Cómo maximizar el retorno de inversión de su presupuesto de ciberseguridad mientras reduce los riesgos

Wayne Anderson
Managing Director, CI | BDO USA
wanderson@bdo.com

En la economía actual, donde lo digital es lo primero, los presupuestos para ciberseguridad están aumentando en todos los sectores. Sin embargo, a pesar de este crecimiento, muchas organizaciones siguen sufriendo incidentes frecuentes, retrasos en la recuperación y estancamiento en sus esfuerzos de transformación.

El verdadero reto no es el tamaño del presupuesto, sino la eficacia con la que se utilizan esos fondos para reducir el riesgo y permitir el rendimiento empresarial.

Crecimiento presupuestario sin mejoras en el rendimiento

Una encuesta global auspiciada por BDO y realizada por IDC revela una desconexión reveladora. Casi la mitad de las organizaciones cuentan con presupuestos flexibles para ciberseguridad, pero aún así sufren un promedio de más de cinco incidentes al año. Esto sugiere que la adecuación del presupuesto por sí sola no garantiza la resiliencia.

El rendimiento depende de cómo se asignen los presupuestos de manera estratégica. Las organizaciones que alinean el gasto con la preparación operativa, la madurez de los procesos y los objetivos de transformación reportan sistemáticamente resultados más sólidos. Por el contrario, aquellas que tratan la ciberseguridad como un centro de costos reactivo a menudo tienen dificultades para traducir la inversión en un impacto medible.

Consejos para maximizar el impacto de su presupuesto de ciberseguridad

Para sacar el máximo partido a cada dólar invertido en ciberseguridad, las organizaciones deben adoptar un enfoque basado en el rendimiento. Esto significa ir más allá del gasto reactivo y centrarse en la ejecución estratégica. A continuación se presentan cinco estrategias clave para ayudar a maximizar el valor de sus inversiones en ciberseguridad.

01

Priorizar las inversiones basadas en el riesgo.

Una planificación presupuestaria eficaz comienza por comprender el panorama de riesgos específico de su organización. Identifique las amenazas más críticas, como el ransomware, las amenazas internas o las vulnerabilidades de la cadena de suministro, y asigne recursos para abordarlas en primer lugar. Las evaluaciones de riesgos deben guiar las decisiones presupuestarias, garantizando que los fondos se destinen a las áreas con mayor impacto potencial.

Por qué es importante: el informe de IDC reveló que las organizaciones con marcos proactivos de modelización y gobernanza de riesgos experimentan menos interrupciones y recuperaciones más rápidas. Dar prioridad a las inversiones basadas en el riesgo ayuda a garantizar que el gasto en ciberseguridad se ajuste a las prioridades empresariales.

02

Invertir en la preparación operativa.

La eficacia presupuestaria está estrechamente relacionada con la madurez operativa. Las organizaciones que cuentan con capacidades de supervisión y respuesta ante amenazas las 24 horas del día, los 7 días de la semana, detectan y contienen las amenazas más rápidamente, lo que reduce el tiempo de permanencia y limita los daños. Estas capacidades proporcionan la visibilidad y la agilidad necesarias para responder a las amenazas en constante evolución en tiempo real.

Las áreas clave que deben financiarse incluyen:
- Supervisión continua (interna o externalizada)
- Detección y respuesta automatizadas ante amenazas
- Protección de terminales para plantillas híbridas
- Manuales de respuesta ante incidentes y simulacros

Las organizaciones con procesos de detección e investigación optimizados, a menudo respaldados por herramientas de inteligencia artificial y detección y respuesta ampliadas (XDR), suelen registrar un número significativamente menor de incidentes y tiempos de recuperación más rápidos.

03

Racionalizar la estructura tecnológica.

La proliferación de herramientas es un problema habitual que genera complejidad, ineficiencia y gasto innecesario. Muchas organizaciones acumulan herramientas que se solapan con el tiempo, lo que crea problemas de integración y aumenta los gastos operativos. La consolidación de la estructura tecnológica puede mejorar la visibilidad, reducir los costes y aumentar la eficacia general..

Consejo: Busque plataformas que ofrezcan coordinación, automatización y visibilidad unificada en todos los puntos finales, redes y activos en la nube. Las soluciones optimizadas no solo reducen la complejidad, sino que también mejoran los tiempos de respuesta y reducen la probabilidad de configuraciones erróneas.

04

Desarrollar capacidades estratégicas internas.

Si bien la tercerización puede ofrecer escala y eficiencia, ciertas capacidades se desarrollan mejor internamente. Entre ellas se incluyen la gobernanza, la modelización de riesgos y los programas de concienciación de los empleados. El desarrollo de estas capacidades a nivel interno garantiza que la ciberseguridad se integre en la cultura y los procesos de toma de decisiones de la organización.

Las áreas de interés incluyen:
- Programas de formación y concienciación sobre ciberseguridad
- Integración de la gobernanza, el riesgo y el cumplimiento normativo
- Marcos de gestión de riesgos de GenAI

A medida que crece la adopción de GenAI, las organizaciones deben abordar nuevos riesgos, como el phishing, la fuga de datos y las deficiencias en la gobernanza. Invertir en la formación de los empleados y en controles de seguridad específicos para la IA es esencial para mitigar estas amenazas emergentes.

05

Mida los indicadores principales, no solo los resultados.

Las juntas directivas y los ejecutivos suelen solicitar métricas como la frecuencia de incidentes o el ahorro de costes. Aunque son importantes, no ofrecen una visión completa de la madurez de la ciberseguridad. Los indicadores adelantados, como el tiempo de detección, las tasas de aplicación de parches y la eficacia de la formación, ofrecen una visión más profunda del estado de los procesos y la preparación operativa.

Por qué es importante: sin visibilidad de los procesos internos, las organizaciones pueden sobreestimar su resiliencia. La medición de los indicadores adelantados ayuda a identificar las deficiencias de forma temprana y favorece la mejora continua.

Prepare su estrategia presupuestaria para el futuro

La elaboración de presupuestos para la ciberseguridad debe ser más estratégica, y las organizaciones deben adoptar modelos que vinculen la financiación con mejoras cuantificables en la reducción de riesgos, la velocidad de recuperación y el éxito de la transformación. Para mantener su eficacia, los presupuestos deben revisarse periódicamente y adaptarse a la evolución de las amenazas y las prioridades empresariales. El informe de IDC destaca tres áreas clave de interés: el aumento de la automatización mediante la inteligencia artificial y el aprendizaje automático, las estrategias de mitigación específicas para abordar los riesgos emergentes de la GenAI y una gobernanza más sólida en torno al riesgo de terceros, que sigue sin contar con la financiación necesaria a pesar de su papel en muchas violaciones de seguridad. Cuando las inversiones en ciberseguridad se vinculan a resultados y objetivos empresariales claros, se convierten en un motor de resiliencia, innovación y crecimiento a largo plazo.

Para explorar todos los hallazgos y conclusiones mencionados en este artículo, le invitamos a que tome la iniciativa:

- **Descargue el Informe** para descubrir cómo los líderes en ciberseguridad están alineando la estrategia con la ejecución para impulsar la transformación.
- **Inscríbase en nuestro próximo webinar** para escuchar directamente al equipo global de BDO hablar sobre cómo desarrollar la resiliencia cibernética en el cambiante panorama actual de amenazas.
- **Explore la herramienta** Cyber Risk Analyzer para evaluar la postura actual de su organización en materia de ciberseguridad e identificar áreas de mejora.

DESCARGUE EL INFORME

INSCRÍBASE EN NUESTRO PRÓXIMO WEBINAR

EXPLORE LA HERRAMIENTA CYBER RISK ANALYZER

Estos recursos están diseñados para ayudarle a tomar decisiones informadas, reforzar su estrategia de ciberseguridad y sacar el máximo partido a su presupuesto.