CHILETECNOLÓGICO
30/05/2025 Audiencia: 320.543 Sección: SOCIEDAD
$6.931.821 Tirada: 126.654 Frecuencia: SEMANAL
$20.570.976 Difusión: 126.654
ada: $20.570.976 Ocupación: 33,7%

PANEL 6

FALTA CONOCIMIENTO DE LA NUEVA NORMATIVA:

Resiliencia e información son claves para proteger los datos

Aunque la entrada en vigencia de la Ley de Protección de Datos Personales todavía no se vea tan cercana, los expertos coincidieron en que las empresas no deben perder tiempo, elaborar un plan de acción, ser proactivas, incorporar herramientas tecnológicas y avanzar en la implementación de las medidas reglamentarias, incorporando a todas sus áreas.

HYPO PHOTOS

ALEXIS IBARRA, periodista de Vida, Ciencia y Tecnología de "El Mercurio", moderó el panel integrado por Vicky Guerra, Romina Garrido, Germán Rodríguez y Felipe Harboe.

BÁRBARA LICHNOVSKY

Hoy las empresas chilenas, grandes y pequeñas, enfrentan desafíos cruciales. Uno de ellos es el cumplimiento de la nueva Ley de Protección de Datos Personales, la cual entrará en vigencia el 1 de diciembre de 2026. Entre otras cosas, la normativa obliga a las organizaciones a hacer auditorías para identificar cómo se gestionan y clasifican los datos personales e implementar medidas tecnológicas para garantizar la seguridad de la información.

Según Felipe Harboe, socio principal H&Co Abogados, existe un gran desconocimiento de los estándares que exige la ley. "Es necesario que las *startups* y todas las innovaciones conozcan la nueva legislación para evitar que después caigan en un riesgo infraccional. La norma habla incluso de multas que van hasta un 4% de las ventas anuales", explicó.

El tema se abordó en el panel "Blindaje digital: protegiendo tus datos y tu negocio", parte del Summit Cybertech South America 2025, realizado en "El Mercurio", y que contó también con la presencia de Vicky Guerra, *specialist manager in cybersecurity, compliance and DPO* de Advansolution; Romina Garrido, directora de Protección de Datos de Prieto Abogados, y Germán Rodríguez, *chief technology officer* (CTO) de Tenpo. Todos ellos entregaron consejos para que las empresas puedan blindarse digitalmente contra los ciberataques.

Es fundamental partir con un diagnóstico en la organización: qué datos, dónde y cómo los tiene. Muchas empresas no conocen realmente esas respuestas.

PARTIR CON LOS USUARIOS

Según Vicky Guerra, una de las claves para protegerse es la resiliencia operacional, lo que implica que toda organización debe contar con un plan de acción para responder a incidentes y realizar simulaciones para verificar que funcione. Agregó que el blindaje digital debe partir con los usuarios. "Todos debemos tener esa visibilidad respecto de dónde vienen los ataques. Muchas veces no lo sabemos (pueden venir desde el interior de la empresa), pero si no tenemos claridad de que tenemos que cuidarnos para poder empezar a implementar o a concientizar desde adentro de la organización, obviamente va a ser bastante difícil", afirmó.

Para Germán Rodríguez, la ciberseguridad se ha convertido en un problema estratégico para todas las compañías y ya no se basa solamente en capacidades reactivas. "Históricamente, nos preparamos para reaccionar lo más rápido posible cuando detectábamos algún tipo de amenaza. Desde hace algún tiempo, casi todas las empresas estamos trabajando en capacidades proactivas, en entender un problema antes que suceda", señaló. Ello implica crear equipos de ingeniería que buscan detectar patrones de ataque nuevos, preocuparse por lo que sucede en la cadena de valor y establecer controles sin friccionar la experiencia del cliente.

Por otra parte, Rodríguez enfatizó en que para lograr el blindaje digital es clave la consistencia, "un apetito muy alto de estar alerta, de entender que puede pasar y de cómo me preparo en el caso de que ocurra, para reaccionar lo más rápido posible y ser resiliente".

A ello, el ejecutivo sumó el uso de tecnologías como la inteligencia artificial (IA), que potencia capacidades, permitiendo mayor eficiencia sin necesidad de una gran inversión en equipos. Pero Vicky Guerra advirtió que hay que usar el criterio personal a la hora de utilizar la IA: "Es una herramienta que viene a complementar, pero hay que saber preguntarle para que dé una respuesta acertada. Potencia tus capacidades, pero no se puede confiar cien por ciento", dijo.

IMPORTANCIA DEL DIAGNÓSTICO

Por su parte, Romina Garrido afirmó que las empresas tienen que blindarse contra la desinformación, adoptando estrategias diversas para la protección de datos, en vista de la entrada en vigencia de la nueva ley. Y que si bien hay compañías como bancos y aseguradoras que ya están en proceso de implementación, es importante que las demás organizaciones hagan un diagnóstico y empiecen cuanto antes con la adecuación. "Esta es una ley que no penaliza tener datos, pero hay que justificar y comprender su uso y eso es muy laborioso dentro de un proceso de consultoría e implementación", dijo.

Felipe Harboe coincidió en la necesidad de hacer un diagnóstico. "Las preguntas claves que hay que hacerse son qué datos tengo, dónde los tengo y cómo los tengo. Deben ser respondidas adecuadamente y, por lo general, las organizaciones no saben lo que tienen ni dónde lo tienen", señaló. Una evaluación que —estimó— demoraría entre uno y dos meses, dependiendo del tamaño de la empresa. A ello se suma la adecuación, la cual tomaría entre cuatro y doce meses según el volumen de la compañía, la criticidad de los datos y las brechas que se encuentren.

Por último, Garrido subrayó que existen desafíos legales y gubernamentales para la puesta en marcha de esta normativa en las empresas. El primero es la excesiva confianza de que creer que su implementación se soluciona solo con abogados. "Esto es un desafío transversal, es tecnológico, es de seguridad, es de gobierno de datos y es del área legal, de cumplimiento normativo", afirmó. A ello se suma que aún no existe un organismo coordinador para la ley, lo que genera incertezas sobre la manera de implementarla.