Cuando cumplir no protege: la ilusión de seguridad digital en el Estado Colombiano

En la montaña hay una regla que no aparece en ningún manual, pero que todo guía aprende, a veces demasiado tarde: no sobrevive quien más equipo tiene, sino quien mejor lee el terreno. El equipo da tranquilidad; la lectura da vida.

En los últimos días, un nuevo ciberataque a una entidad del Estado colombiano volvió a activar el mismo reflejo institucional: informes, explicaciones, cumplimiento de protocolos. La coreografía es conocida, casi ritual. Y, sin embargo, la pregunta incómoda permanece, como grieta en hielo delgado: ¿cómo es posible que organizaciones que cumplen con las normas sigan siendo vulnerables?

La respuesta es corta, pero exige coraje intelectual: porque el cumplimiento no protege. Lo que protege es la capacidad de anticipar, de decidir bajo presión y de adaptarse cuando el terreno cambia. Y esas capacidades no están en los manuales. O, mejor dicho, no viven en ellos.

Aquí aparece un error estructural que hemos normalizado: hemos confundido cumplir normas con gestionar riesgos. Cumplir es necesario —como llevar cuerdas o crampones—, pero no es suficiente. Es como tener un mapa detallado de una montaña que cambia todos los días. El mapa sirve, pero no sustituye la mirada.

El problema se agrava porque el atacante no está jugando el mismo juego. Mientras las organizaciones documentan, reportan y certifican, el atacante observa durante meses, aprende la infraestructura, identifica comportamientos y espera el momento. No cumple, no reporta, no se somete a auditorías. Opera en otra lógica. Es, en términos de montaña, alguien que no sigue el sendero: lo crea.

El ciberataque, entonces, no entra por una puerta. Se desplaza como una figura, como una geometría invisible que conecta una credencial débil, un correo mal interpretado, un proveedor expuesto y una decisión tardía. No es una línea, es una estructura. Lo que en otros trabajos he llamado la geometría del fraude: una configuración que el atacante ve completa, mientras la organización apenas percibe fragmentos.

Y luego llega el momento crítico, ese instante donde la teoría se rompe contra la realidad. Cuando ocurre el ataque, no decide el protocolo. Decide una persona. Alguien que duda, que siente presión, que no tiene toda la información y que, aun así, debe actuar. En ese punto se revela la verdad incómoda: el riesgo no es técnico. Es humano.

El cumplimiento, sin embargo, produce una sensación de control. “Tenemos políticas”, “tenemos controles”, “estamos cubiertos”. Es una tranquilidad que calma, pero también adormece. Porque desplaza la pregunta esencial: ¿somos capaces de responder a lo que no hemos previsto?

Ahí está la fractura. No en la norma, sino en la capacidad.

El problema no es la falta de regulación. Es la ausencia de pensamiento adversarial, de entrenamiento real en toma de decisiones, de aprendizaje estructurado del error y de un diseño organizacional que permita adaptarse. En otras palabras, no falta cumplimiento; falta gobernanza real del riesgo.

Esto no es un problema técnico, es un problema de concepción. Porque gestionar el riesgo en entornos complejos implica aceptar que el error no es una anomalía, sino una fuente de aprendizaje, como lo hemos trabajado en la intersección entre comportamiento, decisión y organización . Implica también reconocer que, en el momento decisivo, siempre hay alguien que firma, que se expone, que lidera la cordada, como el primero en la montaña que enfrenta el viento sin garantía de retorno.

Desde Risco & Riesgo hemos venido explorando una salida a esta trampa conceptual. No una mejora incremental del cumplimiento, sino un cambio de lógica. Lo hemos llamado GARRA —Gobernanza Adaptativa del Riesgo y Respuesta Antifrágil—. No busca que la organización cumpla mejor, sino que piense, que aprenda y que se adapte como un sistema vivo. Porque en entornos complejos, la supervivencia no depende de la rigidez, sino de la capacidad de transformarse.

Esto implica pasar de estructuras que controlan a sistemas que aprenden; de protocolos que ordenan a capacidades que responden; de jerarquías que concentran a redes que interpretan. Es, en el fondo, un cambio de ontología organizacional: dejar de verse como máquina y empezar a operar como organismo.

Al final, la pregunta no es si lo van a atacar. Eso ya no está en discusión. La pregunta es otra, más incómoda y más estratégica: cuando ocurra, ¿su organización entenderá lo que está pasando?, ¿sabrá qué hacer?, ¿y aprenderá lo suficiente para no repetirlo?

Porque en la montaña del riesgo, el problema no es no tener mapa. El problema es creer que el mapa sustituye la mirada.

.