SEGURIDAD DE LA INFORMACIÓN · GUÍA PARA DECIDIR

Cinco preguntas que toda organización debería hacerse

Ninguna de estas preguntas tiene una respuesta técnica. Las cinco tienen una respuesta de negocio. No hace falta saber de seguridad para formularlas. Hace falta coraje para escuchar la respuesta.

01 ¿Qué información, si se hiciera pública mañana, nos costaría un cliente?

No "datos sensibles" en abstracto. Esa carpeta concreta: la lista de precios negociados, el pipeline comercial, los expedientes de personal. Si nadie puede nombrarla, es porque nadie la está cuidando en particular.

02 ¿Cuánto tiempo puede estar caído nuestro proceso más importante antes de que el daño sea irreversible?

La respuesta de negocio, no la técnica. Un banco que no procesa transacciones tres horas tiene un mal día. Uno que no las procesa tres días tiene un problema de licencia. La diferencia entre ambas cifras es toda la conversación.

03 ¿Cómo sabríamos que algo pasó?

Muchas organizaciones se enteran de un incidente porque un tercero se los avisa. Es la peor forma de enterarse: llegás tarde y además quedás expuesto ante quien te avisó.

04 ¿Quién decide cuándo un riesgo es aceptable?

La respuesta correcta nunca es "el área de seguridad". Seguridad describe el riesgo y propone opciones. Aceptarlo es una decisión de negocio, y como toda decisión de negocio, tiene un dueño con nombre.

05 Si el año cierra sin incidentes, ¿cómo sabemos que la inversión sirvió?

La seguridad que funciona es invisible. Y lo invisible es lo primero que se recorta cuando aprieta el presupuesto. Una organización madura mide la seguridad por su capacidad de resistir y recuperarse, no por el silencio.

> Si en tu organización nadie está haciendo estas preguntas, **ese es el primer hallazgo**. Y no requiere comprar ninguna herramienta. Requiere sentarse a preguntar.

Camilo Cordova Marca · Seguridad de la Información, Transformación Digital e IA
ccordova.com

#ViveLibreViveSeguro