LITORALPRESS

Fecha: 31-07-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: **“En la medida que aumente la toma de conciencia de directivos, habrá más presupuesto para proyectos de ciberseguridad”**

Pág. : 37
Cm2: 313,3

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

VITRINA EMPRESARIAL

CÉSAR PALLAVICINI Z., CEO DE PALLAVICINI CONSULTORES:

“En la medida que aumente la toma de conciencia de directivos, habrá más presupuesto para proyectos de ciberseguridad”

La Gestión de Ciberseguridad y Continuidad del Negocio van íntimamente relacionadas, afirma el también fundador de Pallavicini Consultores, empresa con más de 25 años de trayectoria brindando asesorías en Gestión de Riesgo Operacional, seguridad de la información, continuidad de negocio y derecho Informático, a clientes del sector privado y a clientes internacionales.

César Pallavicini Z., CEO de Pallavicini Consultores

“Hay dos tipos de empresa: las que ya fueron atacadas y las que serán atacadas”, afirma César Pallavicini, para quien, en consecuencia, la pregunta es: ¿su empresa tiene definida una política formal, aprobada por el Directorio, que otorgue directrices claras respecto a un ciberataque que genere una paralización total de sus procesos de negocio? ¿Y si los atacantes piden un rescate, la empresa negociará y/o pagará dicho rescate?

Ante un ciberataque con secuestro de datos, si la política es “no pagar”, ¿cuál debería ser el plan de contingencia?

Lo recomendable es tener analizados posibles proveedores de ciberseguridad, que den un buen servicio de desencriptar archivos encriptados con algoritmos robustos (más de 2048 bits), ya que los ciberatacantes utilizan lo más avanzado. Aunque es difícil, lo ideal sería tener un convenio con un proveedor para así tener un precio negociado.

Y en caso de no poder desencriptar los datos, ¿qué se sugiere?

Para abordar este tema, previamente es recomendable que se establezca una gobernanza desde la alta gerencia, formando un comité de crisis, analizando el impacto que puede tener una interrupción prolongada de uno o más procesos de negocio, donde uno de los escenarios puede ser un ciberataque, pero obviamente existen otros.

Acá es donde resulta importante tener un buen BCP (Plan de Continuidad de Negocio, PCN), ya que, a partir de un adecuado sistema de respaldo de la información de toda la compañía, se puede activar un PCN (Plan de Continuidad de Negocio). Aunque la estrategia no sea certificarse, es bueno adherirse a las mejores prácticas basadas en normas internacionales (ISO 22301 e ISO 22317).

Avances y desafíos en nuestro país

¿En Chile las empresas tienen certificaciones en estas materias?

Lamentablemente, el estado de madurez es bajo, ya que las cifras indican que menos de 200 empresas están certificadas en ISO 27001 Seguridad de la Información y cerca de 100 en ISO 22301 de Continuidad de Negocio, en Ciberseguridad, muy pocas utilizan ISO 27032 o CIS Control, y algunas están recién adoptando el Framework NIST, fuertemente utilizado en Estados Unidos y Europa.

Desde nuestra experiencia en consultoría en estos temas, vemos que producto de la presión que hace la CMF a las empresas supervisadas y ellas a los proveedores de servicios, en el cumplimiento de la Gestión de Riesgo Operacional, hay un avance e interés en certificarse.

En dicho escenario, ¿cuál es el valor agregado que Pallavicini Consultores entrega a sus clientes?

En primer lugar, tenemos una visión de Gobernanza y de cumplimiento normativo, y analizamos la Ciberseguridad como parte de la gestión de seguridad de la información, orientando a nuestros clientes en el “camino hacia una certificación ISO 27001:2022” y siempre adheridos a las normas internacionales ISO 22301, 22317, 9001, 27032, 27018, etc.

Adicionalmente, dentro de la consultoría relacionamos la gestión de riesgos operacionales, con el derecho de las tecnologías.

Respecto a la Ley Marco de Ciberseguridad, ¿ayudará al avance del país en gestionar la ciberseguridad?

Sí, se ha notado preocupación desde el sector privado, y en octubre próximo, cuando se materialice la Agencia Nacional de Ciberseguridad y tengamos la “bajada de la Ley”, seguro nos ayudará a mejorar a nivel nacional. En ese sentido, en la medida que aumenta la toma de conciencia de directivos, habrá más presupuesto para proyectos de ciberseguridad, y por ende, mayor protección de los sistemas tecnológicos para así dar cabal cumplimiento a la ley.