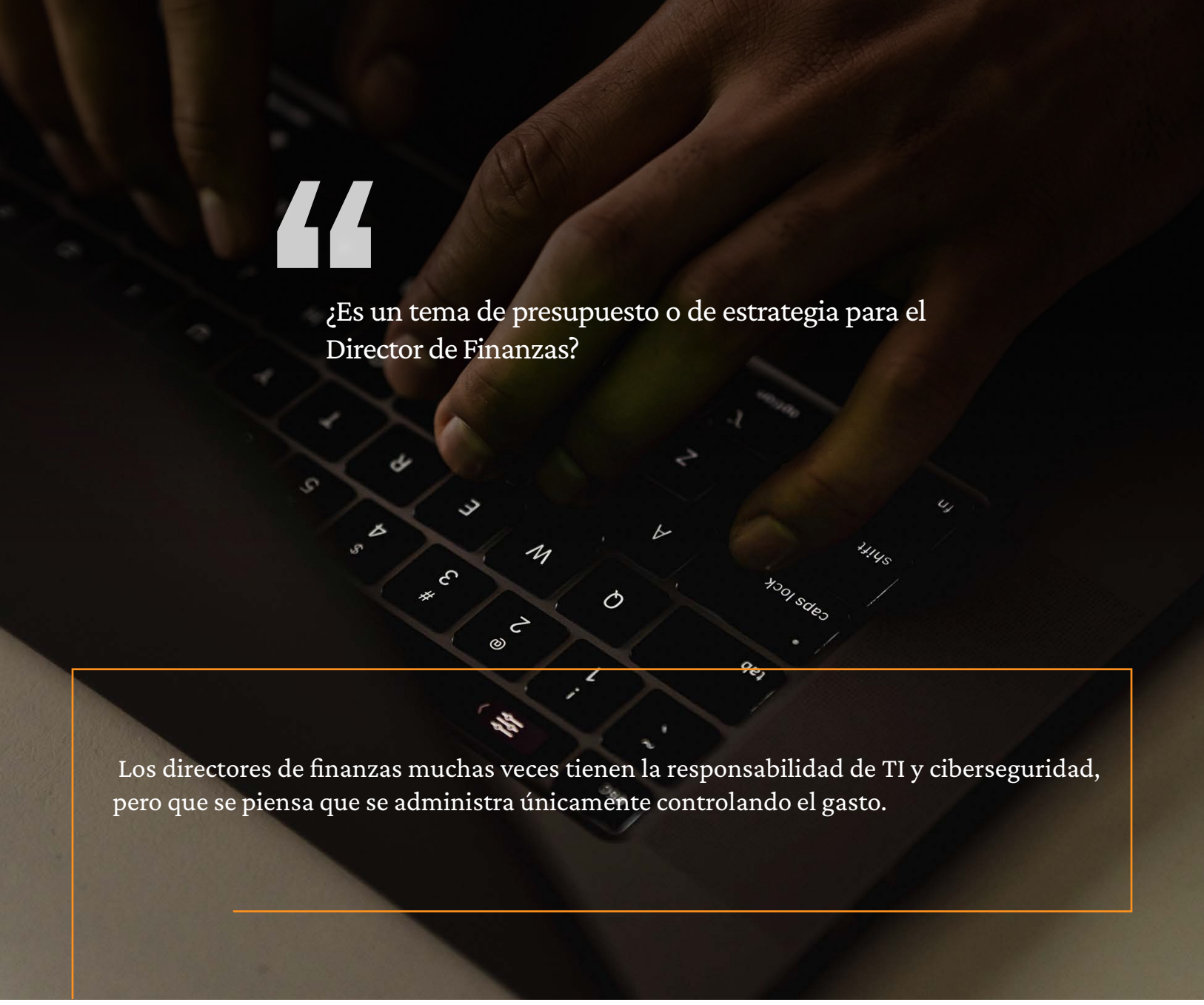
¿Cómo lograr que el CFO entienda de ciberseguridad?

nexus aggity



> ¿Es un tema de presupuesto o de estrategia para el Director de Finanzas?

Los directores de finanzas muchas veces tienen la responsabilidad de TI y ciberseguridad, pero que se piensa que se administra únicamente controlando el gasto.

El director de finanzas es una parte crítica para poder asegurar que la inversión de ciberseguridad permita proteger de los riesgos potenciales, por eso debe imitar el valor y la importancia de la infraestructura de la compañía. Dependiendo de qué tanta infraestructura tecnológica soporta los procesos críticos de la organización, será directamente proporcional a lo que se debe invertir en ciberseguridad.

Lo interesante es que la mayoría de los directores y la alta administración saben que deben invertir en ciberseguridad, el no hacerlo puede poner en riesgo su operación. Muchos están ya tratando de ver TI y ciberseguridad como algo estratégico y no operativo. Saben que deben invertir, pero no entienden cómo invertir. No habrá un retorno de inversión fácilmente identificable.

Entonces, ¿Cuánto es lo que se debe invertir en ciberseguridad?

Algunos especialistas y empresas destacan que, si la inversión en ciberseguridad es menor al 5% del presupuesto total de TI, es momento de replantear las cosas.

Se recomienda que se invierta entre un **6%** y un 14% sobre la inversión total de TI y que sea de por lo menos el **3.2%** de los ingresos anuales de la organización.

Pareciera fácil pero no lo es. Aún invirtiendo estos montos, es posible que se esté invirtiendo en proyectos independientes y no en una estrategia adecuada a las necesidades de la organización. Dando como resultado que la organización no tenga claros los riesgos tecnológicos. Esto hace que la dirección de finanzas vea entonces la inversión como una fuga de dinero.

Cuando entendemos entonces como CFO's que hay un costo por implementar ciberseguridad, tenemos que entender que el costo de no tener ciberseguridad es mayor. Que ante las nuevas amenazas y riesgos como el ransomware, el robo de secretos industriales, las estafas y todas aquellas situaciones que nos afectan la reputación de la organización es mejor estar preparados a tener que pagar los costos de recuperación tanto de gastos directos a la falta de la operación como a los indirectos para regresar a la operación (técnicos y legales).

Aun así, nos puede pasar. Incluso me atrevería a que nos va a pasar y tenemos que estar preparados financiera y operativamente.

¿Qué haremos en ese momento?

Lo más difícil es lograr eliminar la brecha entre los técnicos y los directivos, en este caso, con el director de finanzas. No hablamos el mismo lenguaje; el técnico no entiende de números y el directivo no entiende de fierros. Debemos pronto resolver esto.

El pasado 9 de marzo de 2022, la SEC (Security and Exchange Commission), el regulador en Estados Unidos propuso nuevas reglas que la Alta Administración cuente con conocimiento en ciberseguridad.

El Director de Finanzas no es un experto en ciberseguridad, pero es un especialista en riesgos. Deben hacer las preguntas correctas para poder ayudar al negocio.

El Director de Finanzas abarca todo el negocio, desde su posición o es responsable de ciberseguridad o es quien debe respaldar la ciberseguridad asegurándose que se tengan los presupuestos necesarios para poder tener un nivel aceptable de madurez en tecnología y ciberseguridad.

Hoy prácticamente todas las organizaciones tienen procesos críticos que dependen de la tecnología. La ciberseguridad es un habilitador estratégico del negocio. Esto último es lo que se llevaron los asistentes a la conferencia, esperando que ninguno de ellos regrese diciendo: "a mí no me va a pasar".

Autor: Andrés Velázquez

Fuente de información: forbes.com.mx