El papel de la ciberseguridad en la transformación digital: por qué es importante involucrarse desde el principio

Mes de Concienciación sobre la Ciberseguridad 2025

Rocco Galletto
Global Cybersecurity Leader
rgalletto@bdo.ca

La transformación digital está remodelando las industrias. Las organizaciones están invirtiendo en la nube, la inteligencia artificial y el análisis de datos para impulsar el crecimiento y la agilidad. Sin embargo, la ciberseguridad suele incorporarse demasiado tarde y se trata como una medida de protección técnica en lugar de como un facilitador estratégico. Según un nuevo informe de IDC auspiciado por BDO, solo **el 40% de las organizaciones integran la ciberseguridad durante la fase de planificación** de las iniciativas digitales. Este retraso introduce riesgos que pueden frenar el progreso y erosionar la confianza.

La ciberseguridad debe formar parte de los cimientos. Cuando los equipos cibernéticos se involucran desde el principio, ayudan a diseñar arquitecturas seguras, anticipar amenazas y alinear los controles con los objetivos empresariales. Este enfoque proactivo refuerza la resiliencia y acelera el tiempo de retorno de la inversión.

Pensemos en una empresa minorista que lanza una nueva plataforma de comercio electrónico. Si la ciberseguridad se tiene en cuenta desde el principio, el equipo puede asesorar sobre integraciones de pago seguras, cumplimiento de la privacidad de los datos y prevención del fraude. Si se incorpora más tarde, estos riesgos pueden salir a la luz después del lanzamiento, lo que podría dañar la confianza de los clientes y requerir costosas modificaciones.

Para incorporar la ciberseguridad desde el principio del proceso de transformación digital y garantizar el éxito de dicho proceso, será necesario:

- alinear los presupuestos destinados a la ciberseguridad con la estrategia empresarial
- actualizar los programas de ciberseguridad para que sigan siendo relevantes; y
- desarrollar la madurez cibernética para lograr resiliencia.

Optimización del presupuesto cibernético: alinear el gasto con la estrategia

Los presupuestos destinados a la ciberseguridad están aumentando, pero las mejoras en el rendimiento siguen siendo desiguales. Los datos de IDC muestran que incluso las organizaciones con presupuestos flexibles registran una media de cinco incidentes al año. El problema no es la falta de presupuesto, sino cómo se aplica ese presupuesto.

Una inversión eficaz en ciberseguridad comienza con una alineación estratégica. Los presupuestos deben respaldar capacidades que reduzcan el riesgo y permitan la transformación. Esto incluye la detección proactiva, la automatización y la colaboración entre departamentos. Las organizaciones que incorporan la ciberseguridad en su planificación registran menos retrasos y una mayor confianza por parte de las partes interesadas.

Por ejemplo, cuando una empresa de capital privado y las empresas de su cartera invierten en la migración a la nube, suelen tener en cuenta el rediseño de las aplicaciones, la migración de datos, la modernización, la eficiencia operativa y la disponibilidad del sistema.

Sin embargo, a menudo se pasa por alto la ciberseguridad, especialmente en áreas como las evaluaciones del impacto normativo, las prácticas de codificación segura durante la fase de construcción y la seguridad de las interacciones de las aplicaciones con otros sistemas. Sin los controles adecuados, los datos confidenciales pueden quedar expuestos. Un enfoque más eficaz consiste en alinear el presupuesto con la hoja de ruta de la transformación, incorporando la seguridad en cada capa y paso del proceso.

La participación en fases avanzadas conlleva reprocesos, incumplimiento de plazos y disminución de los beneficios. Para maximizar el impacto, la ciberseguridad debe tratarse como un socio estratégico, no como una solución reactiva. Esta necesidad de alineación estratégica conduce naturalmente a la siguiente consideración: con qué frecuencia las organizaciones se detienen para reevaluar su enfoque de ciberseguridad.

Actualización de la estrategia cibernética: una práctica que merece prioridad

En un entorno que cambia rápidamente, detenerse a reflexionar puede parecer contraproducente. Sin embargo, es esencial. Los líderes cibernéticos deben reevaluar periódicamente sus estrategias para asegurarse de que siguen estando en sintonía con las prioridades empresariales.

Las actualizaciones anuales, las métricas basadas en resultados y la colaboración interfuncional ayudan a los equipos a mantener su relevancia y eficacia. La reflexión también revela prácticas heredadas que obstaculizan el progreso. Al adoptar enfoques ágiles y alineados con el negocio, los equipos de ciberseguridad pueden fomentar la innovación y obtener mejores resultados.

Esta práctica refuerza la colaboración entre las unidades cibernéticas y empresariales, elimina los obstáculos y genera confianza. No se trata solo de mantener el ritmo, sino de liderar con un propósito

Una empresa minorista líder, reconocida por adoptar la innovación tecnológica, ha mejorado continuamente la interacción con los clientes a través de experiencias personalizadas diseñadas para fomentar la fidelidad. Con varias unidades de negocio diferenciadas, la organización se propuso impulsar el conocimiento de la marca, obtener información sobre los comportamientos de gasto y ofrecer ofertas personalizadas que la diferenciaran de sus competidores en nichos de mercado. Su proceso de transformación tecnológica estuvo vinculado a la evolución del negocio, en el que la seguridad desempeñó un papel fundamental al garantizar que los controles respaldaran eficazmente las nuevas capacidades digitales.

Aunque las evaluaciones periódicas formaban parte de su rutina, los últimos avances hicieron necesario reevaluar la estrategia general. Esto incluía integrar nuevas funciones, alinear las medidas de éxito con los resultados empresariales previstos y garantizar que la estrategia se mantuviera alineada con las necesidades cambiantes. La disponibilidad del sistema era crucial para la adopción por parte de los clientes, mientras que la protección de la información de los consumidores era fundamental para mantener la confianza.

La estrategia renovada introdujo una colaboración continua con las unidades de negocio, mejoró los canales de comunicación y estableció indicadores clave de rendimiento. Entre ellos se incluían métricas de tiempo de actividad y tarjetas de puntuación de seguridad, lo que permitía identificar y mitigar rápidamente los riesgos. Este enfoque proactivo garantizó una disponibilidad óptima del sistema y reforzó la confianza de los consumidores en la marca.

A medida que las organizaciones reflexionan y se reajustan, también deben tener en cuenta cómo la madurez en la ejecución afecta a su capacidad para responder a las amenazas.

Madurez cibernética: la verdadera medida de la resiliencia

El tamaño del presupuesto no garantiza la seguridad. Las conclusiones de IDC muestran que **la madurez de los procesos es el indicador más fiable de la resiliencia**. Las organizaciones con capacidades proactivas de detección e investigación registran menos incidentes y tiempos de recuperación más rápidos.

Las organizaciones maduras realizan un seguimiento de indicadores adelantados como el tiempo de detección, las tasas de aplicación de parches y la eficacia de la formación. Estas métricas proporcionan visibilidad sobre el estado operativo y ayudan a cerrar la brecha entre la preparación percibida y la capacidad real.

Los consejos de administración exigen cada vez más pruebas de la reducción del riesgo cibernético. Sin métricas a nivel de procesos que complementen las métricas basadas en resultados, las organizaciones corren el riesgo de sobreestimar su resiliencia. La madurez real proviene de una ejecución disciplinada y una mejora continua.

Por ejemplo, una empresa de servicios financieros cambió su estrategia para dar prioridad a la medición de resultados clave alineados con objetivos específicos de mejora del rendimiento. Al analizar las amenazas desde la perspectiva del adversario, elaboraron un modelo detallado de amenazas que ponía de manifiesto las más frecuentes dirigidas a las empresas de su sector. Esta revisión exhaustiva incluía un resumen de los posibles vectores de ataque, junto con una evaluación de la capacidad de la empresa para resistir ataques de esta naturaleza.

Al recopilar datos sobre organizaciones comparables afectadas por incidentes de seguridad, el equipo de seguridad identificó patrones comunes en los tipos de ataques e integró esta información en un marco de protección prioritario para la empresa. Junto con los líderes empresariales, el equipo desarrolló niveles de servicio vinculados al rendimiento y los resultados, haciendo hincapié en las métricas para mejorar la resiliencia frente a los tipos de ataques más comunes. Este enfoque permitió una asignación específica de recursos y presupuesto a las áreas que presentaban el mayor riesgo.

El equipo de seguridad aumentó la confianza de la organización entre los miembros del consejo de administración y las partes interesadas de la empresa, al tiempo que se mejoró la eficiencia operativa gracias a una reducción significativa de los incidentes de seguridad. Este nivel de madurez se vuelve aún más crítico a medida que las organizaciones adoptan tecnologías emergentes como GenAI.

La ciberseguridad como catalizador de la innovación

Las tecnologías emergentes como GenAI están transformando las funciones empresariales e introduciendo nuevos riesgos. La ciberseguridad debe evolucionar para seguir el ritmo.

Las organizaciones deben integrar GenAI en los marcos de gobernanza, formar a los desarrolladores para que creen sistemas seguros y alinear las inversiones cibernéticas con los objetivos de transformación. La automatización, las métricas basadas en resultados y las asociaciones estratégicas serán clave para el éxito.

La ciberseguridad no se limita a la protección. Cuando se integra desde el principio y se ejecuta con madurez, se convierte en un catalizador de la agilidad, la competitividad y el crecimiento a largo plazo.

Conclusión

La ciberseguridad debe liderar, no seguir. Al integrar la ciberseguridad en el núcleo de la transformación digital, las organizaciones pueden escalar de forma segura, innovar con confianza y estar preparadas para lo que venga.

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

- **Descargue el Informe de IDC** IDC para comprender cómo los líderes en ciberseguridad están gestionando la transformación y alineando la estrategia con la ejecución.
- **Inscríbase en nuestro próximo webinar** para escuchar a nuestro equipo global hablar sobre cómo desarrollar la resiliencia cibernética.
- **Explore la herramienta** Cyber Risk Analyzer para evaluar la situación actual de su organización.

DESCARGUE EL INFORME

INSCRÍBASE EN NUESTRO PRÓXIMO WEBINAR

EXPLORE LA HERRAMIENTA CYBER RISK ANALYZER