Fortalecimiento de la Seguridad y Protección de Datos Personales en Chile: Desafíos y Perspectivas hacia el Futuro.

Sebastian Berrios, *Member, Pontificia Universidad Católica de Valparaíso,* Pamela Hermosilla, *Member, Pontificia Universidad Católica de Valparaíso,* Héctor Allende Cid, *Member, Pontificia Universidad Católica de Valparaíso.*

***Abstract*- La ley chilena de protección de datos personales, establecida en 1999, no logra abordar los desafíos contemporáneos en ciberseguridad. Un análisis comparativo con las leyes europeas y las de otros países latinoamericanos revela una disparidad notable. Esta deficiencia resulta en la persecución o permisión inadecuadas de delitos relacionados con el tratamiento de datos personales. El reciente aumento en las filtraciones de datos subraya la necesidad urgente de modernizar la legislación chilena sobre la protección de datos personales, alineándola con los estándares actuales de ciberseguridad.**

***Index Terms*--Ciberseguridad, Protección de datos, Cibercrimen, Chile.**

I. Introducción

En Chile, la protección de datos personales se ha convertido en un tema de creciente interés y preocupación. Impulsado por el avance tecnológico y la expansión de la digitalización, este tema ha cobrado una relevancia sin precedentes en la sociedad chilena. La legislación chilena sobre protección de datos, que se remonta a 1999, ha demostrado ser insuficiente frente a los desafíos de la era digital actual, especialmente en cuestiones de ciberseguridad. Esta insuficiencia se hace más evidente al comparar la normativa chilena con la de la Unión Europea y otros países de América Latina, donde se han adoptado medidas más avanzadas en este campo.

La creciente incidencia de brechas de seguridad y ciberataques ha puesto en evidencia las debilidades de los sistemas de protección de datos en Chile, generando un llamado urgente a la acción para fortalecer las políticas y regulaciones existentes. Este movimiento busca no solo actualizar la legislación para equipararla con los estándares internacionales, sino también fortalecer la confianza del público en las plataformas digitales y las instituciones que manejan datos personales.

Con una sociedad cada vez más consciente de la importancia de la privacidad de datos, ha surgido una demanda de mayor transparencia y responsabilidad en el manejo de la información personal por parte de entidades gubernamentales y privadas. Esta concienciación ciudadana es un paso crucial hacia la creación de un entorno más seguro y protegido para los datos personales.

En este contexto, Chile enfrenta el reto vital de reformar y actualizar su marco normativo y sus prácticas de gestión de datos personales. Esta actualización no solo es necesaria para la protección de los ciudadanos, sino también para asegurar la adaptación de Chile a un entorno global cada vez más digital y conectado.Desde los inicios de la informática existen los ataques informáticos y virus en los sistemas, uno de los primeros exponentes de este tipo de virus es el programa Creeper, el cual fue creados en 1971 creado por Bob Thomas, el cual era una prueba de seguridad y no buscaba ser malicioso, pero quería comprobar si era posible replicar en la red de ARPANET, cosa que sí pudo hacer, al replicarse e "infectar" un disco duro, procedió a eliminarse a sí mismo y dejar un mensaje que decía: "Soy Creeper, ¡Atrápame si puedes!"Sin embargo, el primer virus creado con malas intenciones fue el virus de Rabbit (o Wabbit), el cual al ingresar en el equipo hacía muchas copias de sí mismo, haciendo que la computadora se ralentizará tanto que resultara en un congelamiento y eventualmente colapsarlo.

Pasado muchos años después, evolucionaron las redes y actualmente nos encontramos en la era del internet donde mucha de nuestra información se encuentra disponible en internet, ya sea de manera pública como en redes sociales, perfiles, entre otros y información privada o sensible, como por ejemplo tarjetas de crédito, credenciales, direcciones, entre otros tipos de datos. En un mundo donde cada vez más y más gente se conecta a internet, accede a servicios, todos estos datos quedan registrados en alguna base de datos, donde se guarda todo tipo de información que el usuario entregue, por lo que mucha de nuestra información se encuentra acá, ya sea públicamente accesible como no accesible. A pesar de que las bases de datos suelen estar inaccesibles al público general, la globalización y el avance de Internet han dado lugar a nuevos desafíos significativos. Entre estos, los ataques cibernéticos y la acción de los piratas informáticos representan una amenaza creciente. Estos actores malintencionados aprovechan las vulnerabilidades en la seguridad de las bases de datos para acceder a información confidencial, poniendo en riesgo la integridad y privacidad de los datos almacenados. Esta problemática subraya la importancia de implementar estrategias robustas de ciberseguridad y protección de datos para contrarrestar eficazmente tales riesgos.

II. Evolución de las Vulnerabilidades

En la actualidad, con las nuevas tecnologías que se van desarrollando a medida que avanzan los años, también se encuentran nuevas vulnerabilidades y puertas traseras, las cuales son oportunidades perfectas para ser interceptado y atacado, por ende, a medida que avanzan los años, cada vez es mas facil o mas probable ser víctima de algún ataque, ya sean grandes como medianas, pequeñas o incluso ataques a individuos. Un estudio realizado por IBM Security determinó que hay 3 principales razones por las cuales es posible tener una vulneración de datos, puede ser mediante el error humano (ser víctima de phishing o ingeniería social), un ataque malicioso o un error del sistema (como no estar actualizado por ejemplo).

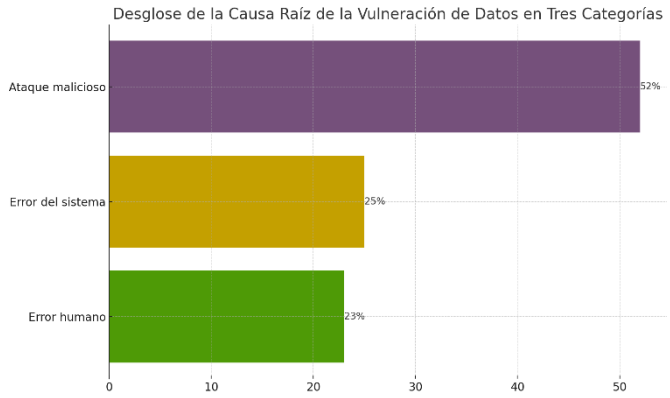


Fig. 1. Gráfico de causales de vulneración de datos, de IBM Security

Además del gráfico anteriormente mencionado por las causas en las que se pueden vulnerar los datos, existe otro gráfico más el cual es más específico con los métodos de ataque utilizados para vulnerar los datos.

Cuentas de Empleados Comprometidas: Estas fueron la causa más costosa de las brechas de datos, con las empresas estudiadas experimentando costos casi $1 millón más altos en promedio por brecha en comparación con el promedio global, llegando a $4.77 millones por incidente. El 80% de estos incidentes resultó en la exposición de información personal identificable (PII) de los clientes, siendo la PII de clientes también la más costosa para las empresas.[1]

Credenciales Robadas o Comprometidas y Configuraciones Erróneas en la Nube: Estos fueron los motivos más comunes de brechas maliciosas, representando casi el 40% de los incidentes maliciosos. Las empresas luchan con la complejidad de la seguridad, lo que contribuye a que las configuraciones erróneas en la nube se conviertan en un desafío creciente. Los atacantes utilizaron estas configuraciones erróneas para violar las redes en casi el 20% de los casos, aumentando los costos de brecha en más de medio millón de dólares en promedio a $4.41 millones.

Ataques Patrocinados por Estados: Aunque representaron solo el 13% de las brechas maliciosas estudiadas, los ataques patrocinados por estados fueron el tipo de adversario más dañino. Estos ataques promediaron $4.43 millones en costos de brecha de datos, superando a los ciberdelincuentes motivados financieramente y a los hacktivistas.

Estas estadísticas subrayan la importancia de abordar las vulnerabilidades de seguridad interna, como las cuentas de empleados comprometidas y las configuraciones erróneas en la nube, así como la necesidad de estar preparado para ataques complejos patrocinados por estados.

Uno de las primeras brecha de datos (o data breach como se le conoce en inglés) fue en el año 2005 a la DSW Shoe Warehouse, una tienda de zapatería ubicada en Estados Unidos, donde se tomó información sensible como tarjetas de crédito, débito y datos personales de cuentas de usuarios de más de 1 millón de personas en EE.UU. Esto generó el llamado a las autoridades, más específicamente la Comisión Federal de Comercio o Federal Trade Commission (FTC) de EE.UU, donde llegaron a la conclusión de que DSW falló en proteger la información de los usuarios de la tienda.Esto se debió a que se encontraron múltiples irregularidades y malas prácticas a la hora de almacenar los datos de los clientes, entre estas malas prácticas se encuentran:

Crear riesgos innecesarios a la información sensible al almacenar muchos archivos cuando ya no hacía falta tener esta información
Almacenar información sensible como IDs de usuario y contraseñas de manera no encriptada
Falta de personal para verificar los accesos no autorizados
Falla en no utilizar el equipamiento de seguridad para limitar los equipos que se podían conectar mediante red inalámbrica

Con toda esta información obtenida, se hicieron cargos de compras fraudulentas y otros actos no deseados, por lo que DSW tuvo que terminar las cuentas, comunicarse con los clientes y ofrecer soluciones y reembolsos, lo que le costó entre 6.5 y 9.5 millones de dólares en pérdidas.

Este tipo de ataques generan mucho más daño de lo que parecen ser y se pasan por tres etapas, incidente, administración y recuperación, cuando ha ocurrido una brecha de datos se tienen que medir y hacer las correspondientes acciones, dentro de las cuales se encuentran las siguientes:

- Reputación de imagen: Al ver que sus sistemas fueron vulnerados y que no tienen la debida seguridad ni protección, genera la desconfianza del público general, haciendo que la gente pierda confianza y los clientes terminan retirándose y buscando una alternativa o no lo ven como una opción atractiva por el pasado que tiene, este daño a la marca puede durar hasta 5 años en poder ser recuperada la confianza.
- Detención de los sistemas: En este contexto, se hace necesario suspender temporalmente las operaciones de todos los sistemas de la organización. Tal acción no solo ayuda a prevenir la propagación del ataque, sino que también facilita la recopilación de evidencia crucial para entender la brecha de seguridad y tomar medidas correctivas eficaces.
- Crear nuevas infraestructuras: Con los equipos que probablemente estaba trabajando estaban desactualizados o sin herramientas especializadas para detener o prevenir este tipo de ataques, por lo que

hay que hacer una nueva actualización de sistemas para poder estar protegido y así evitar otro incidente similar.

- Preparar acciones legales: Una vez investigado el caso, se tiene que hacer las diversas denuncias en caso de encontrar evidencia incriminadora y de esta manera llegar a juicio con los responsables que cometieron estos delitos.

Estos apartados junto con otros más hacen que como resultado, la empresa tenga que gastar muchísimo dinero, millones y millones de dólares para poder recuperarse, volver a operar y de esta manera continuar con el negocio, en caso de que se lo pueda permitir, ya que esto es perfectamente posible administrarlo en una gran empresa con un buen poder adquisitivo, pero si un incidente así le pasa a una mediana o pequeña empresa, el daño es mucho mayor y podría hasta dejarlo fuera de negocio indefinida o permanentemente por el daño causado.

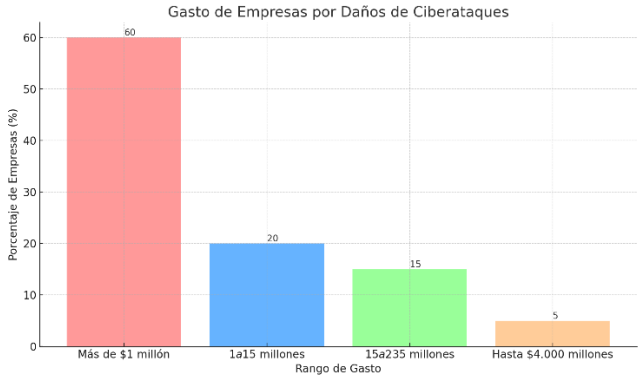


Fig. 2. Gráfico de las brechas de gasto de empresas por daños de ciberataque realizada por MinTIC de Colombia.

Dentro de estos ataques, se puede evidenciar que una gran parte de estos ataques se realizan el robo de las bases de datos, especialmente de las grandes empresas, los cuales tienen un banco importante de personas y credenciales las cuales se pueden hacer cosas como la comercialización, usurpación de identidad, entre otros.

Impacto en la Reputación de la Empresa: Los incidentes no solo tienen un impacto financiero directo, sino también pueden afectar la reputación de la empresa. Esto puede llevar a una pérdida de confianza de los clientes y socios, lo que a largo plazo puede ser más costoso que los daños inmediatos.

Costos Ocultos y a Largo Plazo: Además de los gastos obvios, como reparaciones o reemplazo de equipos, hay costos menos visibles como la disminución de la productividad, el tiempo perdido en la gestión del incidente, y posibles demandas legales. Estos costos pueden acumularse y ser significativos, especialmente para las pequeñas y medianas empresas.

Algunos aspectos para considerar sobre los costos y consecuencias de incidentes en ciberseguridad empresarial:

- Impacto en los Empleados: Los incidentes pueden afectar la moral y el bienestar de los empleados. Esto puede traducirse en una mayor rotación de personal, dificultades para atraer talento, y un descenso en la productividad.

- Costos de Recuperación y Prevención: Las empresas deben invertir en medidas de recuperación y prevención para evitar futuros incidentes. Esto incluye la formación de empleados, actualización de sistemas de seguridad, y posiblemente, seguros más costosos.

- Diferencias en el Impacto Según el Tamaño de la Empresa: Mientras que las grandes empresas pueden tener más recursos para recuperarse y absorber los costos, las pequeñas y medianas empresas son más vulnerables. Un incidente grave puede llevarlas al cierre, especialmente si no cuentan con seguros adecuados o planes de recuperación de desastres.

- Pérdida de Clientes y Mercado: Un incidente grave puede llevar a una pérdida temporal o permanente de clientes. Además, puede dar lugar a que competidores aprovechen la situación para captar una mayor cuota de mercado.

- Impacto en la Cadena de Suministro: Para las empresas que forman parte de una cadena de suministro, un incidente puede tener un efecto dominó, afectando a otros negocios y asociados.

Hoy en día existen múltiples formas en la cual uno pueda ser víctima de un ataque, entre los métodos existen técnicas como los mensajes o correos phishing, donde el atacante se hace pasar por una figura de autoridad y el usuario entrega voluntariamente sus datos personales. Ahora bien, existen ataques mucho más elaborados, los cuales van dirigidos directamente a grandes empresas donde se pueden encontrar una gran cantidad de datos. El ransomware es una de las amenazas más prevalentes y destructivas en el ámbito de la ciberseguridad. Este tipo de malware cifra los archivos del sistema de la víctima, exigiendo un rescate para su descifrado. A continuación, se describen los tipos más comunes de ataques de ransomware, destacando sus características y métodos de operación.Algunos tipos de ataques mas comunes son los siguientes:

- Locker Ransomware

El Ransomware de Bloqueo impide el acceso al dispositivo de la víctima, bloqueando la pantalla o el sistema operativo completo. Este ataque no cifra archivos individuales, sino que niega el acceso general al dispositivo. La víctima ve una notificación de rescate en la pantalla, instruyendo cómo proceder para desbloquear su dispositivo.

- Crypto Ransomware

El Ransomware de Cifrado es más sofisticado y dañino que el locker ransomware. Cifra archivos individuales o sistemas de archivos completos, haciendo inaccesibles documentos, bases de datos, fotos y otra información importante. Este ataque se caracteriza por permitir al usuario acceder al sistema operativo pero no a los archivos cifrados, solicitando un pago para obtener la clave de descifrado.

- Scareware

Aunque no es un ransomware en el sentido tradicional, el Scareware incluye falsos programas antivirus y aplicaciones de limpieza de sistemas que alegan haber encontrado problemas en el dispositivo de la víctima. Estos programas exigen pago para "limpiar" el sistema. A pesar de que no cifran archivos, utilizan tácticas de intimidación para extorsionar a las víctimas.

- Ransomware como Servicio (RaaS)

RaaS es un modelo de negocio en el que los desarrolladores de ransomware ofrecen su malware como un servicio a terceros. Los afiliados distribuyen el ransomware, mientras que los desarrolladores mantienen el software y cobran una parte del rescate. Este modelo ha permitido que individuos sin conocimientos técnicos lanzan ataques de ransomware.

- Ataques de Doble Extorsión

Los ataques de Doble Extorsión combinan el cifrado de archivos con la extracción de datos sensibles. Los atacantes amenazan con publicar o vender la información robada si el rescate no se paga, aumentando significativamente la presión sobre las víctimas para que cumplan con sus demandas.

- Ransomware dirigido

A diferencia de los ataques de ransomware más generalizados, los Ataques Dirigidos se enfocan en objetivos específicos, como organizaciones o industrias particulares. Los atacantes realizan una investigación previa para entender la infraestructura de TI de la víctima y diseñar un ataque que cause el máximo impacto, a menudo pidiendo rescates significativamente más altos.

Un estudio realizado por BitLife Media, hizo un gráfico viendo la cantidad de brechas de datos que han ocurrido entre 2019 y 2022.
Además de esto, el estudio también revela que los métodos de ransomware y accesos no autorizados son los principales ciberataques que se realizan.

Los ataques mediante ransomware son ataques los cuales el atacante encripta o priva de acceso a un equipo, base de datos, o cualquier dispositivo con información valiosa para el usuario y/o empresa y pide una compensación en forma de recuperar los datos, la compensación más común para la “recuperación” de sus datos es el pago de una determinada cantidad de dinero mediante criptomonedas para evitar ser rastreado.

Y los ataques mediante acceso no autorizados son ataques en el que se obtiene acceso a equipos de un individuo, ya sea particular como de una empresa y de esta manera tener acceso a información privilegiada, confidencial o sensible. Además, al tener acceso a estos equipos, el atacante puede ejecutar un virus de ransomware si tiene acceso a las máquinas con permisos de administrador.
Con todo lo anteriormente mostrado, corresponde hacerse la pregunta y decir: ¿quien se hace responsable de nuestros datos en caso de que sean filtrados?. El principal actor de quien tiene que proteger nuestros datos son a quienes se los damos y por ende, cae en ellos la responsabilidad de mantener nuestra información segura, sin embargo, como hemos visto con los gráficos y estudios anteriormente mencionados los ataques solo van en aumento y puede pasarle tanto a una pequeña como una grande empresa, por lo que siempre se corre el peligro de que se genere una brecha y nuestros datos queden expuestos, por lo que la ley tiene que hacerse cargo en caso de que estos incidentes ocurran. Sin ir más lejos, en 2019, la Comisión para el mercado financiero (CMF) reportó que Redbanc tuvo un ciber incidente en la casilla de Incidente Operacionales, donde se filtraron la información de más de 41.000 tarjetas de credito y debito.

Otro caso similar es lo que ocurrió en 2014, donde fue accedida a la equipos de MINSAL y tomaron información médica y datos personales de muchas personas dentro del sistema, quedando totalmente expuesta su información.

Problemas con la ley de protección de datos chilena
En el reglamento de la biblioteca del congreso nacional de Chile, la ley que hablaba sobre la protección de datos es la ley 19.628 esta ley es la que nos indica qué hacer en caso de que los datos de un ciudadano chileno sea vulnerado, modificado o compartido sin el consentimiento del propietario de los mismos y por ende infringir esta ley y aplicar la debida sanción. Esta ley sin embargo, no aplica para casos donde estos crímenes hayan sido cometidos de manera virtual, por lo que tiene que ser complementada.

La regulación permite la trata de datos personales sin el consentimiento del titular en distintas ocasiones, como fuentes accesibles al público y la trata de personas juridicas, trata de datos por parte de organismos publicos y datos relacionados a la salud. En este sentido se llega a considerar el consentimiento al punto de corresponder a una excepción a diferencia de un principio fundamental.

La ley no define lo suficiente el dato personal para diferenciarlo entre un dato personal y un dato estadístico(dato que no puede ser asociado a un individuo en específico), dejando la posibilidad a la difusión de datos que constitucionalmente se encuentran consagrados, como es el caso del data leak de SERVEL del año 2022.La regulación no define específicamente el consentimiento respecto a las nuevas tecnologías y se tiene incerteza respecto a qué autorización es necesaria y como cuando se habla de datos sensibles y datos personales.
La ley no establece si se aplica a individuos u organizaciones que traten datos de nacionales, dejando la posibilidad de impunidad frente a brechas de datos personales realizadas a organizaciones fuera del territorio nacional.
La ley no establece específicamente quienes intervienen en el tratamiento de datos.[2]

Esta ley posee los siguientes artículos en los cuales se menciona la infracción de la ley de protección de datos.

En el artículo 16 se dice que si el responsable del registro o banco de datos no se pronuncia sobre la solicitud del requirente dentro de dos días hábiles, o la deniega por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente[3]

Y en el artículo 17 en particular, se establece que los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas sean requeridas por organismos públicos o por el titular de los datos. Además, se establecen las sanciones por infracciones a las normas de protección de datos personales, que pueden incluir multas, clausura temporal o definitiva del registro o banco de datos, y la responsabilidad civil por los daños y perjuicios causados.[4]

Entre las sanciones en caso de haber incumplimiento de esta ley, se encuentra la clausura temporal o definitiva del banco de datos y el dueño de este hacerse responsable de los potenciales daños causados por esta filtración. Además de esto,en caso de que el dueño de los datos sea negligente con la entrega o lo solicitado por el dueño de estos, se le aplicará una sanción con el pago de una multa que puede ir desde las dos a cincuenta UTM (Unidad de Tributarias Mensuales), haciendo que solamente reciba una pena monetaria el atacante y nuevamente pueda ser libre de realizar crímenes similares, a diferencia de otras leyes como España, o argentina.[5][6]

La ley anteriormente mencionada no toma en cuenta los casos en los cuales se haya perpetrado esta infracción mediante el uso de algún ordenador, computador o base de datos, por lo que se tiene que complementar con la ley 19.223, la cual habla principalmente del ataque directo de equipos, ya sea utilizándolos, de manera malintencionada, tratamiento de información, difusión, entre otros, sin embargo, la ley habla de casos muy generales, a esto hay que sumarle que esta ley posee una única planta y sus sanciones no son claras fuera de un nivel de gravedad, por lo que da a lugar a múltiples vacíos legales y evasiones de ley por lo ambiguo de esta.[7][8]

III. Comparación entre la ley chilena de protección de datos y otros países

En Argentina , la cual es la ley N°25.326 esta ley por sí sola no funciona para poder ser aplicada en caso de que los datos hayan sido comprometidos en algún medio digital, pero esta ley si esta afiliada a la normativa de Ciberseguridad que tiene Argentina, por lo que sí está relacionada la protección de datos con la seguridad informática, a diferencia de la ley Chilena, donde no se reconocen o se asocian a una normativa informática o de ciberseguridad, solamente a la ley 19.223.[9][10]

Acompañado de lo anteriormente mencionado, en el capítulo VI de la ley argentina, se encuentra el apartado de Sanciones, en la cual se habla de sanciones administrativas y penales, donde en las sanciones administrativas de pueden tener penas con multas desde los mil pesos hasta cien mil pesos, clausura o cancelación del banco de datos, suspensión, entre otros cargos, y en el caso de las penales, dependiendo si se incorpora con el artículo 117 bis del Código penal o el artículo 157, en el caso del primero, se puede tener una pena de prisión desde un mes hasta tres años dependiendo de la gravedad que se estime, y en el caso del segundo artículo, puede sufrir de una pena de un mes hasta dos años en caso de revelar información que tuviera que estar preservada por disposición de una ley.[11]

Otro país en donde se puede ver una gran diferencia es con España, la cual es la ley Orgánica 7/2021, la cual es la ley de protección de datos española. En esta ley se establecen múltiples cosas, Una de las mayores diferencias especialmente con la ley de Chile, es que ahora existen múltiples autoridades las cuales regulan, previenen y detectan estas infracciones penales, como las Fuerzas y cuerpos de seguridad, administraciones penitenciarias, Dirección adjunta de vigilancia aduanera de la agencia estatal administración tributaria, entre otras entidades.

Junto a lo anteriormente mencionado, las penas en caso de cometer infracciones son mucho mayores y más graves, por ejemplo, la multa más alta que un ciudadano chileno puede recibir por incumplimiento de la ley 19.628 es de 50 UTM, o equivalente a $3.198.000 millones de pesos chilenos o aproximadamente 3600 dólares, por el contrario, la ley Española, si se hace la falta más grave que sería una infracción de tipo muy grave, la multa puede rondar entre los 360.001 euros hasta 1.000.000 de euros o más de 1 millón de dólares.

Con estas comparaciones anteriormente vistas, podemos concluir que la ley de protección de datos chilena le falta mucho desarrollo para poder estar a la altura de los tiempos actuales donde este tipo de problemas se desarrollan principalmente en internet, por lo que se tiene que hacer algo al respecto para poder solucionar este problema y arreglar los vacíos legales que posee esta ley.

Menciones sobre la legislación penal sobre la protección de datos y cibercrimen

Las leyes anteriormente mencionadas son un antecedente de que, a pesar de que si existían protección de datos como tal, se hablaba de manera muy general y dejaba de lado el ámbito informático, por lo que se podían dar a interpretación o invalidación por lo ambiguo de este. Acá es donde, el convenio de Budapest, se genera la nueva ley de protección de datos (2022), donde esta se especializa y deroga la ley 19.223 (1993) y modifica otros cuerpos legales.[12]

La ley 21.459, toma en cuenta las primeras disposiciones y definiciones del acuerdo de Budapest, de modo que establece y tipifica los delitos informáticos, de la misma forma toma en cuenta la manera para procesar estos delitos y la forma de investigarlos. Finalmente, la ley establece las penas asociadas a estos delitos.[13]

Una de las mayores diferencias respecto a la ley 19.628, es que la protección de datos ahora si abarca los delitos informáticos, dentro de los cuales se incluyen delitos como el ataque a la integridad de un sistema informático, acceso ilícito a un sistema informático, falsificación de documentos, sabotaje informático, entre otros informáticos del mismo tipo. Junto a esto, con esta ley ahora la multa no solamente es mucho más alta la cual puede ir desde las 100 a 500 UTM, sino que con esta nueva ley ahora se pueden establecer penas de presidio menor a mayor, por lo que ahora con si es posible tener una sanción penal e ir a prisión por incumplimiento de ley, el cual debe ser evaluado con un abogado.

Con todo lo anteriormente mencionado con la nueva ley, podemos concluir que es un avance significativo al compararla con la ley 19.223 por ser muy poco específica y no abarcar específicamente la figura de la protección de datos personales, y una cantidad de posibles casos donde se pudieran cometer crímenes sobre esa

materia.

IV. Ley 21.096, acercamiento a una nueva ley de protección de datos

La ley 21.096 (2018) establece y consagra a nivel constitucional el derecho a la protección de datos personales, corresponde a un avance significativo hacia una ley de protección de datos, sin embargo, deja al dominio legal o de la ley la consagración de los derechos ARCO, siendo estos: derecho al acceso, rectificación, cancelación y oposición dispuestos en la ley 19.628.

Entre los derechos ARCO que existen, se especifican los siguientes:

A. Derecho de acceso o información: Se puede solicitar información de los datos, como propósito de almacenamiento, lugares de almacenamiento,entre otros.

B. Derecho rectificación o modificación: Se puede solicitar la modificación de los datos cuando son inexactos, erróneos, incompletos, entre otros.

C. Derecho de oposición: Evitar que los datos sean usados con otros fines, como publicitarios, investigación de mercado, entre otros

D. Derecho de bloqueo: Suspensión de banco de datos bajo ciertas circunstancias.

V. Necesidad de una nueva legislación sobre la protección de datos.

Desde principios de la década el fenómeno de data leak se ha hecho un fenómeno cada vez más frecuente, de acuerdo al portal de ciberseguridad de entel es posible apreciar que el tuvo un aumento exponencial el año entre los años 2021-2022, como es posible observar en el presente gráfico.
Incremento de Eventos Registrados: Entre 2021 y 2022, hubo un incremento del 69% en la cantidad de eventos de filtración de datos registrados, y solo en los primeros 9 meses de 2023, se observó un aumento adicional del 22% sobre el total de eventos de 2022.
Filtraciones de Datos en Chile: Se identificaron 33 eventos de filtraciones de datos en Chile, involucrando a 14 actores de amenaza diferentes. Algunos de los actores más activos incluyen a Sombraman1919, Kung_Liao, y LeakBase, quienes se enfocan principalmente en compañías de telecomunicaciones y gobiernos .
Contexto en América Latina: En total, se registraron 295 eventos de filtraciones de datos en América Latina, con Brasil, México y Chile siendo los países más afectados. Estos incidentes son atribuidos en parte a la estabilidad de la moneda local y el desarrollo tardío de leyes y políticas de TI en la región.[14]

Este patrón refleja un aumento constante en la actividad de ciberamenazas en la región, especialmente en plataformas de Deep y Dark Web, y resalta la necesidad de medidas de seguridad y prevención más robustas en la industria TI.

Es posible además, apreciar en el siguiente gráfico que en comparación a otros países de Latinoamérica, este corresponde al tercer mayor país con filtraciones de datos después de Brasil con el primer lugar y México con el segundo.[15]

Fig. 3. Gráfico de las leaks de datos ocurridos durante el año 2023 realizado por Entel.

Entre otras formas de evidenciar el aumento de ciberataque se puede observar en el presente gráfico sobre los ataques por ransomware a los datos de organizaciones en Chile. Es evidente que diversas organizaciones actualmente manejan como método de identificación de usuario o como dato para almacenar información del usuario, como por ejemplo Correos de Chile, SP digital, entre otros. Organizaciones que pueden en algún momento ser vulnerables a ataques a sus bases de datos, en donde almacenar estos datos personales como el Rol Único Tributario no se justifica.

Datos personales a los cuales actualmente es posible acceder a través de Rol Único Tributario/Nacional son:

A. Nombre completo.
B. Fecha de nacimiento.
C. Lugar de nacimiento.
D. Edad.
E. Sexo.

F. Estado civil.
G. Pertenencia a un grupo étnico.
H. Familiares.
I. Estado de salud.
J. Local y mesa de votación de elecciones.
K. Becas ganadas
L. Listado de fármacos que se consumen
M. Frecuencia de consultas médicas
N. Bienes inmuebles que se poseen
O. Historial de compras en retail
P. Medios de pago utilizados
Q. Lugares de trabajo
R. Militancia política

Es posible evidenciar que el solo al acceder al RUT/RUN de una persona es posible obtener una gran cantidad de datos personales a través de los propios servicios del Estado o bien en los repositorios de páginas en los cuales se permite buscar a una persona por RUT/RUN, asimismo, es posible encontrar el RUT/RUN de una persona conociendo su Nombre completo.[16]

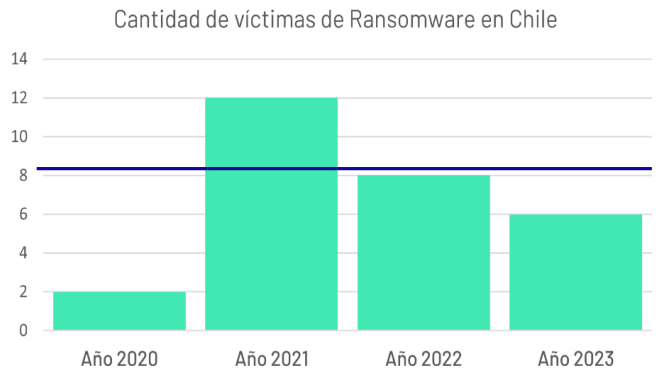


Fig. 4. Gráfico de cantidad de víctimas por ransomware en Chile proporcionado por Entel.

Es difícil determinar un número exacto de víctimas por ransomware en Chile, ya que no todas las empresas o instituciones reportan los ataques públicamente. Sin embargo, existen algunos datos que nos permiten estimar el impacto de este tipo de ataques en el país, De acuerdo a los datos disponibles, podemos estimar que ha habido al menos 28 víctimas de ransomware en Chile desde 2020 al 2023. Sin embargo, es importante destacar que esta cifra podría ser mayor, ya que no todos los ataques se reportan públicamente.Ejemplo de una vulneración a los datos personales corresponde al fenomeno sucedido año 2020, en el cual se registra un Data Breach masivo sobre la institución de Carabineros de Chile, exponiendo más de 10.000 documentos confidenciales y los datos personales de todos los funcionarios de la institución entre ellos, nombres, RUTs asociados, sexo, zona y comisarías, información de carácter sensible que pone en riesgo la integridad de los miembros del cuerpo policial.

El año 2021, en las elecciones municipales de mayo el organismo SERVEL sufrió una masiva vulneración y brecha de datos personales (data leak), correspondiente a los datos de 15 millones de personas de territorio nacional, entre cuyos datos existían; RUTs asociados a cada nombre, género, edad, y datos de pertenencia a pueblo originario. Nuevamente, el año 2022 el organismo SERVEL filtro los datos de las 15 millones de personas, correspondientes esta vez, RUTs asociados a cada nombre, género, edad, militancia, habilitación para votar y preferencia de voto.

El año 2023, octubre se registra un data breach sobre la información de 10 millones de chilenos, cuyos datos corresponden a RUTs, nombre asociado, sexo.
Los efectos de estos Data Leak corresponden a nuevas formas de que las personas sean vulneradas ya sea utilizando estos datos para realizar elaboradas estafas de phishing o spoofing, tomando en cuenta que se hacen uso de los datos personales de las personas. En este ámbito también es posible observar un aumento exponencial y generalizado de ataques phishing en Latinoamérica, de acuerdo a Kaspersky existe un aumento del 617% durante los 12 meses anteriores a julio de 2023 en comparación a los 12 meses anteriores a julio del año anterior. Así mismo es posible observar que Chile corresponde a uno de los países con mayor porcentaje de ataques por phishing en el mundo.
Las estadísticas de Kaspersky sobre ataques de phishing revelan una preocupante tendencia en el aumento y la sofisticación de estas amenazas en los últimos años:

Estadísticas Generales de 2022: Kaspersky bloqueó más de 500 millones de intentos de acceder a sitios web fraudulentos en 2022, lo que representa el doble en comparación con las cifras de 2021. Los servicios de entrega, mensajería y plataformas de criptomonedas fueron los anzuelos más comunes utilizados en estos ataques. Los usuarios de servicios de entrega fueron los más afectados, constituyendo el 27.38% de todos los intentos bloqueados, seguidos por tiendas en línea (15.56%), sistemas de pago (10.39%) y bancos (10.39%). Además, se observó un aumento en la distribución de ataques a través de mensajeros, con la mayoría de los intentos bloqueados provenientes de WhatsApp (82.71%), seguido de Telegram (14.12%) y Viber (3.17%).[17]

Estadísticas de Malware en 2023: Durante el período reportado en 2023, Kaspersky detectó un promedio de 411,000 archivos maliciosos por día, con un aumento del 3% en comparación con el año anterior. En particular, se observó un aumento del 53% en ataques que involucran documentos maliciosos de Microsoft Office y otros tipos. Kaspersky también notó un aumento significativo en el uso de backdoors para infiltrarse en sistemas de manera no detectada.[17]

Estadísticas Específicas de Phishing en 2023: En los primeros

diez meses de 2023, Kaspersky identificó 30,803,840 ataques de phishing dirigidos a tiendas en línea, sistemas de pago y bancos. Las plataformas de comercio electrónico fueron el objetivo principal, representando el 43.5% del total de ataques (13,390,142 ataques). Las páginas de phishing que imitaban plataformas de compras populares como Amazon, eBay, Walmart, AliExpress y Mercado Libre sumaron 6,232,882 en los primeros diez meses de 2023. Apple fue consistentemente el señuelo más popular, con intentos de phishing que utilizaban su nombre alcanzando 2,844,828 en el mismo período.

Estos datos subrayan la creciente amenaza de los ataques de phishing y la importancia de implementar medidas de seguridad robustas para protegerse contra estas tácticas cada vez más sofisticadas.

Se hace necesario una legislación más específica y atingente a los problemas actuales, teniendo en cuenta que el cibercrimen y la tecnología son algo que están en constante evolución.

VI. Nuevo Proyecto de ley: Ley de protección de Datos

El nuevo proyecto de ley actualmente se encuentra en tercer trámite constitucional y constituye la consagración del derecho de protección de datos. Así mismo, es posible desglosar los siguientes puntos del nuevo proyecto:

A. Creación de la Agencia de Protección de datos Personales, organismo público que tiene por objetivo velar por la efectiva protección de los derechos consagrados en la ley

B. La ley se aplicará cuando la persona en cuestión se encuentre en territorio nacional, en este sentido se toma en cuenta que el mandatario independiente del lugar de establecimiento o constitución, realice la trata de datos personales a nombre de un responsable o constituido en territorio nacional. Especificando también cuando, el responsable o el mandatario no se encuentren en territorio nacional, pero sus operaciones de trata de datos personales fuesen destinados a titulares que se encuentren en Chile.

C. Se definen los derechos ARCO, tales son personales, intransferibles y no pueden limitarse por ningún acto o convención.

D. El tratamiento de datos personales requiere el consentimiento del titular, salvo en casos específicos como: obligaciones económicas, obligaciones legales, obligaciones de contrato, para el ejercicio de un derecho ante los tribunales u órganos públicos.

E. El tratamiento de datos personales sensibles requiere el consentimiento expreso del titular, o en el caso específico de que ya los haya hecho públicos, cuando resulte indispensable para salvaguardar la vida o salud de una persona, y en materia judicial. Aquellos datos sensibles corresponden a información relativa a la salud y al perfil biológico, de carácter biométrico y referente a niños, niñas y adolescentes

F. Las obligaciones del responsable de datos es deber informar al titular, asegurar que el tratamiento sea lícito, informar de manera precisa, suprimir o anonimizar los datos cuando esto sea necesario y cumplir con el resto de deberes y principios que establece la ley.

En suma, la nueva legislación corrige la ausencia de un organismo fiscalizador que se encargue de velar por la protección de datos personales, además de tomar en cuenta cuando se lleve a cabo la trata de datos personales de nacionales por organismos fuera de Chile. Define específicamente los límites del consentimiento del titular respecto a los datos y responsabiliza al organismo que almacene los datos de informar al titular sobre las acciones a realizar sobre estos.

VII. Estándar Europeo de la regulación de protección de datos y el Nuevo Proyecto de ley

Una vez revisada la ley de protección de datos de Chile, sus inicios, evolución y futuro es posible comparar que tan completa está en relación al reglamento general de protección de datos (RGPD) de la Unión Europea. Debido a la extensión del reglamento europeo será desglosado en los siguientes puntos:[18]

A. Ámbito de aplicación: El reglamento aplica a todas las organizaciones que procesen datos personales de residentes en la Unión Europea, independientemente de la ubicación de la organización

B. Principios básicos:
   1. El procesamiento de datos debe realizarse de manera lícita, leal y transparente para el titular de los datos.
   2. Los datos personales deben recogerse con fines específicos y explícitos y no deben procesarse de manera incompatible con estos fines.
   3. Se deben recoger solo los datos estrictamente necesarios para la finalidad prevista.
   4. Los datos deben ser precisos y estar actualizados.
   5. Los datos personales deben conservarse solo el tiempo necesario para la finalidad del procesamiento.

C. Derechos de los interesados:
    1. Las personas tienen derecho a obtener confirmación de si se están procesando sus datos personales y, en caso afirmativo, a acceder a estos datos.
    2. Los titulares de datos tienen derecho a corregir datos inexactos o incompletos. Las personas tienen derecho a que se borren.
    3. Las personas tienen derecho a que se borren sus datos personales en determinadas circunstancias.
    4. Los titulares de datos tienen derecho a recibir sus datos personales en un formato estructurado y legible, y a transmitir esos datos a otra organización.

D. Responsabilidad y rendición de cuentas: Las organizaciones son responsables de demostrar el cumplimiento de los principios del Reglamento y deben implementar medidas para garantizar la protección de datos personales.

E. Delegado de protección de datos (DPD): Algunas organizaciones deben designar un DPD, un responsable de supervisar la conformidad con el reglamento.

F. Notificación de violaciones de datos: Las organizaciones están obligadas a notificar a la autoridad de control y, en algunos casos, a los titulares de datos, en caso de una violación de seguridad de los datos

G. Transferencias internacionales: Las transferencias de datos personales fuera de la Unión Europea solo están permitidas bajo ciertas condiciones.

Al realizar una comparación entre el reglamento europeo y la legislación chilena actual (19.628), es posible advertir las distintas falencias y ausencias existentes respecto a la protección de datos personales; como la ausencia de un órgano fiscalizador, la inexistencia de la hipótesis de que un tercero preste sus servicios de trata de datos fuera del país a un nacional en el ámbito de la territorialidad, el problema de no definir específicamente qué es un dato personal en comparación al reglamento, como también alguna especificación respecto a datos de carácter sensible, la definición del principio de consentimiento queda al debe en comparación a la europea.[19][20]

La nueva legislación en relación al reglamento corresponde a un avance ya que implementa ciertas normativas de la regulación europea, entre ellos toma la territorialidad de la ley, los principios básicos, los derechos de los interesados, e incluso adopta la creación de un delegado de protección de datos en la normativa europea y agrega el carácter general que representa la agencia de protección de datos, ya que el delegado de protección de datos debe existir para que vele por la seguridad de los datos y el cumplimiento de la normativa, mientras que la agencia de protección de datos es un organismo general que fiscaliza, finalmente es posible evidenciar la diferencia existente entre la extensión respecto a las extensiones del reglamento en comparación con la nueva normativa chilena.[21]

VIII. Posibles efectos de la nueva legislación

Tomando en consideración la nueva normativa a llegar en los próximos años es necesario evaluar cuáles serían las consecuencias respecto a los efectos que esta legislación podría tener en cuanto a la protección de datos personales. De esta forma es posible asumir, que las responsables de los datos personales hagan una re evaluación y reestructuración respecto a qué datos son necesarios para realizar sus servicios. Es además imperativo crear otros medios por los cuales se puedan reemplazar estos métodos de identificación de usuarios como lo es el RUT/RUN. Otro efecto no inmediato de la ley corresponde a la probable desaparición de los sitios de búsqueda de personas por medio de Rol Unico Tributario, esto tomando en cuenta que las legislaciones y aplicaciones de la ley tienen un efecto transitorio en cuanto a respecta a su promulgación y su entrada en vigencia, el cual es necesario para la correcta adaptación de las organizaciones respecto a esta nueva legislación. En suma, es plausible asumir que los datos de las personas nacionales ya no estarán disponibles de la manera que actualmente se presenta o disponen en internet.[22]

La introducción de nueva normativa sobre la protección de datos personales conllevará varios cambios importantes:

- Reevaluación de la Necesidad de Datos: Las organizaciones tendrán que revisar qué datos personales son realmente necesarios para sus operaciones y servicios. Esto implica una reestructuración de sus prácticas de recolección y procesamiento de datos.

- Búsqueda de Alternativas al RUT/RUN: Será crucial desarrollar métodos alternativos para la identificación de usuarios, reduciendo la dependencia del Rol Único Tributario o Rol Único Nacional como principales medios de identificación.

- Impacto en Sitios de Búsqueda de Personas: Probablemente, los sitios web que permiten la búsqueda de personas utilizando el RUT/RUN experimentarán cambios significativos o incluso podrían desaparecer, en conformidad con las nuevas regulaciones de privacidad.

- Período Transitorio y Adaptación: La implementación de la nueva legislación incluirá un período transitorio que permitirá a las organizaciones adaptarse a las nuevas normas. Este período es crucial para garantizar una transición suave y el cumplimiento efectivo de la ley.

- Disponibilidad de Datos en Internet: Es probable que la información personal de los ciudadanos ya no esté disponible en Internet de la manera en que lo está actualmente, lo que refleja un enfoque más estricto en la privacidad y protección de datos.[24]

IX. Conclusion

Desde los albores de la era informática, los ataques cibernéticos y los incidentes relacionados con la seguridad de la información han sido una amenaza persistente. En la actualidad, con la omnipresencia de Internet y la proliferación de servicios digitales, la información personal y sensible está cada vez más expuesta, incrementando el riesgo de filtraciones y uso indebido de estos datos.

Este informe ofrece un análisis detallado de la situación actual de la ley de protección de datos personales en Chile, explorando su evolución histórica, su estado presente y las perspectivas a futuro. Se enfoca en el proceso de reforma legislativa en curso, que busca actualizar la ley 19.628 a los estándares contemporáneos y abordar los retos actuales en materia de ciberseguridad. La investigación destaca las limitaciones de la legislación vigente, comparándola con las normativas de otros países y en particular con la legislación europea. El estudio concluye enfatizando la necesidad imperiosa de reformar la ley chilena de protección de datos para adecuarla a las realidades del mundo digital actual, y examina las implicaciones que el nuevo proyecto de ley podría tener en el tratamiento de datos personales por parte de las organizaciones, invitando a una reevaluación de sus prácticas en este ámbito.

El fenómeno de los ataques informáticos y los incidentes cibernéticos ha sido una constante desde los primeros días de la informática. En la era actual, donde la interconexión a través de Internet y el uso de diversas plataformas digitales son omnipresentes, la exposición de información personal y sensible se ha incrementado dramáticamente. Esto conlleva un mayor riesgo de que los datos personales sean filtrados y utilizados de manera indebida, una preocupación creciente tanto para individuos como para organizaciones.

Abarcando su desarrollo histórico, desde su promulgación en 1999 hasta la actualidad, se analiza cómo ha evolucionado esta legislación frente a los desafíos emergentes en el campo de la ciberseguridad. Se observa que, a pesar de los esfuerzos iniciales, la ley ha quedado rezagada frente a las demandas del entorno digital moderno. Actualmente, Chile se encuentra en un proceso de transformación legislativa, buscando actualizar la ley 19.628 para alinearla con los estándares actuales de protección de datos y ciberseguridad. Este esfuerzo de modernización apunta a abordar las deficiencias identificadas en la ley vigente, especialmente en lo que respecta a la prevención de filtraciones de datos y la protección contra el uso indebido de información personal.

El análisis incluye una comparación detallada entre la ley chilena y las legislaciones de otros países, destacando cómo ciertas regiones, especialmente Europa con su Reglamento General de Protección de Datos (GDPR), han establecido marcos legales más robustos y efectivos en este ámbito. Esta comparación internacional resalta las áreas en las que Chile podría mejorar para garantizar una mejor protección de los datos personales.

Finalmente, el informe subraya la urgencia de una reforma legislativa en Chile en materia de protección de datos personales. Se enfatiza la importancia de adaptar la legislación a las necesidades y desafíos del mundo digital contemporáneo, considerando los posibles efectos que el nuevo proyecto de ley podría tener en el manejo de datos personales por parte de las organizaciones. Esta reevaluación legislativa es crucial para asegurar que tanto las entidades privadas como las públicas manejen los datos personales con los más altos estándares de seguridad y responsabilidad, adaptándose a un panorama global cada vez más enfocado en la ciberseguridad y la privacidad de datos.

X. Referencias

[1] Tipifica figuras penales relativas a la informática, ley N° 19223, Biblioteca del Congreso Nacional de Chile, 7 de Junio de 1993. Disponible en el siguiente enlace: https://www.bcn.cl/leychile/navegar?idNorma=30590&buscar=ley%2B19223

[2] Sobre protección de la vida privada, Ley N° 19623, Biblioteca del Congreso Nacional de Chile, 28 de Agosto de 1999, Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=141599

[3] Establece normas sobre delitos informáticos, deroga la ley N° 19223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest , Ley N° 21459, Biblioteca del Congreso Nacional de Chile, 20 de Junio del 2022, disponible en:Ley Chile - Ley 21459 - Biblioteca del Congreso Nacional (bcn.cl)

[4] "Ley 21.096, que consagra el derecho a protección de los datos personales," Biblioteca del Congreso Nacional de Chile, 2018. [En línea].Disponible: [https://www.bcn.cl/leychile/navegar?idNorma=1119730&tipoVersion=0

[5] "Nueva ley de datos personales en Chile," WeLiveSecurity, 2023. [En línea]. Disponible: [https://www.welivesecurity.com/es/privacidad/nueva-ley-datos-personal es-chile/].

[6] "Evaluación de la Ley 19.628, Cámara de Diputados," Evaluación De Ley, 2019. [En línea]. Disponible: [https://www.evaluaciondelaley.cl/wp-content/uploads/2019/07/informe_final_ley_19628_con_portada.pdf].

[7] "Ley 21.096, acercamiento a una nueva ley de protección de datos: Historia de La Ley::Historia de la Ley (bcn.cl)," BCN, 2023. [En línea]. Disponible: [https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/7551/].

[8] "Proyecto de ley de protección de datos," Cámara, 2023. [En línea]. Disponible: [https://www.camara.cl/cms/noticias/2023/05/08/tratamiento-de-datos-personales-tendra-nuevo-marco-legal/].

[9] "Nueva ola de correos extorsivos circula en Chile y otros países," WeLiveSecurity, 2023. [En línea]. Disponible: https://www.welivesecurity.com/laes/2023/07/06/nueva-ola-de-correos-extorsivos-circula-en-chile-y-otros-paises/].

[10] "Vulneración de datos personales: lo privado en público," CiperChile, 2022. [En línea]. Disponible: [https://www.ciperchile.cl/2022/05/06/vulneracion-de-datos-personales-lo-privado-en-publico/].

[11] "Aumento de los ciberataques en Chile en 2023: Lo que dicen las cifras," Guioteca, 1 abril 2023. [En línea]. Disponible: [https://enteldigital.cl/blog/chile-registra-aumento-de-ciberataques-duran te-primer-trimestre-del-2023-y-es-el-tercer-pa%C3%ADs-con-m%C3% A1s-v%C3%ADctimas-de-latam].

[12] "El sumario del Servel que terminó con funcionario destituido por masiva filtración de datos personales," BioBioChile, 2023. [En línea]. Disponible: [https://www.biobiochile.cl/especial/bbcl-investiga/noticias/articulos/2023/05/05/el-sumario-del-servel-que-termino-con-funcionario-destituido-por-masiva-filtracion-de-datos-personales.shtml].

[13] "Panorama de amenazas en América Latina 2023," Kaspersky, 2023. [En línea]. Disponible: [https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/#:~:text=Nueva%20epidemia%3A%20el%20phishing%20se,a%205%20ataques%20por%20minuto].

[14] "Hackeo a Carabineros en medio de la crisis expone 10.515 archivos: entre ellos hay datos de inteligencia," CiperChile, 2019. [En línea]. Disponible: [https://www.ciperchile.cl/2019/10/29/hackeo-a-carabineros-en-medio-de-la-crisis-expone-10-515-archivos-entre-ellos-hay-datos-de-inteligencia

[15] J. Carey, A. Pinochet y C. Silva, "Los cambios que establece la nueva ley de datos personales en Chile", Lex Latin, 2021. [En línea]. Disponible en: . [https://www.carey.cl/wp-content/uploads/filebase/Lex-Latin-Los-cambi os-que-establece-la-nueva-ley-de-datos-personales-en-Chile.pdf].

[16] "Fundación Datos Protegidos. (2023). No doy mi Rut y tengo mis razones. [En línea]. Disponible: [https://datosprotegidos.org/no-doy-mi-rut/].

[17] "Ciberataque expone información de 10 millones de chilenos en foros de hackers," ElMostrador, 2023.[Enlínea].Disponible:[https://www.elmostrador.cl/noticias/sin-editar/2023/10/18/ciberataque-e xpone-informacion-de-10-millones-de-chilenos-en-foros-de-hackers/].

[18] "Desafíos para adecuarse al margen europeo," Revistas CES, [En línea]. Disponible: [https://revistas.ces.edu.co/index.php/derecho/article/view/6806].

[19] "Carta fundamental Europea, artículo de datos personales," Consilium, [En línea].Disponible: [https://www.consilium.europa.eu/es/policies/data-protection/#:~:text=El%20art%C3%ADculo%208%20de%20la,conciernan%20y%20a%20obt ener%20su%20rectificaci%C3].

[20] "Reglamento Europeo de protección de datos personales," Europa, [En línea]. Disponible: [https://eurlex.europa.eu/legalcontent/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504].

[21] "Las claves sobre el nuevo reglamento europeo de protección de datos," Signaturit, [En línea]. Disponible: [https://blog.signaturit.com/es/las-claves-sobre-el-nuevo-reglamento-europeo-de-proteccion-de-datos].

[22] "Una breve historia de los virus informáticos y los que nos depara el futuro", Kaspersky,[En linea], Disponible:[https://latam.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds]

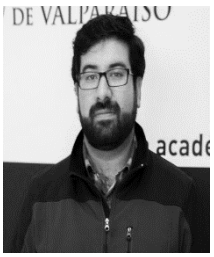
[23] "Cuanto gasta una empresa para recuperarse después de un ciberataque". La Republica, 27 de Julio de 2019, [En linea], Disponible [https://www.larepublica.co/internet-economy/cuanto-gastan-las-empresas-para-recuperarse-despues-de-un-ciberataque-2889536]

[24] Informe del costo de una vulneracion de datos 2020, Autor: IBM [En linea],Disponible: https://sadvisor.com/wp-content/uploads/2021/05/LA-Spanish_CostOfADataBreachReport_2020_eBook_ES.pdf

XI. BIOGRAFIAS

Pamela Hermosilla nacida en Valparaíso, Chile, el 8 de octubre de 1974. Graduada de Universidad Téecnica Federico Santa Naría (UTFM Ingeniero Civil en Informática (UTFSM), Diplomada en Comercio Electrónico y Logística Empresarial (UTFSM), Auditor Interno ISO 9001 (Brain & Cia Consultores), MBA of Chief Information Officer CIO (Abet Open University), Diplomada en Docencia Universitaria de la Pontificia Universidad Católica de Valparaíso (PUCV), Diplomada en Formación Virtual Universitaria (PUCV), Symposium for Entrepreneurship Educators (Luksic Scholars – Babson College). Asesorías: miembro del Consejo Público Privado de la red Fortalece Pyme, Valparaíso - Corfo, integrante del Boardd de Directores, de la incubadora Chrisalys PUCV. Desarrollo profesional en áreas de Aseguramiento de calidad en gestión de proyectos, Planificación estratégica organizacional, Rediseño curricular basado en competencias, Habilidades de Innovación y emprendimiento en estudiantes de ingeniería, Gamificación en el proceso de enseñanza y aprendizaje.

Dr.(c)Sebastián Berrios nacido el 7 diciembre de 1986.Actualmente candidato a doctor en Ingeniería informática en la Pontificia Universidad Católica de Valparaíso. Graduado de Ingeniería Civil en Computación e Informática en la Universidad De Las Américas. Magíster en Ciencias de la Ingeniería y Magíster en Ingeniería en Informática en la Pontificia Universidad Católica de Valparaíso. Actualmente docente del área de Ciberseguridad y Administrador de TI de la escuela de ingeniaría informática de la Pontificia Universidad Católica de Valparaíso. Cursando un Diplomado de Inclusión en Educación en la Pontificia Universidad Católica de Valparaíso, con una duración de 140 horas. Además, se cursó un Diplomado en Seguridad de la Información de 132 horas en la Universidad de Chile y un Diplomado en Ciberseguridad de 96 horas en la misma universidad. También se obtuvo un Diplomado en Ciberseguridad de 100 horas en el Instituto Profesional IACC.



Dr. Héctor Allende destacado profesional en el campo de la ingeniería informática. Obtuvo su Doctorado en Ingeniería Informática en 2015 en la Universidad Técnica Federico Santa Maria, Chile, un reconocido centro de estudios en la región. Antes de ello, en 2009, completó su Magíster en Ciencias de la Ingeniería Informática y se graduó como Ingeniero Civil Informático en la misma universidad. Su formación académica en estas prestigiosas instituciones le ha proporcionado una sólida base en la ingeniería informática, permitiéndole desarrollarse y destacarse en su campo.