DF
DIARIO FINANCIERO®
SUPLEMENTO
SANTIAGO DE CHILE
VIERNES 28 DE ENERO DE 2022

DÍA INTERNACIONAL DE PROTECCIÓN DE DATOS

¿QUÉ LE DEPARA 2022 A LA CIBERSEGURIDAD?

Las empresas están integrando más tecnologías, mientras nuevos negocios se abren para generar nuevos puntos de entrada a los sistemas empresariales. Por eso, el desafío es proteger los datos con una mirada más holística. POR FABIOLA ROMO

En 2015 ocurría un ataque cada dos minutos con costos empresariales asociados a ciberseguridad cercanos a US$ 325 millones. Hoy los ataques suceden cada 11 segundos, con costos que superan los US$20 mil millones, según datos globales de la consultora Cybersecurity Ventures. Las cifras dan cuenta de cómo han evolucionado los delitos informáticos.

"Con el aumento de los dispositivos tecnológicos, crece exponencialmente la superficie susceptible de ataques (la cantidad de dispositivos por persona, o por empresa se entiende como superficie disponible para un ataque). Cada vez hay más personas conectadas a Internet y, por ende, una mayor cantidad y variedad de dispositivos y de información", afirma Ricardo Dorado, director de Crecimiento de la Fundación País Digital y vicepresidente de la Alianza Chilena de Ciberseguridad.

Según el especialista, es imperativa una evolución de la seguridad digital desde la creación y el desarrollo de soluciones puntuales, hacia plataformas que permitan, desde el punto de vista de la administración, manejar y tener visibilidad de todo, de punta a punta, así como bloquear, tomar acciones, poner en cuarentena o sacar de la red cualquier dispositivo que represente una amenaza.

"El desafío es integrar una mirada holística a la ciberseguridad, no solo técnica. Hoy el factor humano es el eslabón más débil de la cadena, y eso se debe cambiar con formación, educación y concientización", complementa el ejecutivo.

La ciberseguridad para las infraestructuras críticas como las redes de telecomunicaciones, los puertos, los aeropuertos, el sistema eléctrico, entre otros, son una necesidad, analizan desde Huawei, ya que los ciberataques podrían afectar la disponibilidad de los servicios esenciales. No obstante, en el caso de las redes de telecomunicaciones no es una preocupación nueva con la ventaja de la estandarización, que incluye características de seguridad nativas que hacen que los equipos 5G sean más seguros que los 4G.

Algunas tendencias

Según Fernando Graterol, subgerente de Seguridad de Ecomsur, las tendencias más relevantes en ciberseguridad están relacionadas con la Inteligencia Artificial, utilizada en la defensa y detección de ataques en tiempo real; el uso de Blockchain para garantizar autenticidad en algunas operaciones y transacciones; y el crecimiento en el uso del modelo zero trust, que implica desconfiar de todo, salvo que exista una validación de la identidad del usuario.

A nivel de amenazas, destaca el Ransomware, las vulnerabilidades generadas por el Internet de las Cosas (IoT) y el teletrabajo, así como los ataques a la cadena de suministro.

Como sea, la ciberseguridad encabeza la lista de prioridades de todo gerente de tecnología. "El mundo digital crece y se expande con las nuevas integraciones de dispositivos y redes, por lo que cada punto final de conexión a la red representa un factor de riesgo para la seguridad. Tanto en el sector público como en el privado, los infiltrados buscan acceder a información sensible o provocar un caos financiero a individuos, empresas y comunidades a cambio de un beneficio económico", señala Ricardo Dorado.

Recomendaciones

En FirmaVirtual, por ejemplo, utilizan una capa de Blockchain para proteger los datos de sus clientes. Además, recomiendan a las PYME proteger sus activos tecnológicos creando un entorno seguro para quienes trabajan desde su casa. En tanto, Yorki Bautista, arquitecto cloud Rex+, dice que la capacitación del equipo de trabajo siempre será vital. "Esto ayudará a que cada persona ponga mayor atención a la exposición de este tipo de amenazas y sepa evitarlas", afirma.

En Huawei, en tanto, aconsejan hacer uso del cifrado, la redundancia y las copias de seguridad, ya que es más difícil para los hackers acceder a la información y más fácil de recuperar la información en caso de ataques.

PUBLIRREPORTAJE

FORTINET:

Compañía 100% enfocada en ciberseguridad, para una protección amplia, integrada y automatizada

Con la mayor cantidad de expertos del rubro en nuestro país, Fortinet tiene el 46% del total de equipos de seguridad empresarial que están instalados en Chile, según IDC. De la mano de Fortinet Security Fabric, que es la plataforma de ciberseguridad de mayor rendimiento en la industria, brinda a sus clientes soluciones completas en este ámbito, por ejemplo, para la protección de datos, un activo clave en las organizaciones.

Desde el año 2021, Fortinet ha sumado importantes innovaciones en su propuesta de valor, la cual se basa principalmente en Fortinet Security Fabric, plataforma de ciberseguridad que brinda a sus clientes una protección amplia, integrada y automatizada. “Hemos expandido nuestra plataforma para trabajo remoto seguro, protección en IoT y OT, y automatización avanzada para respuestas ante amenazas sofisticadas que requieren inteligencia artificial”, complementa Pía Salas, country manager de Fortinet Chile. La ejecutiva agrega que “un punto estratégico de la inversión en ciberseguridad, es que las soluciones sean 100% integradas. Respondiendo a dicho desafío, todos nuestros sistemas tienen la capacidad de comunicarse entre sí, compartir la información, prevenir las amenazas, responder de manera automatizada ante cualquier tipo de ataque cuando estos ocurren y mitigarlos lo más rápidamente”.

Pía Salas, country manager de Fortinet Chile.

Con servicios y soluciones a la medida de cada cliente, Fortinet puede suministrar, entre otras, capacidades de Secure SD-WAN y soporte de FortiCare actualizado para una resolución más rápida de los problemas y una mayor continuidad del negocio.

Hoy Fortinet dispone de soluciones en ciberseguridad para todo tipo y tamaño de empresas, desde Pymes hasta grandes compañías, además de entidades del Estado. En ese marco, a medida que las redes se van complejizando, van surgiendo amenazas más sofisticadas que ponen en riesgo la protección de los datos. “La información que maneja una empresa respecto de sus clientes, o información sensible en general, es un activo incalculable que, al estar bajo amenaza de ciberataques, las deja expuestas frente a la competencia y frente al mercado”, señala Pía Salas.

Según datos de FortiGuard Labs -la organización de investigación e inteligencia de amenazas de Fortinet-, durante el primer semestre de 2021 Chile sufrió más de 2.100 millones de intentos de ciberataques, mientras que en América Latina esa cifra se empinó a más de 91 mil millones en el mismo período, siendo el principal ataque el ransonware (secuestro de datos), un tipo de malware que puede generar importantes daños económicos y reputacionales a las empresas. “Un dato relevante registrado por FortiGuard Labs en el segundo semestre de 2021, es que tanto empresas como personas tomaron mayor conciencia de estas amenazas, y por ende más resguardos, porque cuando comenzó la pandemia aumentó el uso de plataformas”, observa la country manager de Fortinet Chile.

El año 2022, la ciberseguridad será una capacidad estratégica cada vez más relevante. En ese escenario, Fortinet cuenta con una potente oferta integral para networking y seguridad digital, consultores expertos en el país y un ecosistema de canales de venta y distribución, al servicio de sus clientes.

https://www.fortinet.com/lat

FORTINET®

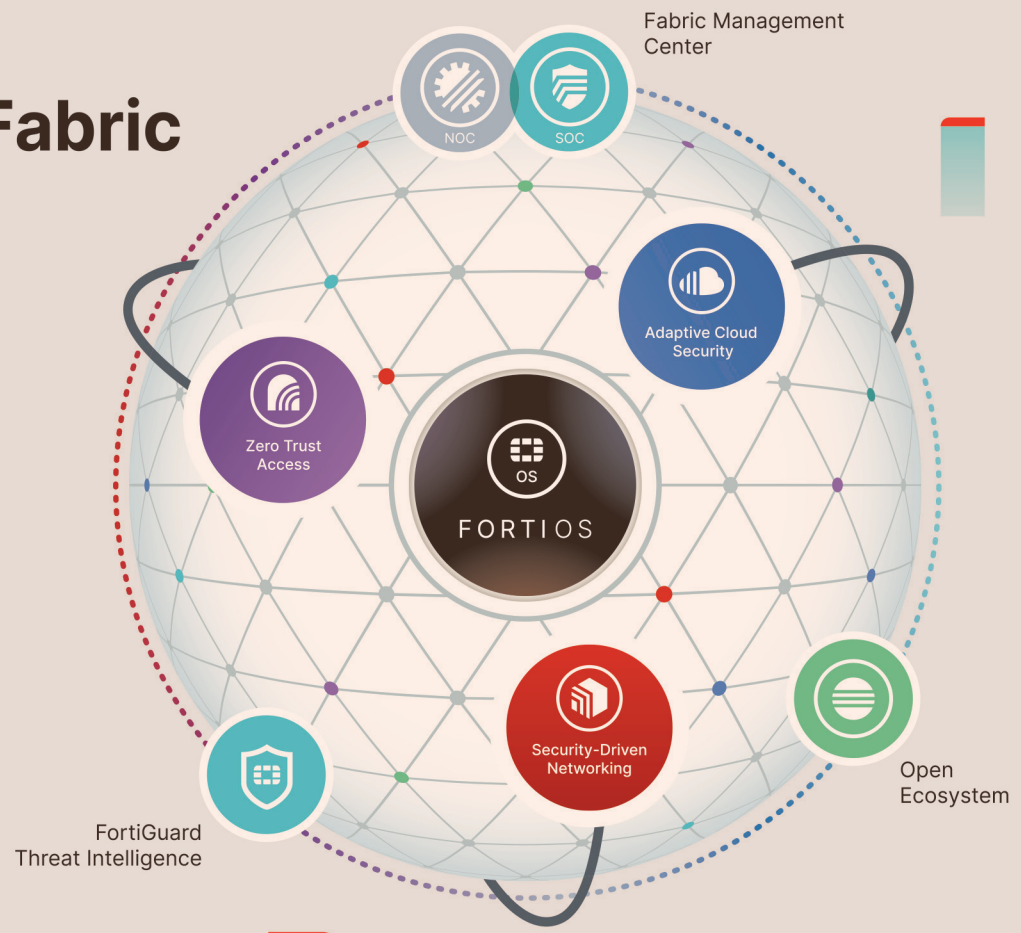
Las empresas de hoy requieren un Security Fabric

La plataforma de ciberseguridad de mayor rendimiento de la industria con tecnología FortiOS.

Amplia
Reduzca el riesgo y administre toda la superficie de ataque digital.

Integrado
Cierre las brechas de seguridad y reduzca la complejidad.

Automatizada
Reducción del tiempo de prevención y operaciones eficientes.



www.fortinet.com/lat

METAVERSO: LA PLATAFORMA QUE PROMETE REVOLUCIONAR TODO

A través de videojuegos, la animación digital y el desarrollo de experiencias inmersivas nos acercamos a la próxima generación de Internet. Un espacio donde la ciberseguridad y la privacidad serán vitales.

La tecnología no se detiene y una nueva generación de Internet ya se acerca. Se trata del llamado metaverso, una red en proceso de desarrollo que estará basada en la realidad virtual y que operará en paralelo a la realidad física en la que nos desenvolvemos cada día.

Según Bloomberg Intelligence, este espacio proyecta mover nada menos que US$ 800 mil millones para el año 2024. Una estimación que está impulsando a empresas de todas las áreas a invertir grandes sumas de dinero para reservar o derechamente adquirir un lugar.

Hace una semana el mercado fue remecido por la compra que realizó Microsoft sobre Activision Blizzard. A raíz de ello el decano de la Facultad de Diseño Digital e Industrias Creativas de la Universidad San Sebastián, Carlos Hinrichsen, plantea dos preguntas esenciales: ¿por qué una apuesta tan millonaria por esta empresa de videojuegos? y ¿qué supondrá el metaverso para la industria, la sociedad y las personas?

"A través de videojuegos, la animación digital y el desarrollo de experiencias inmersivas nos aproximamos a la puerta de entrada de la próxima generación de Internet. De acuerdo con las proyecciones de Bloomberg, este será un mercado emergente para nuevas empresas tecnológicas y que según varias estimaciones moverá casi cuatro veces el PIB de Chile", explica el profesional, quien añade que el metaverso ofrecerá múltiples oportunidades para la creación de productos, servicios y experiencias que se moverán entre el mundo físico y el digital.

Privacidad y seguridad

El académico de la facultad de Economía y Negocios de la Universidad de Chile, Miguel Ángel Díaz, explica que muchas compañías están apostando altas sumas de dinero en este desarrollo, comprendiendo que el metaverso será el próximo lugar donde se generarán las operaciones, las transacciones y donde las personas pasarán la mayor parte de su tiempo.

"Es como al inicio de Internet cuando una IP representaba la posibilidad de estar presente en la red. Hoy nadie cuestionaría esa inversión. Se estima que un terreno virtual permitiría alojar tiendas y realizar eventos a los cuales se puede invitar, como en propiedades reales. Ya sea por especulación o para desarrollar proyectos en el metaverso, las operaciones de bienes raíces digitales se está transformando en un negocio muy real", puntualiza.

> "Con el metaverso podríamos volcar completamente nuestra cotidianidad en Internet, por lo que la ciberseguridad y la privacidad adquieren un rol protagónico, tal como ocurre en la actualidad", dice Fernanda Mattar, de Entel.

Tan concreto como lo explica la subgerenta de Ingeniería de Seguridad de Entel, Fernanda Mattar, al recordar la novela Ready Player One, de Ernest Cline, que posiciona al metaverso como eje central de su historia: una sociedad futura que escapa de su realidad a través de un espacio llamado Oasis y que para acceder exige el uso de lentes y trajes con sensores.

"Con el metaverso podríamos volcar completamente nuestra cotidianidad en Internet, por lo que la ciberseguridad y la privacidad adquieren un rol protagónico, tal como ocurre en la actualidad, ya que aún nos enfrentamos a muchos de los mismos riesgos. En gran medida, estos problemas se centran en la recopilación de información personal y en la forma en que se protegerán estos datos e identidades digitales ante posibles ataques de ingeniería social, vulnerabilidades de día cero o configuraciones inseguras", analiza.

Grandes proyecciones

Al visualizar el desarrollo del metaverso es posible anticipar el nacimiento de un nuevo territorio que, al mismo tiempo, es una plataforma tecnológica innovadora: un espacio inmersivo y que ofrece múltiples promesas y propuestas en educación, salud y entretenimiento, entre muchos otros ámbitos de acción. En ese contexto Díaz advierte que como todo avance luce aspectos positivos, de gran potencial y enormes oportunidades, pero que también podría conllevar riesgos para los usuarios y quienes invierten.

"En la vida real y en los espacios virtuales nada es completamente seguro. Dependerá de la evolución de la tecnología, la educación y la disciplina digital de los usuarios", prevé Díaz.

Una visión que comparte Mattar, quien resalta que, tal como ocurre con cualquier plataforma tecnológica, en el metaverso indudablemente se podrían generar problemas de seguridad en torno a los datos y la privacidad. Por lo tanto, las firmas deberán trabajar para contar con medidas y protocolos destinados a proteger su información. Al igual que Internet, necesitará de dispositivos, infraestructura y software para su buen funcionamiento y proyección.

GRUPO DF
DF · DFLIVE · DEMAS · 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 y 11, Las Condes, Fono: 23391000 / e-mail: buzondf@df.cl / **Impreso por** COPESA IMPRESORES S.A., que sólo actúa como impresor.

LOS DESAFÍOS DE SEGURIDAD QUE TRAE LA **MASIFICACIÓN DE LA RED 5G**

Si bien esta tecnología llega con un sinfín de beneficios en conectividad, productividad y comunicaciones, también conlleva riesgos para los datos. POR FRANCISCA ORELLANA

"Podremos ver nuevos ataques, como los de agotamiento de baterías -ahora cinco veces más rápido-, la degradación de servicios al utilizar técnicas criptográficas para obligar a abandonar modos de alta calidad, así como de identificación, permitiendo al atacante descubrir dispositivos en la red y revelar su hardware y software", comenta Hugo Galilea, director de la Alianza Chilena de Ciberseguridad (ACC), sobre las amenazas que se visualizan con la implementación de las redes 5G, cuyo ancho de banda podría beneficiar a los ciberdelincuentes para potenciar sus delitos.

La nueva red presenta falencias aún no resueltas en ámbitos de autenticación, dice Claudio Ordóñez, director de Ciberseguridad de Accenture Chile. A eso se suma que la virtualización o realidad extendida permite un seguimiento preciso de la ubicación del usuario, aumentando los problemas de privacidad.

De hecho, un estudio de esa consultora reveló que el 58% de las firmas a nivel mundial dijo estar consciente de los riesgos de esta tecnología, siendo un desafío prioritario de abordar.

"Lo básico para la protección del dato es la adopción de antivirus, pero también es fomentar un programa de cultura en ciberseguridad. Para el resguardo de datos, también es fundamental comenzar a respaldar información de manera inmutable.", destaca Juan Pablo Sanhueza, socio fundador de Global Catalog.

No obstante, Galilea acota que hoy el 40% de los ataques exitosos son producto de una vulneración de un proveedor. Un escenario que para Pía Salas, Country Manager de Fortinet Chile, requerirá repensar las redes y seguridad, donde "todo lo relacionado con el ecosistema de la empresa debe identificarse y evaluarse en términos de criticidad y confirmarse su estado".

Salas agrega que la transformación digital generará grandes cantidades de datos nuevos, la mayoría de los cuales serán encriptados (hoy constituyen más del 70% del tráfico de red). Esto requerirá herramientas de seguridad de alto rendimiento en IoT y otros dispositivos perimetrales que puedan inspeccionar el tráfico encriptado tanto a velocidad como a escala.

"Es prudente generar ambientes de monitoreo que permitan en tiempo real generar las correcciones y así evitar casos de indisponibilidad, accidentes e inaccesibilidad a los recursos informáticos", recomienda Rodrigo Simpson, arquitecto de soluciones TI de ITQ Latam, quien propone además agregar algoritmos de Machine Learning e Inteligencia Artificial para lograr resiliencia ante algún ataque o indisponibilidad de algún componente en la cadena de suministros del servicio 5G.

"ES NECESARIO AVANZAR Y PERFECCIONAR **EL RÉGIMEN DE DELITOS INFORMÁTICOS"**

La celebración del Día de la Protección de Datos se recibe en Chile con novedades legislativas sobre la modificación a la Ley 19.628 y a la de delitos informáticos. Desde la ACTI destacan los avances, pero con cierta preocupación. POR RITA NÚÑEZ

Este año, la celebración del Día Internacional de la Protección de Datos se da en un momento de discusión sobre la legislación en la materia. Para Raúl Arrieta, representante del Grupo Legal de la Asociación Chilena de Empresas de Tecnologías de la Información (ACTI), es importante la adecuación de la normativa chilena a los estándares internacionales, puesto que "uno de los grandes problemas que tiene nuestra ley es la ausencia de una autoridad de protección de datos", la que, entre otras cosas, debe educar a las personas al respecto.

Arriesta dice que la creación de esta autoridad ayudaría a que "haya reglas más claras sobre cómo tratar la información y terminar con la inseguridad regulatoria, porque dado que este proyecto de ley no termina de ver la luz, estamos todos los días enfrentados a proyectos de ley nuevos, los que son incluso incoherentes entre sí mismos", precisa.

Por ello, cree que es positiva la modificación a la Ley 19.628 de protección de datos, que esta semana terminó su tramitación en el Senado y ahora se va a la Cámara de Diputados para su segundo trámite constitucional.

Delitos informáticos

Durante los últimos días, en una declaración firmada por la ACTI junto a otras siete entidades, se cuestionó que una Comisión Mixta del Congreso haya aprobado modificar el Código Penal para permitir al Ministerio Público solicitar datos personales de los ciudadanos a los prestadores de servicio sin orden judicial.

A raíz de ello, Arrieta cree que se "ha tratado de construir que la industria está en contra de la aprobación de la ley" y aclara que la ACTI "no está en contra". Por el contrario, creen que "es necesario avanzar y perfeccionar el régimen de delitos informáticos".

Sin embargo, subraya que "el proyecto de ley excede con creces lo que plantea el Convenio de Budapest" y añade que "para que la gente confíe en la tecnología, no se puede pretender construir un estatuto jurídico diferenciado, dependiendo de si estoy en el mundo digital o en el mundo físico. Los derechos fundamentales son derechos fundamentales siempre".

Es por eso que plantean que tiene que mediar una autorización judicial cuando el Ministerio Público quiera acceder a información de las personas que se encuentre en poder de los prestadores de servicio.

"Cómo no va a ser razonable que si se van a afectar los derechos fundamentales de alguien, se tome conocimiento de que eso está pasando", insiste, mientras hace un llamado a las próximas autoridades para dar urgencia en el avance de la ley de protección de datos personales.

PUBLIRREPORTAJE

REFORZANDO LA CIBERSEGURIDAD ANTE UN COMPLEJO ESCENARIO:

Respaldo Inmutable, la estrategia de Global Catalog y Veeam® frente a la protección del dato

Con el avance del Ransomware y demás ciberataques acechando en cada esquina, la seguridad de los datos se vuelve vital para garantizar la privacidad de las organizaciones y el éxito del negocio. Global Catalog en compañía con Veeam® fomentan la confianza ayudando a diferentes organizaciones a almacenar, proteger y recuperar los datos de sus backups, con tranquilidad durante todo su ciclo de vida.

Si hablamos de protección contra el borrado accidental, malintencionado o fortuito de datos, hay ciertos componentes que, en conjunto con el cumplimiento de la regla del 3-2-1 y un monitoreo de la infraestructura, nos permiten tener una estrategia de DR completa con un repositorio ultrarresiliente que tiene alguna o todas las siguientes características: debe ser offline, aislado, e inmutable. Cuando un backup es "inmutable", éste no puede alterarse de ninguna forma o borrarse a lo largo de su ciclo de vida mientras reside en el almacenamiento local y en la nube. Aprovechando los sistemas de inmutabilidad integrados que existen en los sistemas de archivo Linux y el almacenamiento S3, se puede garantizar que el backup está a salvo y listo para su recuperación, siendo además opciones muy atractivas para la retención a largo plazo y el archivado general.

Desde la versión 11 de Veeam®, la solución tiene la capacidad de aumentar la seguridad de los datos del backup, mediante la integración con almacenamiento Linux y Amazon S3, que permiten tener backups inmutables de forma nativa.

Ofrecer una estrategia de respaldos que sea seguro, ya no es un lujo para las empresas, sino que debe transformarse en una prioridad del negocio. Si proyectamos el incremento de los ataques durante el 2022, estos servicios serán claves y ello obedece a la relevancia que está adquiriendo la protección de los datos.

En Global Catalog ayudamos a las empresas a proteger sus datos, contamos con ingenieros altamente calificados y la confianza de casi 15 años de experiencia en el rubro TI.

Servicios de backup y replicación

Global Catalog implementa servicios de backup y replicación con Veeam, donde los clientes obtienen:
Protección sin bloqueo de fabricante con el NUEVO Repositorio Linux reforzado que almacena los backups en almacenamiento inmutable, evitando de esta forma la modificación o el cifrado.
Los backups cloud son recuperables y están protegidos al 100 % del ransomware con Amazon S3 Object Lock Immutability
Reducción del delta entre el almacenamiento primario y los backups con copia de backup automatizada al almacenamiento de objetos, para conseguir cumplir con la regla 3-2-1-1-0 más rápido que nunca.

https://globalcatalog.cl/
https://www.veeam.com/es

TRES MIRADAS A LO QUE VIENE PARA EL TEMA EN CHILE

El país vive un momento de cambios, donde nuevas oportunidades están surgiendo para avanzar en distintas materias, incluyendo a la protección de datos. Por eso, tres especialistas desde tres veredas distintas analizan los próximos desafíos en una materia que está más vigente que nunca y que enfrenta también múltiples retos frente al avance de la tecnología, las comunicaciones e, incluso, de la discusión constitucional.

Macarena Gatica, socia de Alessandri Abogados.

La oportunidad de consagrar la protección de datos en la nueva Constitución

Regulaciones aisladas y un ordenamiento jurídico carente de coherencia son las principales causas de que en Chile las vulneraciones a los datos personales carezcan de una tutela eficaz. Y dada la falta de homologación de la regulación chilena por otras jurisdicciones, no es posible exportar productos y servicios asociados al tratamiento de datos.

En 1999 se aprobó el proyecto de ley sobre protección a la vida privada, constituyendo la primera ley en Latinoamérica en protección de datos personales. Sin embargo, a la fecha, Chile no cuenta con una ley que se adecue al tratamiento de datos que el avance de la tecnología ha permitido. Argentina, Colombia, Uruguay, Perú y Brasil cuentan con regulaciones ad hoc a la cuarta revolución industrial. Y aunque en 2018 nuestro país consagró como garantía constitucional la protección de datos personales, recién esta semana el proyecto de ley sobre protección de datos (boletín 11.144) pasó a segundo trámite constitucional.

Chile tiene la oportunidad de consagrar la protección de datos, el derecho de accesibilidad, la ciberseguridad y la alfabetización tecnológica en la nueva Constitución. La expectación estará en la nueva facultad fiscalizadora del Sernac respecto de los datos y la aprobación del boletín 11.144, para así dar cumplimiento a la Política Nacional de Inteligencia Artificial, la implementación del open banking y coronar a Chile como centro tecnológico.

Rodrigo Espinosa, presidente de la Asociación de Marketing Directo y Digital de Chile (AMDD).

La importancia de la protección de datos para la comunicación y el consumo

El tratamiento ético y transparente de datos, relevante y con consentimiento, es clave y beneficioso, tanto para las personas como las organizaciones, ya que permitirá generar mejores comunicaciones y relaciones de consumo más informadas entre las partes.

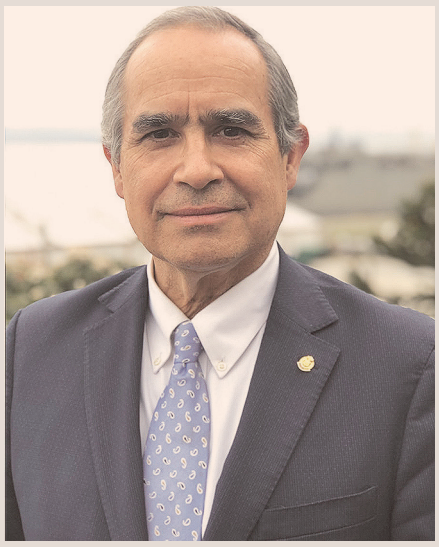
La protección de datos personales debe transformarse en un higiénico, ser un "desde" sobre el cual trabajen equipos dedicados a esta materia. Las personas confían sus datos a distintas organizaciones y estas deben ser capaces de responder a esa confianza, velando por el correcto uso de estos, a través de la creación de procesos y sistemas robustos de cumplimiento de protección.

Plataformas tecnológicas, inteligencia artificial, ecommerce altamente desarrollado, medios de pago móviles, millones de transacciones y puntos de contacto digital, entre otros, representan hoy un ecosistema tremendamente desafiante a la hora de hablar de datos, por lo que el rol del regulador y la capacidad de autorregulación de las empresas es fundamental.

Un aporte en esta materia es el de la Asociación de Marketing Directo y Digital de Chile (AMDD), la cual entrega conocimiento, recomendación de buenas prácticas y un marco ético en el tratamiento de datos, que permite a las empresas anticiparse a cambios en la regulación y aplicar mejores estándares en materia de protección.

Kenneth Pugh, senador de la Región de Valparaíso.

Protección de datos personales en Chile



Las llamadas desde callcenters hacia las personas son "pan de cada día", y se han vuelto parte de la rutina de la gente, que ve cómo las empresas manejan su información y la distribuyen a su libre albedrío y al mejor postor. Pero, ¿qué hacer cuando suceden estas situaciones y a quién recurrir?

Los ciudadanos cuentan con mayor conciencia sobre la relevancia de la protección de sus datos personales, pues se dan cuenta del mal uso de estos en su vida cotidiana. Desde que se reformó la Constitución en 2018 y se añadió el nuevo derecho a la protección de datos personales en el Artículo 19 -el mismo artículo que protege la vida-, se hizo algo que los chilenos estaban pidiendo.

Cada vez más las personas se han dado cuenta de que sus datos son esenciales, y esto se ve reflejado por la cantidad de información que terceros tienen de ellos: las personas se sorprenden de que las llamen por anuncios, promociones y servicios que ellos nunca han solicitado y de ahí parte la sospecha.

En relación con las leyes que tramitan, cabe destacar que la nueva Ley de Protección de Datos se encuentra en proceso de votación en sala del Senado y se espera pueda completar a la brevedad el primer trámite legislativo. Nos quedamos atrás en décadas respecto de la actualización de la normativa de protección de datos, y tanto en el Congreso como en el Gobierno se han comprometido para avanzar en esta normativa que tiene como base la regulación europea.

Esperamos que este año el proyecto se convierta en ley, ya que nuestra legislación en materia de protección de datos es de 1999, por lo que necesitamos con urgencia que se apruebe para entregar seguridad y tranquilidad a las personas, y no perder competitividad en mercados globales y el interés de inversionistas que eligen países que tengan regulación en esta materia.

ACCENTURE

Directorios, datos y ciberseguridad

Por Claudio Ordóñez, Líder de Ciberseguridad de Accenture Chile

Hoy la protección de los datos es una demanda cada vez más creciente entre clientes, inversionistas y el mercado en general. Y a medida que aumentan los riesgos y los costos de los ciberataques, la ciberseguridad se ha convertido cada vez más en un tema prioritario de los directorios a nivel mundial. Esto se debe a que un gobierno de ciberseguridad débil o inexistente amenaza el crecimiento global de la economía digital, que el Foro Económico Mundial estima que impulsará el 60% del PIB mundial este año.

Se proyecta que los costos de la ciberdelincuencia aumenten un 15% anual, alcanzando potencialmente los 10,5 billones de dólares anuales en 2025. La lección es clara: el conocimiento de los líderes sobre este tema se está convirtiendo en algo cada vez más fundamental para ayudar a reducir el riesgo y proteger los beneficios. Y sin duda, estos riesgos están aumentando.

Los atacantes más sofisticados, por ejemplo, están trabajando para explotar el riesgo sistémico de los sistemas digitales en amplia expansión. Esto significa que las amenazas pueden propagarse rápidamente entre los socios comerciales y los sistemas conectados, con un daño cada vez mayor. Los riesgos patrimoniales, de litigio y de negocio que conlleva la amenaza cibernética exigen que el gobierno de ciberseguridad sea una competencia fundamental de los consejos de administración y directorios.

Afortunadamente, todos los directorios pueden hacer un progreso significativo a corto plazo hacia el desarrollo de un consejo corporativo ciber-competente. Estos pasos implican el desarrollo de entendimiento general de ciberseguridad en todos los directores corporativos y la incorporación de expertos en ciberseguridad a la sala de juntas.

Así también, la comunicación sobre riesgos cibernéticos entre el directorio y el CISO es una parte fundamental para gobernar y gestionar riesgos empresariales importantes. Pero las comunicaciones deben ser pertinentes, oportunas y adecuadas a su finalidad. La próxima generación de CISOs debe ser a la vez experta en negocios y en tecnología, y sentirse tan cómoda en la sala de juntas como en el centro de operaciones de seguridad, hablando el lenguaje de la empresa.

Hay tres elementos que pueden ayudar a los directorios a supervisar cualquier plan de comunicación de riesgos de ciberseguridad durante la pandemia y más allá. El primero es la táctica. Se deben realizar informes trimestrales regulares de los CISOs a los directorios, los

que se centren en las métricas operativas clave de la gestión de riesgos de ciberseguridad. Esto puede incluir análisis sobre las amenazas detectadas, los tiempos de permanencia y la formación de los empleados.

El segundo elemento es el operativo, no operativo técnico, sino en cuanto el riesgo de ciberseguridad afecta a la operación de la empresa. Muchos enfoques de comunicación de riesgos de ciberseguridad se detienen en la fase táctica, lo que hace que sean en gran medida ineficaces a la hora de ayudar a la junta directiva a entender realmente el riesgo en este ámbito y su impacto en el negocio. Las comunicaciones operativas pueden ayudar a los directores a ver cómo la ciberseguridad afecta al valor del negocio, y a dar una idea del efecto a largo plazo sobre la estrategia y el crecimiento.

El tercer elemento clave es practicar. Evaluar en terreno la rapidez con la que una organización puede recuperarse de un ataque. Utilizar ejercicios de respuesta a incidentes simulados para ilustrar cómo un enfoque integral durante una crisis puede dar lugar a eventos bien gestionados.

La ciberseguridad efectiva es una prioridad empresarial. Cada sala de juntas y cada director corporativo es un punto de control crítico en la defensa contra riesgos. Tan pronto como sea posible, las organizaciones deben desarrollar un directorio corporativo altamente competente en ciberseguridad para gobernar este riesgo de manera efectiva.

www.accenture.com