desarrollar significativamente la resiliencia cibernética de su organización deben resistirse a soluciones rápidas o exageradas. A menudo, más herramientas que prometen ser la panacea pueden aumentar el problema al crear capas adicionales de complejidad en el ecosistema.

"Un componente fundamental de la seguridad es una buena higiene. La falta de higiene de TI en lo que respecta a la ciberseguridad es negar lo obvio, lo cual significa poder ver todos sus activos y evaluar sus vulnerabilidades. Desafortunadamente, es una brecha enorme", dice Zac Warren, jefe asesor de seguridad de Tanium.

En la búsqueda de la resiliencia cibernética, las empresas deben duplicar la higiene de TI. Obtener la claridad necesaria para lograr un progreso estratégico requiere una visión precisa de todo el parque informático de una organización. Es esencial organizar eficazmente los activos de SaaS, locales y en la nube antes de poder obtener datos precisos sobre el riesgo.

Esto implica mantener los activos de TI organizados y ordenados al garantizar que los inventarios estén actualizados y completos. La importancia de estos pasos fundamentales no puede exagerarse. Al minimizar las preocupaciones comunes relacionadas con la salud e higiene del parque informático, es más fácil determinar qué riesgos y vulnerabilidades están presentes.

Automatización

> "Estamos estudiando cómo podemos automatizar más los inventarios estándar".

Barry Panayi
Director de Datos e Información, John Lewis

Si bien implementar y mantener la higiene de TI es esencial, puede ser un negocio que consume mucho tiempo. El esfuerzo manual de llevar a cabo inventarios de TI, aplicaciones y datos también puede ser ineficiente y estar sujeto a errores humanos. Incluso para los expertos en seguridad más cualificados, la recopilación de datos de una gran cantidad de herramientas especializadas con interoperabilidad limitada dificulta su capacidad para recopilar información oportuna y rica en contexto.

> "Queremos que nuestros desarrolladores trabajen sin restricciones, sabiendo que todo lo que hacen pasa por procesos y procedimientos de calidad automatizados. Utilizamos el proceso de creación para destacar cualquier cosa que no supere nuestros estándares de seguridad".

Paul Curtis
Director de Tecnología, Easyjet Holidays

Al automatizar los procesos relacionados con la higiene de TI y el mantenimiento de la seguridad, una empresa puede liberar su talento para centrarse en proyectos que están estratégicamente alineados con los objetivos empresariales. Esto ayuda a convertir la actividad relacionada con la seguridad de un centro de costos en un generador de ingresos.

"Una parte integral de poder hacer esto con éxito es observar los mecanismos que podemos usar para la automatización. Porque confiar en grandes esfuerzos manuales no aporta valor empresarial. Así que tendremos que construir mucho de esto con automatización para proporcionar esa observabilidad. De lo contrario, se vuelve muy difícil porque las cosas se mueven muy rápido", dice James Tomkins, arquitecto principal de Met Office.

> **"El simple hecho de ampliar nuestros equipos de seguridad no es una solución a largo plazo. En este momento, no podemos identificar amenazas con la suficiente rapidez ni defendernos a la mayor velocidad posible. La automatización, la integración y la interoperabilidad son nuestros medios para llevar a cabo y cumplir los objetivos de seguridad de la industria a largo plazo de manera demostrable".**

Director de Seguridad e Información
Departamento gubernamental

Cuando un terminal puede estar en peligro, la automatización también permite a los equipos de incidentes acelerar los tiempos de respuesta al proporcionar una imagen rápida y precisa del entorno en minutos en lugar de días.

> **"Automatizar lo que hacemos día a día ayuda a solidificar y proteger una organización".**

Ketan Patel
Director de Información del Grupo, WH Smith

Colaboración

Junto con la mejora de los procesos y la tecnología, un componente clave de una mejor gestión del riesgo de la información es la cultura. Un elemento central del éxito es la capacidad de trasladar la seguridad de un silo a una parte integral del negocio.

Esto comienza en la parte superior de la organización, con un trabajo más colaborativo entre los CIO, los CISO y el consejo de dirección. Se expande a las formas de trabajar, lo que garantiza que los profesionales de seguridad formen parte del diseño y la entrega, y no solo de la agenda general de TI, sino también de la agenda general del negocio.

> "Los modelos de SecOps son importantes porque muestran un tipo diferente de mentalidad sobre cómo encaja la seguridad en las operaciones generales de la organización".

Que Tran
Director regional de Información, DP World

La introducción de modelos de SecOps busca lograr este objetivo, lo que fomenta una mayor colaboración entre los equipos de seguridad y las operaciones de TI. Para que los modelos de SecOps pasen con éxito de la estrategia a la implementación, las empresas deben obtener una comprensión profunda de las herramientas que tradicionalmente sustentan cada disciplina y encontrar formas de integrarlas de manera significativa para permitir que los equipos aislados se unan de manera impactante.

> "Intentar diseñar sin involucrar al equipo de seguridad desde el principio muestra una falta de visión a futuro".

Barry Panayi
Director de Datos e Información, John Lewis

Al impulsar una mayor colaboración entre los equipos de seguridad y operaciones de TI, las organizaciones pueden aumentar la visibilidad de los riesgos de seguridad y las prioridades de TI para impulsar de forma dual el crecimiento y la resiliencia del negocio. Al integrar y automatizar la seguridad y las operaciones de TI, se pueden obtener más beneficios en forma de agilidad y eficiencia.

> "La colaboración con su equipo y sus líderes realmente vale la pena. Al colaborar a lo largo del recorrido, la entrega es mucho más oportuna y rentable".

Gerente sénior
CERT, Vodafone

> "Se consideraba que la seguridad era un tema con el que los empleados no podían involucrarse fácilmente y, por lo tanto, se desconectaban. Como resultado, cayó en manos de algunos especialistas. Para contrarrestar esto, introdujimos programas de comunicación y educación amplios en toda la organización para incorporar la seguridad como responsabilidad de todos".

James Tomkins
Arquitecto principal, Met Office

CONCLUSIÓN

El total es mayor que la suma de sus partes

> "Muchas empresas intentan resolver amenazas complejas de ciberseguridad con soluciones lineales. Pero el panorama del riesgo no se presenta como una serie de problemas lineales. Para un problema dinámico como la seguridad, las empresas tendrán que apoyarse más en las plataformas integradas que proporcionan el panorama completo".

Erik Gaston
Vicepresidente de Colaboración Ejecutiva Tanium

A medida que la gestión de la información y la seguridad evoluciona y madura más a fondo, los profesionales de esta área seguirán viendo desafiadas sus expectativas. Sin embargo, al apoyarse en principios rectores, las organizaciones pueden introducir enfoques basados en el riesgo y modelos colaborativos que hacen de la seguridad una parte integral de la actividad empresarial, cerrando así la brecha entre las expectativas y las realidades.

Los problemas dinámicos y en constante cambio, como la seguridad, necesitan una solución que sea mayor que la suma de sus partes. Ninguna solución, equipo o metodología proporcionará una solución rápida, porque para resolver problemas dinámicos se necesitan soluciones integradas. Para lograr un enfoque estratégico y preventivo, las empresas deben centrarse en optimizar e integrar las herramientas que tienen y consolidarlas para proporcionar una mejor visión general del panorama de amenazas.

> "Obtener visibilidad hace más de lo que está escrito. No solo reduce enormemente el riesgo, que es un factor muy importante, sino que también acelera la innovación porque podemos ver cuáles activos de datos tenemos dentro de la organización".

Jon Roughley
Director de Estrategia e Innovación de Datos, Experian

CHIEF DISRUPTOR

Chief Disruptor es la comunidad para líderes empresariales y tecnológicos.

Al igual que nosotros, los líderes disruptivos creen que la disrupción es un catalizador de la oportunidad, y Chief Disruptor representa con orgullo y celebra esa mentalidad. Desde 2005, nuestra comunidad de miembros para líderes empresariales y tecnológicos ha reunido a innovadores, creadores de cambios y pensadores disruptivos para compartir experiencias, estrategias e información procesable.

Nuestro propósito siempre ha sido dejar atrás el revuelo y permitir que nuestros miembros aprovechen estas tendencias y tecnologías disruptivas mediante nuestros informes de conocimientos, contenido y actividades comunitarias dirigidos por miembros.

Con los continuos disturbios geopolíticos y la sombría realidad de la recesión en el horizonte, las organizaciones ahora más que nunca necesitan un liderazgo ágil y decidido que aproveche las oportunidades y gestione proactivamente las amenazas de la disrupción. No va a ser fácil, pero estamos aquí para ayudarlo. Conéctese. Aprenda. Sea disruptivo. **chiefdisruptor.com**

TANIUM

Tanium, único proveedor del sector para la gestión convergente de terminales (Converged Endpoint Management, XEM), lidera el cambio de paradigma en los enfoques heredados para gestionar entornos complejos de seguridad y tecnología.

Solo Tanium unifica equipos y flujos de trabajo y protege cada terminal de las amenazas cibernéticas al integrar TI, Cumplimiento, Seguridad y Riesgo en una plataforma única que ofrece una visibilidad integral en todos los dispositivos, un conjunto unificado de controles y una taxonomía común para un único propósito compartido: proteger la información crítica y la infraestructura a escala. Tanium ha sido incluida en la lista Forbes Cloud 100 por siete años consecutivos y forma parte de la lista Fortune de las mejores empresas grandes para trabajar en el sector tecnológico. De hecho, más de la mitad de las empresas de la lista Fortune 100 y las Fuerzas Armadas de EE. UU. confían en Tanium para proteger a las personas y los sistemas, defender los datos y ver y controlar todos los terminales, equipos y flujos de trabajo en cualquier lugar. Ese es el poder de la certeza.

Visítenos en **www.tanium.com** y síganos en **LinkedIn** y **Twitter**.