DF
DIARIO FINANCIERO®
SUPLEMENTO
SANTIAGO DE CHILE
JUEVES 28 DE JULIO DE 2022

CIBERSEGURIDAD

LOS CAMINOS QUE ABRE LA NUEVA LEY DE DELITOS INFORMÁTICOS

Revisar los alcances de los programas de cumplimiento en las organizaciones es una de las oportunidades que abre la Ley N° 21.459 de delitos informáticos, que está llevando a las empresas a adaptar políticas y nuevos instrumentos legales.

POR FABIOLA ROMO P.

La nueva normativa en delitos informáticos, promulgada el mes pasado, vino a actualizar una ley con cerca de 30 años de vigencia, que ofrecía ciertas limitaciones en el ámbito de los tipos penales regulados y las herramientas que brindaba para poder investigar los delitos asociados a ciberseguridad. Su actualización impone nuevas responsabilidades, tanto en la forma en que se obtienen los datos, como en la manera en que se procesan. Y además, se ajusta a los tiempos que corren, en un mundo cada vez más digitalizado.

Cristopher Reyes, gerente de Enterprise Risk de Consultoría de EY, destaca que la nueva ley considera los sistemas donde se almacena y resguarda esa información, lo que se traduce, por ejemplo, en las debidas revisiones sobre el origen de los datos que procesa una empresa. "Ello requiere necesariamente de capacidades tecnológicas y de ciberseguridad, así como legales y de cumplimiento, para abordar íntegramente los desafíos", acota el especialista.

Para Gabriel Quiroga, gerente general de WSecurity, sin duda, la Ley N° 21.459 representa un avance en materia de ciberseguridad, acorde a los nuevos desafíos y necesidades que implican la transformación digital y el avance de la tecnología. "Esta ley desincentivará a los ciberdelincuentes, garantizando la continuidad operativa de las organizaciones y la protección de su información, además de otorgar a las empresas mecanismos legales para la persecución de dichos delitos", afirma.

En tanto, Camilo Mix, analista en Ciberinteligencia de CronUP Ciberseguridad, valora la posibilidad de poder establecer acusaciones y sanciones contra aquellas personas que resulten ser responsables. "Además, es una oportunidad para ir modernizando una legislación que pecaba de varias falencias, considerando el actual contexto tecnológico y establece también un marco para seguir debatiendo otros conceptos muy importantes ligados a la ciberseguridad, como el rol del hacker ético, por ejemplo", argumenta.

Adecuar políticas e instrumentos que no tengan un correlato con procesos y sistemas informáticos, probablemente, sea insuficiente para hacer frente a los nuevos delitos, afirma Cristopher Reyes, de EY.

El auge del cibercrimen

En los últimos años, la ciberseguridad se ha transformado en una prioridad de los países, de cara a prevenir y detectar tempranamente el aumento sostenido de los delitos informáticos. "Por eso Chile ratificó el convenio de Budapest sobre la ciberdelincuencia del Consejo de Europa", enfatiza Miguel Moreno, gerente comercial de Btres, sobre el instrumento al que adhirió el país en 2017.

En este contexto, Hugo Galilea, director de la Alianza Chilena de Ciberseguridad, destaca la incorporación del artículo 3° de la ley 20.393, que establece responsabilidad a dueños, controladores, ejecutivos principales, representantes, y a quienes realicen actividades de administración y supervisión. "Se podría esperar un cambio sustancial en la concientización e importancia que se le otorga a los delitos informáticos", comenta.

Ocho puntos clave

En resumen, Mauricio Espinoza, gerente comercial de ITQ Latam, enumera los ocho comportamientos que la nueva norma tipifica como delitos informáticos, eliminando a la ley 19.223:

- Ataque a la integridad de un sistema informático.
- Acceso ilícito.
- Interceptación ilícita.
- Ataque a la integridad de los datos informáticos.
- Falsificación informática.
- Receptación de datos informáticos.
- Fraude informático.
- Abuso de los dispositivos.

Otro punto interesante, a ojos del ejecutivo, es la posibilidad de que se puedan realizar interceptaciones de comunicaciones telefónicas, fotografías, filmaciones u otros medios de reproducción de imágenes como evidencias para un esclarecimiento de los hechos vinculados a delitos informáticos.

PUBLIRREPORTAJE

SONDA:

¿Qué es Zero Trust y por qué es la clave para una transformación digital eficiente?

Carlos Bustos H., Director Regional de Servicios de Ciberseguridad en SONDA.

Las **estrategias Zero Trust (ZT)** componen un marco de seguridad fundamental para la transformación de las organizaciones ya que, a partir de un enfoque defensivo integral, clasifican de por sí a todo usuario y/o dispositivo como una posible amenaza activando un protocolo de protección y verificación avanzada de credenciales. A través de este proceso se resguarda la integridad de los datos y activos digitales de la empresa ante amenazas dentro o fuera de su red, mitigando impactos y mejorando la toma de decisiones estratégicas.

Estas estrategias están centradas en la visión íntegra del entorno digital, i**dentificando usuarios, aplicaciones, dispositivos, puntos de conexión, red, datos e infraestructura.** A partir de esto, es posible enfocarse en la automatización de acciones y respuestas ante ciberataques y analítica avanzada de la información.

Hoy, son cada vez más las organizaciones que requieren de un **modelo de seguridad ágil y responsiva a las complejidades del entorno moderno**, que se adapte a las necesidades de conexión remota y escenarios híbridos de trabajo, junto con garantizar la **operatividad, productividad, experiencia y usabilidad** a sus colaboradores y usuarios, además de una integración eficiente a los ambientes cloud, cerrando toda brecha de seguridad y minimizando riesgos y vulnerabilidades.

En síntesis, se trata de una iniciativa defensiva que previene brechas de información al eliminar el concepto "confianza" dentro de la arquitectura de red de una organización. Básicamente, "no se confía en nadie hasta que se pruebe lo contrario".

Si bien los proyectos Zero Trust se pueden desarrollar dentro de una arquitectura tradicional, es necesario enfocarlos a todos los procesos de la organización, priorizando una implementación por fases, planificada y ejecutada en forma correcta, que vele por una mejor adopción, experiencia de usuario y operatividad de la organización.

En este sentido, en SONDA lideramos la transformación digital de la región, a través de la consolidación de un amplio portafolio de soluciones y servicios de Ciberseguridad. En la actualidad, trabajamos en conjunto con los principales referentes tecnológicos a nivel mundial, para garantizar los más altos estándares de calidad y una óptima asesoría en el camino hacia la transformación digital de tu organización, junto con la adopción y desarrollo de estrategias de prevención Zero Trust más eficientes del mercado y acordes a los desafíos de hoy.

EFECTIVIDAD Y SEGURIDAD: LA IMPORTANCIA DE LAS ESTRATEGIAS ZERO TRUST

Capacitar a profesionales y organizaciones, junto a la adopción de modelos y herramientas necesarias para un ciberataque, son los puntos que destacan los expertos para lograr un modelo efectivo de ciberseguridad

POR PAULINA SANTIBÁÑEZ T.

Actualmente, solo un 5% de las empresas en el mundo cuenta con una estrategia de seguridad confiable y efectiva. Esto podría explicar que, según un informe de la consultora Accenture, solo el año pasado se hayan producido alrededor de 400 millones de ataques a empresas de Chile.

Para Camilo Mix, analista en Ciberinteligencia de CronUp Ciberseguridad, este hecho es preocupante y demostraría que, independiente del sector, las organizaciones "no se encuentran preparadas para afrontar un ataque informático, o no saben cómo afrontarlas de manera proactiva, durante o después de un incidente".

Esta preparación solo llegaría si las empresas logran anteponerse a cualquier situación de peligro. "Una estrategia de seguridad efectiva es aquella que asume que un ataque puede ocurrir en cualquier momento, sin importar los controles o herramientas que se tengan", explica Gustavo Mármol, CSOC manager de Arkavia Networks.

Confianza Cero

Bajo el ideal de "no confiar nunca y verificar siempre", como plantea Mármol, Zero Trust es uno de los modelos favoritos de las organizaciones.

"Es un enfoque estratégico de la ciberseguridad que protege a una organización al eliminar la confianza implícita y validar continuamente cada etapa de una interacción digital", explica Mauricio Espinoza, gerente comercial de ITQ Latam.

Según el experto, este modelo tiene un enfoque holístico y estratégico de la seguridad que "garantiza que todos y cada uno de los dispositivos con acceso sean quienes dicen ser".

Un modelo que además tiene la ventaja de que, al ejecutarlo, el impacto en la experiencia de usuario es mínima, añade Gustavo Mármol.

"El sistema no confiará en tu identidad, sin antes verificar -en base a diferentes procesos- que en verdad eres tú y cuáles son tus atribuciones y limitantes", proceso que dificulta el trabajo de los atacantes de las organizaciones, agrega Camilo Mix.

Todos son parte

El líder de Ciberseguridad de Accenture Chile, Claudio Ordóñez, explica que para enfrentar estas crecientes amenazas se necesita ejecutar cambios que abarquen a toda la organización.

"Es necesario un cambio profundo en la forma en que la ciberseguridad se planifica y ejecuta en las empresas. Los CEOs no deberían dejar este cambio únicamente en manos de los equipos de TI. Por el contrario, deben liderar el cambio", detalla Ordóñez.

Para Camilo Mix, una de las mayores fallas que existen en las empresas es "no establecer un proceso de formación y capacitación de seguridad informática al personal interno y externo".

Para la funcionalidad de programas cibernéticos eficientes, Ordóñez señala que los ejecutivos centrados en la seguridad (CIOs) necesitan "cultivar un profundo conocimiento de las operaciones críticas de la empresa y contar con una compresión horizontal de las funciones que requieren la mayor atención y protección".

Por eso, Gustavo Mármol enfatiza que las empresas deben apuntar al reclutamiento de profesionales capacitados, así como también a entregar el constante entrenamiento que este tema requiere y a generar políticas de retención de talento.

GRUPO DF

DF · DFLIVE · MAS · ED · BAZARED

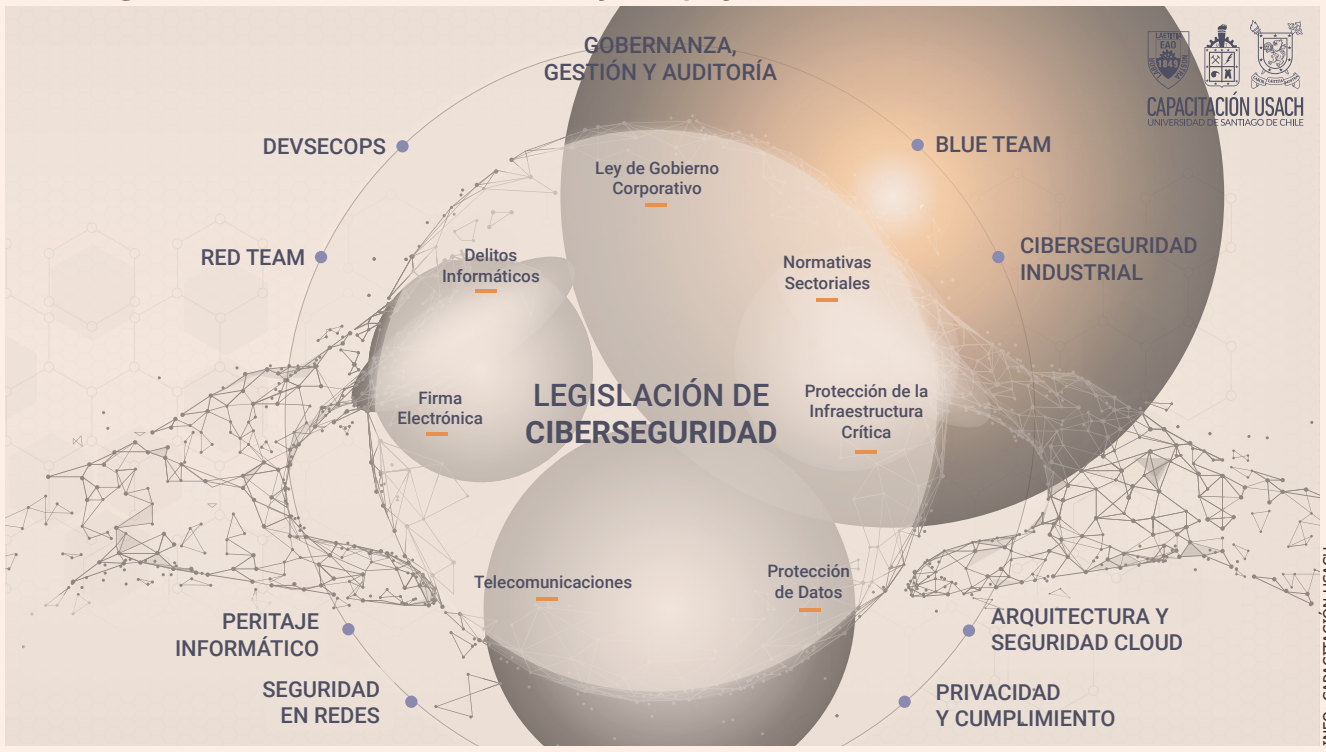
Directora: Marily Lüders / **Subdirectora:** Teresa Espinoza / **Gerente Comercial:** José Ignacio De la Cuadra / **Editora:** Claudia Marín / **Director Creativo y Arte:** Rodrigo Aguayo / **Coordinadora:** Marcia Aguilar / **Dirección** Edificio Fundadores, Badajoz 45, pisos 10 Las Condes, Fono: 23391000 / e-mail: buzondf@df.cl / **Impreso por** COPESA IMPRESORES S.A., que sólo actúa como impresor.

EXPERTOS DE CAPACITACIÓN USACH COMPARTEN SUS DIAGNÓSTICOS:

Nueva Ley de Delitos Informáticos actualiza a Chile y refuerza el desafío de la especialización en Ciberseguridad

La creciente sofisticación de los ciberdelitos hace cada vez más necesario potenciar la especialización de capital humano en este ámbito en Chile.

Ciberseguridad: Un ecosistema dinámico y complejo



INFO: CAPACITACIÓN USACH

La Ciberseguridad exige una legislación moderna y, como consecuencia de ello, capital humano en permanente actualización.

Con la creciente sofisticación de los ciberdelitos, cada vez más necesario potenciar la especialización de capital humano en este ámbito en Chile.

El 20 de junio de este año ha marcado un hito de suma relevancia en el ámbito de la ciberseguridad, con motivo de la publicación de la Ley 21.459 de Delitos Informáticos. Este nuevo cuerpo legal ha incorporado una serie de mejoras, entre las que destacan: una visión más contemporánea a ciberdelitos con respecto a la derogada Ley 19.223, incorporando nuevos ciberdelitos no contemplados previamente, dotando a los organismos investigadores de nuevas atribuciones y ampliando el alcance de la Responsabilidad Penal de las Personas Jurídicas.

Los ciberataques evolucionan, exigen respuestas nuevas y, por tanto, un capital humano a la altura del desafío. Fernando Soto, director comercial de EFUSACH, destaca al respecto: "Por la naturaleza crítica para el funcionamiento de organizaciones, instituciones y empresas, potenciar la formación de capital humano en esta materia debe ser asumido como un desafío país. En ese sentido, Capacitación USACH cuenta con una robusta oferta de programas de formación en Ciberseguridad, recogiendo los vertiginosos cambios".

La incorporación de la Receptación de datos informáticos y del Fraude Informático como delitos informáticos "es algo que se hacía muy necesario, específicamente en lo relativo a conductas que debían ser cubiertas con las antiguas figuras de estafa del Código Penal y otras que simplemente no eran delito", señala Felipe Sánchez, docente del Diplomado de Blue Team de Capacitación USACH y especialista en Peritaje Judicial, Fraudes y Delitos Informáticos.

Con la ampliación del alcance de la Responsabilidad Penal de las Personas Jurídicas, las empresas podrán ser responsables penalmente por delitos informáticos que le generen una ventaja o beneficio y que sean cometidos por personal que se encuentre bajo su dirección y supervisión. Felipe Sánchez complementa: "Por ejemplo, podrían ser condenadas empresas que realicen marketing por contacto directo a personas, cuyo origen de los datos utilizados sea ilícito, sin poder apelar al desconocimiento de su origen, así como también empresas de ciberseguridad que para demostrar sus habilidades técnicas accedan a sistemas informáticos sin contar con la debida autorización".

La prueba de delitos informáticos requiere de la incorporación y articulación transversal de buenas prácticas de ciberseguridad en el ámbito de la ciberdefensa, la respuesta a ciberincidentes y una investigación forense digital con un correcto tratamiento de las evidencias digitales, donde nada puede quedar al azar ni a la improvisación. Para lograr éxito en ello, algunas de las condiciones más primordiales son: competencias y experiencia del personal, actuar con independencia garantizada, utilización de equipamiento y tecnologías especializadas, procedimientos formales y calidad de los registros digitales existentes. "Estos aspectos marcarán una gran diferencia respecto de los resultados a obtener en una investigación forense digital y su respectivo aporte en procesos judiciales, investigaciones internas y respuesta a ciberincidentes complejos", añade Felipe Sánchez.

Capacitación para los nuevos tiempos

Capacitación USACH es el organismo técnico de capacitación de la Universidad de Santiago de Chile, y pertenece a Empresas y Fundaciones USACH (EFUSACH). Su misión es articular el conocimiento que genera el quehacer académico de la universidad con el mundo productivo, tanto a nivel nacional como regional. En ese marco, y atendiendo a las nuevas tendencias en el ámbito de la formación, Capacitación USACH cuenta con una completa aula virtual.

Para más información: educacionejecutiva@usach.cl

Sin duda que aún existen muchos desafíos pendientes en la legislación en ciberseguridad en nuestro país. No obstante, se han dado importantes pasos en materias como Protección de Datos, Protección de Infraestructura Crítica y Operadores Esenciales, a lo que se suma el establecimiento de regulaciones sectoriales en los sectores Financiero, Eléctrico, Pensiones, entre otros.

Con la nueva Ley de Delitos Informáticos, cada empresa tiene la obligación de evaluar los riesgos particulares a los cuales se encuentra expuesta desde la perspectiva del compliance penal, asociados a los delitos informáticos. Esto, de modo que les posibilite actuar de manera diligente con objeto de identificar y potenciar los controles que mitiguen dichos riesgos.

En un escenario crecientemente complejo en materia de ciberseguridad, Chile ha logrado importantes avances en el combate contra la ciberdelincuencia, lo que también implica responsabilidades, tales como estar preparados para enfrentar ciberataques cada vez más sofisticados, siendo la especialización del capital humano uno de los grandes desafíos.

AUMENTAR LA PARTICIPACIÓN FEMENINA: CLAVE PARA LA PRODUCTIVIDAD E INNOVACIÓN

En TI, y especialmente el rubro de ciberseguridad, hay actualmente un gap de capital humano. En una industria donde la participación femenina es baja, son ellas quienes están frente a una oportunidad de oro, no solo por el déficit de personal, sino también para dinamizar los equipos. POR AIRAM FERNÁNDEZ

En 2021, las mujeres representaban solo el 15% de la fuerza laboral en el ámbito de la seguridad cibernética, según datos de la Alianza Chilena de Ciberseguridad. El panorama no ha cambiado en lo que va de año, confirma Karin Quiroga, directora ejecutiva de esta iniciativa. Pero tanto ella como otros actores de la industria coinciden en que aumentar la participación femenina es un tema asumido y del que están conscientes.

Quiroga destaca el impulso de iniciativas en ámbitos de gobierno, organizaciones y educación para generar acciones concretas y lograr los cambios necesarios. Pero releva la necesidad de sumar a más mujeres a formarse en áreas STEM, pues, al final, esta es la barrera detrás de las cifras de la baja presencia femenina.

¿Puede marcar alguna diferencia en la industria el hecho de que más mujeres se sumen? Hay consenso en que sí.

Para Quiroga, la importancia de esto no radica en diferencias de habilidades o capacidades. Pero sí "en que contribuyen a generar ambientes de equilibrio y comunicación, y además, mejores enfoques en la resolución de problemas".

Andrea Fernández, gerente general de Kaspersky en la región SOLA, añade que las carreras de TI requieren soft skills como priorizar el trabajo en equipo y el fomento de relaciones laborales, algo que a sus ojos destaca en los perfiles femeninos. Y dice que un ejemplo de eso es la experiencia en la pandemia: "Las mujeres, y no solo las de la industria tech, hemos confirmado que poseemos las habilidades necesarias para tener éxito en cualquier entorno e incluso para el 'multitasking' sin perder la capacidad de entregar resultados en el ámbito profesional y bajo una carga de estrés que nunca habíamos vivido".

Otro punto clave, dice Fernández, es que hombres y mujeres suelen aportar diferentes visiones sobre un mismo tema. "Esa diversidad de opiniones es beneficiosa para las empresas. Y a lo largo de mi carrera he sido testigo de que los equipos diversos son los más eficientes", señala.

Carlos Bustos, director regional de Ciberseguridad en Sonda, dice que aumentar la participación femenina ayudaría a impulsar la innovación y la creatividad, pero cree que también impactaría en reducir los requerimientos de personal. "Esto ha crecido muy rápidamente", advierte.

Justo ahí es donde Quiroga observa una oportunidad de oro: "Lo que realmente marca un precedente es que el sector requiere de capital humano con urgencia y esta es una oportunidad histórica para que las mujeres encuentren un área de desarrollo profesional que está necesitando el país".

PUBLIRREPORTAJE

TRUSTTECH Cybersecurity

UNA VISIÓN CRÍTICA DEL NUEVO CUERPO LEGAL EN EL CHILE DE HOY:

Las interrogantes en materia de Ciberseguridad que abre la nueva Ley de Delitos Informáticos

Felipe Hott Delgado, director de TRUSTTECH Cybersecurity e investigador de ciberseguridad, señala que la nueva Ley 21.459 (promulgada el 20 de junio de 2022), abre inquietudes para el ecosistema de Ciberseguridad de Pymes y grandes corporaciones.

Los mismos días en que se promulgaba en nuestro país la nueva Ley de Delitos Informáticos (que deroga la Ley 19.223), medios de prensa informaban que la Fiscalía buscaba a un hacker chileno, apoyándose para ello en datos del FBI.

Algunos medios publicaron la presentación del fiscal a cargo del caso ante tribunales por el delito de sabotaje informático, presentación que aparece pertinentemente "ofuscada" en todo lo que se considera dato sensible en una causa en curso. "Me pregunto, ¿de verdad pensaron que publicar un PDF ofuscado con una capa que va por sobre la capa de texto, le da seguridad y confidencialidad? Producto de esto, cualquier persona puede descargar el documento, abrirlo con cualquier visor PDF, seleccionar, copiar y pegar y... magia: ahí están todos los datos sensibles", observa Felipe Hott Delgado, director de TRUSTTECH Cybersecurity e investigador de ciberseguridad.

El profesional sostiene que la nueva Ley de Delitos Informáticos debiese procurar que los profesionales que cometen este tipo de faltas en el tratamiento de información confidencial, y muchos otros "descuidos tecnológicos", sean debidamente castigados, señal que él no ve en el nuevo cuerpo legal.

Felipe Hott Delgado, director de TRUSTTECH Cybersecurity e investigador de ciberseguridad.

Felipe Hott profundiza su crítica: "Hay quienes creen que la nueva ley es la solución, pero lo único que esta logra es que, si antes había un 50% de vulnerabilidades explotadas sin que las víctimas lo supieran, ahora será el 100%, pues quienes expresamente piden un Ethical Hacking son solo una minoría de la extensa lista de empresas en nuestro país".

5G: LA GRAN ALIADA DEL DESARROLLO EN CHILE QUE ABRE NUEVOS DESAFÍOS DE SEGURIDAD

Según el informe IDC Latin America IT Investment Trends 2022, el 34% de los CIOs chilenos priorizará las inversiones para mejorar la experiencia del cliente en 2022. Frente a eso, 5G juega en la delantera.

POR FABIOLA ROMO P.

La pandemia permitió descubrir los grandes cambios que generan las comunicaciones móviles. Desde el comercio minorista hasta la salud se benefician de la conectividad que facilita la tecnología. Además, muchas personas descubrieron que pueden trabajar a distancia desde cualquier lugar con una banda ancha fiable.

"Según la Revisión de las Perspectivas de la Urbanización Mundial de 2018 de la ONU, alrededor del 68% de la población mundial vivirá en zonas urbanas en 2050, lo que añadirá 2.500 millones de personas más a nuestras ciudades en comparación con la actualidad. El 5G aportará un importante valor añadido a la economía mundial y proporcionará nuevos puestos de trabajo", afirma José Ignacio Díaz, analista senior de Telecomunicaciones de IDC Chile.

Por su parte, Miguel Moreno, gerente comercial de Btres, comenta que gran parte de la infraestructura de telecomunicaciones inalámbricas 5G se basa en tecnologías heredadas, como las redes 4G LTE, por lo que cualquier vulnerabilidad ya existente en esas redes amenazará la seguridad de las redes 5G. "Al transmitirse muchos más datos a través de los dispositivos, a los ciberdelincuentes les parecerá más atractivo llevar a cabo la extracción de datos", sostiene.

Adicionalmente, con la masificación de la Internet de las Cosas, la posibilidad de sufrir un ataque a través de los dispositivos nos deja bastante expuestos, según el ejecutivo de Btres. Por eso, considera fundamental mejorar la protección de datos a través de soluciones de ingeniería novedosas y apoyados por fabricantes de primer nivel.

Aunque la tecnología 5G traerá consigo mejoras en la comunicación, aumentando el ancho de banda y disminuyendo tiempos de respuesta, es necesario considerar que eso conlleva retos respecto de la infraestructura que la sustenta. "Uno de los principales desafíos es lograr la cobertura necesaria de fibra óptica y antenas, por lo que las empresas de telecomunicaciones necesitarán realizar grandes inversiones", afirma Gerardo Guajardo, cofundador de S4E.

Lo anterior, sin embargo, trae buenas noticias, como "nuevos empleos y oportunidades de negocio e inversión para empresas que les brindan servicios a las empresas de telecomunicaciones", indica el especialista de S4E.

En definitiva, la tecnología de quinta generación abre todo un abanico de opciones, especialmente para retroalimentar datos en tiempo casi real y acelerar la toma de decisiones, gracias a los sensores y otras tecnologías.

"En un contexto industrial, el análisis en tiempo real permite el mantenimiento predictivo y preventivo de máquinas, mejorando la disponibilidad del proceso", concluye José Ignacio Díaz.

PUBLIRREPORTAJE

EL DESAFÍO DE CONTRARRESTAR EL ROBO DE DATOS:

Arkavia y LUMU, expertos en seguridad contra ciberdelitos

A nivel mundial, la pandemia acrecentó el uso de plataformas y medios digitales, lo que dio por consecuencia un aumento de hasta un 45% en ciberdelitos ocurridos el año 2021, según la PDI. En dicho escenario, el 20 de junio de 2022 se publicó en el Diario Oficial la Ley 21.459 que establece normas sobre Delitos Informáticos, deroga la ley 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest, al cual Chile se encuentra suscrito.

Arkavia, empresa líder latinoamericana de ciberseguridad, en su propósito de prevenir y contrarrestar el robo de datos, ha realizado una innovación dentro de su cartera de productos y servicios para brindar soluciones que contribuyen a implementar esta nueva ley, incorporando a LUMU, empresa líder de Análisis Continuo del compromiso, que permite implementar las capas de visibilidad adicionales necesarias para la prevención de estos hechos.

Desde LUMU afirman que "la nueva normativa de delitos informáticos representa un gran avance en cuanto a las sanciones que enfrentarían los ciberdelincuentes y contribuye a desincentivar las actividades delictivas. Sin embargo, lo que vemos no solo en Chile sino en toda la región es que, a pesar de las inversiones millonarias en ciberseguridad, las organizaciones siguen siendo víctimas de ataques a la integridad de sus sistemas informáticos. De hecho, tal como lo muestra nuestro Ransomware Flashcard 2022 (https://lumu.io/resources/2022-ransomware-flashcard/), aproximadamente 68% de las empresas reporta haber sido víctima de ataques de ransomware".

Esto demuestra, subrayan desde LUMU, que no es suficiente con aumentar las sanciones: "Se debe fomentar la implementación de estrategias de ciberseguridad eficientes, aplicables para cualquier tipo de organización, que se basen en la búsqueda continua e intencional de compromisos, que permitan identificar de forma precisa las amenazas y habiliten una respuesta temprana y automatizada ante los incidentes detectados".

https://www.arkavia.com
https://lumu.io/es