LITORALPRESS

Fecha: 30-04-2025
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: **Detección y prevención, claves para una ciberseguridad exitosa**

Pág. : 3
Cm2: 306,1

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

COLUMNA DE OPINIÓN

Detección y prevención, claves para una ciberseguridad exitosa

NÉSTOR STRUBE, GERENTE GENERAL DE ITQ LATAM

En Chile, muchas organizaciones aún basan sus políticas y medidas de ciberseguridad en la capacidad que tengan para dar respuesta y recuperarse ante un ciberataque, para contener y eliminar amenazas, cayendo en un escenario desfavorable donde las acciones y medidas son esencialmente reactivas y pueden causar mayores impactos, como altos costos económicos y materiales, además de continuidad operacional, daño a la imagen y prestigio.

Es urgente comprender que los costos de reaccionar a los impactos son mucho más altos en comparación con la inversión preventiva que se podría haber realizado en el proceso de ciberseguridad. Así, tenemos aún el gran desafío de reforzar políticas y estrategias que consideren la prevención como piedra angular en esta materia.

En efecto, la ciberseguridad tiene que ser entendida como un proceso continuo, que requiere adaptación y previsualización; que se aborda por capas, con una mirada integral y una estrategia de ciberdefensa en profundidad. Es un *must* para toda mesa directiva o gerencial empatizar con esto a fin de conseguir un proceso de ciberdefensa que incluya fuertes medidas preventivas y de detección temprana, lo que será clave para un resultado exitoso.

Lo anterior, porque no basta con tener tecnologías reactivas (por vanguardistas que sean), de alta capacidad de recuperación; tampoco una alta capacidad para operarlas. Una ciberamenaza puede haber logrado su objetivo, de daño e impacto, antes de ser detectada. De ahí la necesidad de prevenir y anticipar tempranamente, a nivel interno, con políticas de prevención abordadas integralmente en tres dimensiones: tecnología, procedimientos y personal concientizado.

No obstante, la prevención en la estrategia de ciberseguridad de las organizaciones abarca mucho más que lo interno. Esta debe unirse al ecosistema externo que rodea a la empresa, lo que se conoce como cadena de suministro, integrada por proveedores, socios de negocios y clientes. Aquí, lo relevante es que todos aquellos actores que interactúan con las plataformas de la compañía estén en sintonía en sus políticas integrales de ciberseguridad. El alineamiento y trabajo conjunto con ellos es clave en la estrategia preventiva de ciberseguridad.

Adicionalmente, es crucial tener presente que el nivel de especialización y técnicas utilizadas por el cibercrimen evolucionan constantemente, con ingeniería social cada vez más desarrollada y sofisticada, utilizando inteligencia artificial y logrando, por ejemplo, niveles de suplantación de identidades que son muy difíciles de detectar. De manera tal que, constantemente, busca el eslabón más débil de la cadena de suministro para lograr el daño a la organización.

Peor aún, la ciberdelincuencia se complementa con "especializaciones" de ataques por industria, con ciberataques específicos para los sectores financiero, *retail*, educación, instituciones públicas, FF.AA., transportes, *utilities*, energía y minería. Claramente, la prevención en cada uno de estos tiene que tener matices y diferencias.

Con todo, lo cierto es que en Chile, como país, existen ya niveles de conciencia ascendentes en cuanto a prevención en ciberseguridad. Buscamos prepararnos cada vez mejor, contando hoy con importantes normativas y leyes, como lo es la ley marco de ciberseguridad y la ley de protección de datos personales; ambas incluyen, de hecho, la prevención como un ámbito primordial en materias de ciberseguridad. Ahora, es de alta relevancia a nivel país que las organizaciones públicas y privadas den alta prioridad, refuercen y consoliden la prevención en su estrategia de ciberseguridad.

> **"La ciberseguridad tiene que ser entendida como un proceso continuo, que requiere adaptación y previsualización; que se aborda por capas, con una mirada integral y una estrategia de ciberdefensa en profundidad".**