Estrategia vs Conflicto de Intereses: Reflexiones sobre el reporte del CISO en la seguridad cibernética

mexis aggity

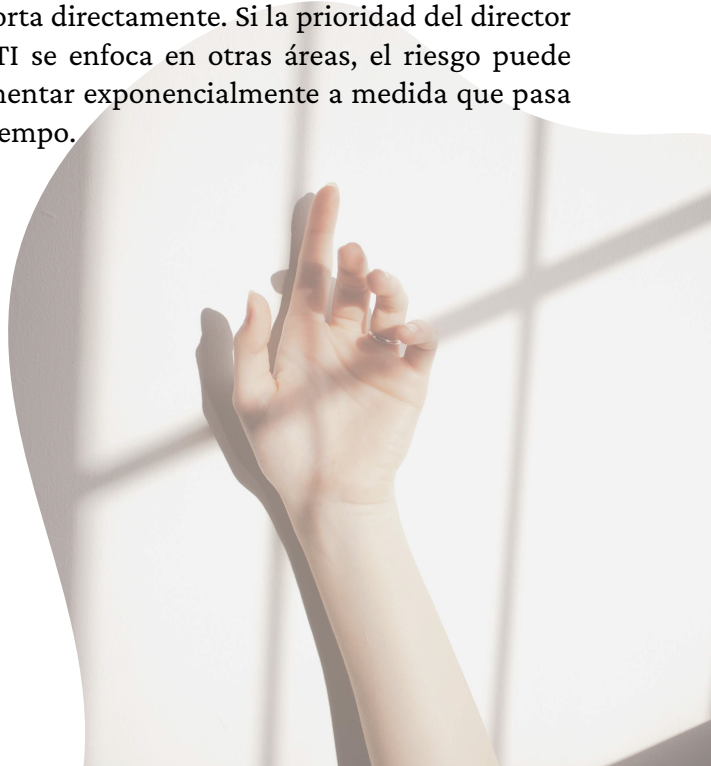
> Al final, es crucial encontrar una estructura que equilibre la necesidad de una protección efectiva y las características y requisitos propios de cada empresa: un gobierno de ciberseguridad claro y eficiente.

Hay muchas posturas y consideraciones de a quién debería reportar el CISO (Chief Information Security Officer) quien es el principal responsable de la seguridad de la información y de la ciberseguridad en una organización.

En América Latina, muchas empresas han incorporado especialistas en ciberseguridad debido a requisitos normativos, especialmente en el sector financiero, que se destaca por ser altamente regulado y maduro en temas de ciberseguridad. Esta situación ha llevado a movimientos dentro de las instituciones financieras, donde el reporte del CISO ha pasado de la tecnología al área de finanzas o contraloría, para luego llegar a la Dirección General, siempre y cuando sea aceptado por esta última. En ocasiones, el CISO se encuentra en una posición que no implica la formulación de estrategias de ciberseguridad, sino más bien actúa como intermediario entre la entidad y el regulador. Estas situaciones, sin embargo, ayudan a identificar claramente las ventajas y desventajas de la ubicación del CISO.

Es importante reconocer que no siempre se sabe dónde debería estar el CISO. Aunque la colocación del CISO bajo el área de TI o sistemas suele ser la opción predeterminada en las organizaciones, esto puede generar desventajas significativas. Existe un evidente conflicto de interés al priorizar el rendimiento y la operación de los sistemas sin considerar los riesgos asociados. Además, el presupuesto centralizado a menudo limita los recursos asignados a la ciberseguridad y promueve un enfoque técnico en lugar de uno estratégico. Quizás lo más preocupante sea la falta de independencia del CISO, ya que, si desarrolla estrategias, no podrá ser un contrapeso cuando el área de TI o sistemas se retrase en la implementación de los controles necesarios.

Imaginemos una situación en la que se realizan pruebas rutinarias de penetración según el plan establecido por el CISO, pero las vulnerabilidades no se resuelven en el tiempo estipulado. En este caso, el CISO no puede confrontar al CIO (Chief Information Officer o director de TI) ya que le reporta directamente. Si la prioridad del director de TI se enfoca en otras áreas, el riesgo puede aumentar exponencialmente a medida que pasa el tiempo.



Entonces, surge la pregunta: **¿debería el CISO reportar directamente a la Dirección General?** Permitir que el CISO le reporte al director general brinda una perspectiva más estratégica de la ciberseguridad, establece una rendición de cuentas compartida y facilita una mejor comunicación, lo que agiliza la toma de decisiones y la obtención del presupuesto operativo necesario, como mencionamos en columnas anteriores. Sin embargo, es importante considerar que esta estructura puede presentar desafíos, como la sobrecarga de responsabilidad para el CEO, las dificultades de comunicación y comprensión de los temas técnicos por parte del director general, así como la falta de experiencia estratégica del CISO.

Cuando se me pregunta a quién debería reportar el responsable de ciberseguridad, mi respuesta siempre es “depende”. Depende del tamaño de la organización, de la madurez y la comprensión de la alta dirección sobre estos temas, e incluso si existen regulaciones que ya hayan tomado decisiones al respecto.

Una forma de abordar esta situación y evitar conflictos de interés es la creación de un comité de ciberseguridad o seguridad de la información. Este comité permite la participación de los directores de la organización y, si es necesario, la incorporación de miembros externos. De esta manera, se pueden tomar decisiones informadas y presentarlas al director general o al consejo para su consideración.

Durante mis más de 6 años de experiencia en comités de ciberseguridad en diversos sectores, he aprendido la importancia de presentar resultados de manera efectiva, abogar por la resolución de vulnerabilidades críticas y fomentar la participación del director general en sesiones clave. También he trabajado para que los departamentos de Recursos Humanos y Jurídico comprendan la importancia de involucrarse en la estrategia de ciberseguridad.

En última instancia, la ubicación y el reporte del responsable de ciberseguridad pueden ser factores determinantes para el éxito en la protección de la información y la mitigación de los riesgos cibernéticos en una organización. Sin embargo, no hay una respuesta única.

Personalmente, creo que es beneficioso para el CISO ocupar una posición estratégica y evitar reportar directamente al director de TI o sistemas, ya que esto puede generar conflictos de interés. Una alternativa podría ser que el CISO reporte desde Contraloría.

No hay que olvidar la importancia del área de Auditoría para evaluar y verificar la efectividad de los controles de ciberseguridad y en algunos casos identificar estos posibles conflictos de interés.

Al final, es crucial encontrar una estructura que equilibre la necesidad de una protección efectiva y las características y requisitos propios de cada empresa: un gobierno de ciberseguridad claro y eficiente.

Autor: Andrés Velázquez
Fuente de información: forbes.com.mx