LITORALPRESS

Fecha: 13-01-2026
Medio: La Tribuna
Supl. : La Tribuna
Tipo: Columnas de Opinión
Título: **Columnas de Opinión: El riesgo que nadie quiere ver**

Pág. : 2
Cm2: 215,9

Tiraje: 3.600
Lectoría: 14.800
Favorabilidad: No Definida

El riesgo que nadie quiere ver

Ricardo Arellano
Senior Manager Application Security
Cybertrust Latam

En el mundo de la información, datos y sistemas, solemos hablar mucho de ciberataques, ransomware y amenazas externas. Sin embargo, con el paso de los años, he llegado a una convicción incómoda: uno de los riesgos más serios para una organización no viene de afuera, sino que se construye desde adentro, silenciosamente, a través de una deficiente segregación de funciones.

La segregación de funciones no es un concepto nuevo ni sofisticado. Es, de hecho, uno de los principios más básicos del control interno. Aun así, sigue siendo uno de los más ignorados. En la práctica diaria, se diluye entre la urgencia operativa, la falta de recursos y una cultura organizacional que confunde confianza con ausencia de control.

He visto sistemas robustos, ERP de clase mundial y plataformas tecnológicas capaces de registrar cada movimiento. Pero también usuarios con permisos para crear proveedores, modificar datos críticos y ejecutar pagos sin una segunda validación real. No siempre por mala fe, sino porque "así se ha hecho siempre" o porque "no hay nadie más que lo haga".

Aquí aparece el primer gran error: creer que el control interno existe porque desconfiamos de las personas. No es así. El control existe porque entendemos que las personas se equivocan, se presionan, se cansan y, en algunos casos, ceden a la tentación. Cuando una sola persona concentra funciones críticas, el problema no es quién es hoy, sino qué podría pasar mañana.

Uno de los escenarios más peligrosos es aquel donde nunca ha ocurrido nada grave. Esa aparente tranquilidad genera una falsa sensación de seguridad. En auditoría sabemos que la ausencia de incidentes no elimina el riesgo; simplemente indica que aún no se ha materializado. Y cuando lo hace, suele ser tarde y costoso.

Más grave aún es cuando ocurre un evento y la organización no logra responder preguntas básicas: quién hizo qué, con qué permisos, bajo qué autorización. En esos casos, la falla no es solo del sistema, sino del diseño del control. Sin segregación, no hay trazabilidad confiable. Sin trazabilidad, no hay defensa posible.

Desde una mirada preventiva, la segregación de funciones no debería verse como una traba operativa, sino como una protección. Protege a la organización, pero también a las personas. Evita sospechas injustas, reduce la dependencia de individuos clave y fortalece la transparencia. Cuando no es posible segregar completamente, existen controles compensatorios. Lo que no existe es la excusa de no hacer nada.

El verdadero desafío no es técnico, es cultural. Requiere que la alta dirección entienda que el control no es sinónimo de burocracia, y que la confianza no se contradice con la verificación. Requiere aceptar que un buen diseño de accesos dice más de la madurez de una organización que cualquier discurso sobre ética o cumplimiento.

Mi opinión es clara: el riesgo en la segregación de funciones no está en su complejidad, sino en su constante postergación. Es un riesgo silencioso, invisible mientras todo funciona, pero devastador cuando falla. Y cuando eso ocurre, casi siempre alguien dice: "nadie lo vio venir". La verdad es que muchos lo vieron, pero pocos quisieron incomodarse lo suficiente como para corregirlo.