LITORALPRESS

Fecha: 17-12-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: **Ciberseguridad: un problema del negocio y no de la infraestructura TI**

Pág. : 16
Cm2: 545,4
VPE: $ 4.833.178

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

ANIDA
Innovación a tu medida

Ciberseguridad: un problema del negocio y no de la infraestructura TI

La primera edición del evento anual de Ciberseguridad de Anida Latam combinó el marco normativo y legal que impacta a las organizaciones y casos concretos de fuga de información que han generado grandes incidentes y accesos no autorizados en entidades hasta ahora desconocidas.

Santiago, 21 de noviembre 2024.- "El Robo del Siglo puede ser Digital", así se denominó la primera edición del evento de Ciberseguridad de Anida Latam, enfocado en los desafíos que el marco legal y normativo trae a las organizaciones, a propósito de la nueva Ley de Protección de Datos Personales y de la Ley Marco de Ciberseguridad. Además, contó con un panel de expertos en ciberseguridad quienes coincidieron en las necesidades estratégicas de las organizaciones para abordar las amenazas cibernéticas.

Fernando Fernández, socio fundador de Alt Legal y especialista en derecho y tecnologías de la información, planteó que existen grandes sesgos cognitivos en las organizaciones, que juegan en contra de la ciberseguridad y la protección de datos: "Efecto de Arrastre: todo el mundo lo hace así", "Atribución Fundamental: sino nos ha pasado nada es porque lo estamos haciendo bien", "Sobre Optimismo: a mí no me va a pasar" y "Observación Selectiva: como no lo veo físicamente no merece mi preocupación".

En concreto "el gran problema de la ciberseguridad es que no se percibe de la misma manera que la seguridad física (como dejar abierta la puerta de la casa), y al ser humano le cuesta adoptar medidas para proteger bienes inmateriales porque no visualiza que las consecuencias de su pérdida pueden ser incluso mucho más graves", asegura Fernández.

"Los departamentos TI están profundamente solos"

Para poder dar un cambio en la percepción de la ciberseguridad, Fernández enfatiza en: la necesidad de subir el tema a los directorios, promover la gestión de cambio con la experiencia comunicacional de los equipos de recursos humanos, contar con la asesoría de los hackers éticos y contratar tecnologías que se adecuen a las necesidades de las empresas.

"Los departamentos TI están profundamente solos y es un área muy incomprendida" y la ciberseguridad "al tener un carácter estratégico debe subir hacia los directores, pero también supone un proceso de gestión de cambio" asegura Fernández.

Los expertos coinciden que el fortalecimiento institucional para los temas de ciberseguridad requiere no solo de un nivel estratégico sino táctico "eso significa tener políticas claras y estar preparados en el contexto propio de tecnología y de las personas" mencionó, Juan Carlos Lanas Ocampo, director general de tecnologías en la Universidad Técnica Federico Santa María, quien destaca la importancia del rol de los liderazgos en ciberseguridad y en el desarrollo, retención y fortalecimiento de los talentos.

La responsabilidad de los directivos ante la nueva Ley

Con la nueva Ley de Protección de Datos Personales, las empresas enfrentan varios desafíos y uno de ellos es que tendrán 24 meses para prepararse "a diferencia de lo que pasó en los países de la Comunidad Europea, quienes hoy cuentan con una ley avanzada en términos de protección de datos, es que ellos ya tenían regulaciones antiguas y habían avanzado" manifestó Carolina Pizarro, fundadora de la Red de Mujeres en ciberseguridad en Chile.

Pizarro explica que con esta nueva Ley prácticamente las empresas no tienen una experiencia previa para su implementación, por lo que 24 meses no es mucho tiempo para identificar dónde está el dato "Nosotros empezamos desde 0 porque no tenemos una ley previa ajustada a los nuevos tiempos y en este sentido observamos que muy pocas empresas tienen un área de gobierno de datos, a veces, ni siquiera tienen identificado dónde tienen el dato".

Las empresas que entregan información de sus clientes a proveedores externos serán las responsables de recibir el castigo en caso de que sus proveedores incumplan la ley "si el proveedor filtra alguna información, no es el proveedor el responsable del dato, por tanto es la empresa la que será castiga con multas que representan hasta 4% de la venta anual" asegura.

Tus credenciales son mías

En medio de la discusión normativa surgen interrogantes como ¿hasta qué punto tus credenciales son realmente de tu propiedad? Pese a que muchas empresas han adoptado procedimientos y políticas para el resguardo de los datos de las personas, esto no implica que los datos realmente están seguros.

Durante La primera edición del evento anual de Ciberseguridad de Anida Latam, Felipe Hott Delgado, CEO de Trusttech Cybersecurity y partner de la estrategia de Ciber Seguridad de Anida Latam presentó diferentes casos de fuga de información tanto en Chile como la región, que han generado importantes incidentes y accesos no autorizados.

Hott no solo evidenció algunos ejemplos significativos de vulneración de datos, sino que entregó cifras relevantes desde su trabajo como hacker ético, "en los últimos 6 meses hemos podido recuperar más de 250mil URL´s únicas correspondientes a Chile, con sus respectivas credenciales. Lo que es más grave es que nada tiene doble factor o factor de verificación". Dentro de las principales URL´s expuestas corresponden a credenciales bancarias, claves únicas, entre otros "que incluye cualquier sector que ustedes se puedan imaginar".

La necesidad de un cambio cultural

Aún el ciudadano común no ha concientizado la importancia de sus datos, así lo explica Fernández "uno de los grandes problemas que tenemos como personas es que nosotros entregamos nuestros datos sin saber para qué lo están usando y cuáles son las consecuencias de eso, estamos todo el día subiendo información en las redes sociales y no sabemos en qué manos pueden llegar a caer".

Por su parte Pizarro, añade que "debemos dejar de normalizar que nos pidan nuestro número de rut, por un descuento o por fidelidad a una marca" y para esto es necesario un cambio cultural.

El apoyo de las tecnologías en la ciberseguridad

Las empresas hoy deben enmarcar sus desafíos operativos y competitivos dentro de las normativas vigentes "un desafío para el cual Anida Latam está preparado porque la ciberseguridad es hoy nuestro pilar para asegurar la continuidad operativa de las empresas" resalta Adolfo Tassara, gerente general de Anida Latam.

"El marco normativo no solo impacta a las empresas, sino que demanda del desarrollo de estrategia para lo cual contamos con las capacidades para desarrollarlas" manifiesta Mario Martínez, gerente de comercial de Anida Latam.

En definitiva, las normativas legales vigentes en conjunto con el advenimiento de las tecnologías emergentes traerán consigo desafíos para las organizaciones, las personas y las futuras generaciones.