CUANDO PERDEMOS EL PODER SOBRE NUESTRO DINERO. NOCIONES DE CIBERSEGURIDAD EN LA EMPRESA FAMILIAR [1]

WHEN WE LOSE POWER OVER OUR MONEY. NOTIONS OF CYBERSECURITY IN THE FAMILY BUSINESS

Por *María Raquel BURGUEÑO* [(*)]

RESUMEN: El presente trabajo tiene como objetivo generar conciencia dentro de las empresas familiares sobre las vulnerabilidades, amenazas y exploits que se observan en el ecosistema de las comunicaciones electrónicas y particularmente en el patrimonio digital que tanto pymes como empresas familiares han venido construyendo desde el surgimiento de las Tecnologías de la Información y la Comunicación (TIC). Así como en el plano analógico las pymes y empresas familiares han sabido resguardar celosamente secretos industriales, fórmulas de elaboración de productos y modelos de gestión de procesos, en el universo digital es preciso afianzar conductas relativas a los Sistemas de Gestión de la Seguridad de la Información, aprendiendo a desarrollar Políticas de Seguridad de la misma, sensibilizar a directivos, empleados, proveedores y clientes consumidores y fortalecer los aspectos técnicos con herramientas específicas de ciberseguridad. El daño reputacional por exfiltración de sus bases de datos -con la consecuente pérdida de información y datos personales de clientes y consumidores- será otra de las nuevas temáticas a abordar en los tiempos venideros, máxime frente a la realidad imperante en la que el cibercrimen se erige en la actualidad como la tercera economía a nivel global.

PALABRAS CLAVES: Ciberseguridad. Patrimonio digital. Pymes. Empresas Familiares. Sistemas de Gestión de Seguridad de la Información (SGSI). Concientización. Protección de Datos Personales. Exfiltración de datos. Ciberataque. Amenazas. Vulnerabilidades. Confidencialidad. Integridad. Disponibilidad de la Información. Educación Digital. Tecnologías de la Información y la Comunicación (TIC).

ABSTRACT: The objective of this work is to raise awareness within family businesses about the vulnerabilities, threats, and exploits observed in the electronic communications ecosystem, particularly in the digital heritage that both SMEs and family businesses have been building since the emergence of Information and Communication Technologies (ICT). Just as in the

[1] Artículo recibido el 19 de septiembre de 2024 y aprobado para su publicación el 30 de septiembre de 2024. El presente es una adaptación del trabajo presentado ante el Instituto Argentino de Empresa Familiar (IADEF) en el marco del análisis de la convocatoria "Poder y Dinero en la Empresa Familiar", que resulta presentada en el mes de mayo de 2024 en el seno del citado Instituto.

[(*)] Abogada, Escribana Titular del Registro 803 CABA. Especialización en Derecho Informático (UBA). Diplomada en Blockchain y Smart Contracts (UCC); Fintech y Blockchain (ITBA); Gestión de la Ciberseguridad (UCEMA); Dataprivacy e Infosec (DATALAB UBA). IA y Derecho y Web 3, Gaming y Metaverso (UBA IALAB). Maestranda Escuela de Economía y Negocios (UNSAM) en la Maestría Gestión y Diseño de la Tecnología y la Innovación. Consultora de Empresa Familiar Certificada (IADEF). Profesora Adjunta Seminario de Nuevas Tecnologías y Notariado en Postítulo Notariado (USAL). Prof. Adjunta Catedra Teoría y Práctica del Derecho Registral. (USAL). Docente Auxiliar CPO (UBA DERECHO).

analog world, SMEs and family businesses have carefully guarded industrial secrets, product formulation recipes, and process management models, in the digital universe, it is necessary to strengthen behaviors related to Information Security Management Systems (ISMS), learning to develop Security Policies, raising awareness among executives, employees, suppliers, and consumer clients, and strengthening technical aspects with specific cybersecurity tools. Reputational damage due to the exfiltration of their databases—with the consequent loss of information and personal data of clients and consumers—will be another new topic to address in the coming times, especially given the current reality in which cybercrime is currently the third-largest economy globally.

KEY WORDS: Cybersecurity. Digital heritage. SMEs. Family businesses. Information Security Management Systems (ISMS). Awareness. Personal Data Protection. Data exfiltration. Cyberattack. Threats. Vulnerabilities. Confidentiality. Integrity. Information Availability. Digital Education. Information and Communication Technologies (ICT).

DOI http://dx.doi.org/10.22529/rbia.2024(5)04

I. INTRODUCCIÓN

Sabemos que las tecnologías atraviesan de manera disruptiva todos los ámbitos de trabajo en las organizaciones y la empresa familiar no resulta ajena a ello.

Muchas empresas, incluso las familiares, se ven desbordadas por el fenómeno tecnológico que está imponiendo un cambio cultural y paradigmático en sus economías, procesos productivos y comercialización.

El uso cotidiano de herramientas digitales nos advierte la existencia de importantes contingencias, algunas de ellas vinculadas al uso descuidado e irresponsable de las tecnologías que pueden dar lugar a severas falencias en el resguardo de la información de una organización, como así también respecto de la privacidad de los datos personales tanto de los clientes, proveedores como de los mismos miembros de la empresa familiar.

Estos y otros temas generan una constante tensión que no puede pasar inadvertida para los profesionales que asisten a la empresa familiar, quienes deben encontrarse capacitados para resolver conflictos frente a los cambios tecnológicos que siempre llevan la delantera respecto de las normas que regulan la materia.

La aparición de tecnologías disruptivas dentro de lo que llamamos Web 2 -y el surgimiento de la Web 3- vienen a abstraer del mundo físico el patrimonio de las personas, organizaciones y empresas para migrarlo al ámbito del e-commerce, los pagos en línea, el uso de billeteras digitales, los algoritmos y sistemas de comercialización que corren bajo la tecnología blockchain o cadenas de bloques. A esto debemos agregar la aparición de un sinfín de herramientas diseñadas con Inteligencia Artificial Generativa, la implementación de espacios inmersivos, la realidad aumentada y la realidad virtual como protometaversos y metaversos que ya se están aplicando en diversas áreas como es el caso de las tiendas on line. [3]

Frente a este mundo en constante cambio necesitamos recurrir a la concientización, la educación e inclusión digital para articular una adecuada protección de este patrimonio digital de las empresas familiares como de sus demás activos digitales mediante la adopción de estas habilidades técnicas con una mirada humanística donde la tecnología sea una herramienta más al servicio de las personas y no se convierta en un factor de riesgo al que se lo conoce por sus

[3] https://xnova360.com/empresas-realidad-aumentada/

efectos, que en muchos casos pueden ser dañinos y hasta devastadores para las personas, empresas y organizaciones.

El cibercrimen y el ciberdelito constituyen la tercera economía mundial y según datos publicados del año 2023, han causado unos ocho billones de dólares de pérdida en el mundo. En la República Argentina los ciberdelitos en el mismo período han aumentado casi un cuarenta por ciento. Los incidentes reportados ascienden a dos mil doscientos eventos por mes y éstos son sólo los denunciados.4 Esto nos invita a reflexionar que los grupos criminales no detendrán sus actividades delictivas. Los Estados buscan reforzar sus sistemas y los de los ciudadanos con los llamados CSIRT (Equipos de Respuesta a Incidentes de Seguridad o su traducción del inglés: Computer Security Incident Response Team) cuyos objetivos principales son prevenir, detectar y responder a un incidente de seguridad.

No obstante, toda implementación de políticas públicas en la materia requiere del interés de los usuarios y de la toma de razón sobre la necesidad de implementar medidas de seguridad no sólo desde los aspectos técnicos, sino también desde las conductas de las personas y los procesos organizacionales. Es por ello por lo que entendimos pertinente introducir en esta obra un aspecto diferente, como la ciberseguridad, respecto del dinero y el poder, de manera que pueda ser entendido como toda potencialidad de perder el poder que ostentamos sobre nuestro dinero ante la falta de medidas preventivas, como la concientización y el generar interés dentro de la empresa familiar por las temáticas que hacen a la Seguridad Jurídica de la Información. Este capítulo busca aportar estrategias y soluciones como así también ilustrar el panorama normativo en la materia para fortalecer y empoderar a las empresas familiares. Quienes integramos el ecosistema de la Empresa Familiar necesitamos desarrollar "cultura de ciberseguridad". 5

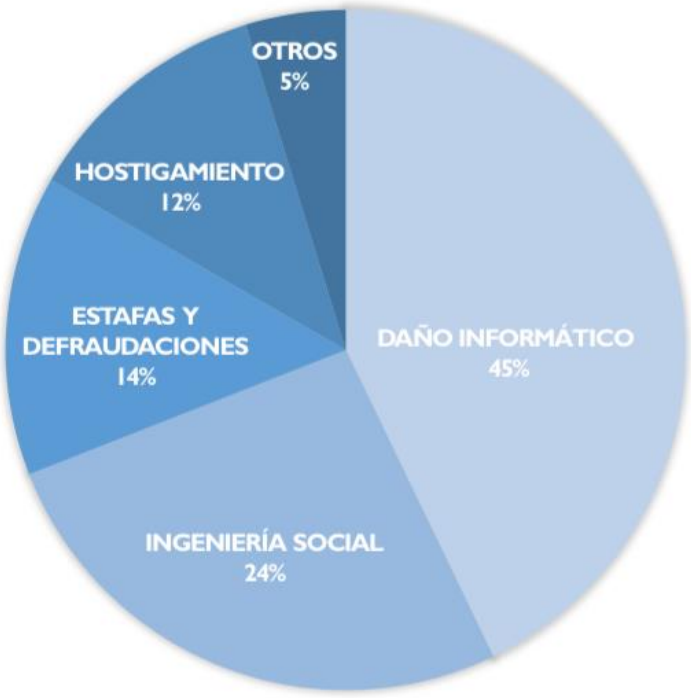
Nada más real que las estadísticas para entender que la seguridad de la información es una urgencia por atender por parte las empresas familiares, antes de que pasen a protagonizar los titulares de noticias donde se reportan los ciberataques, la pérdida de información y la

[4] https://www.lanacion.com.ar/editoriales/cibercrimen-la-tercera-economia-nid28012024/#:~:text=Se%20estima%20que%20en%202023,y%20China

[5] https://www.lanacion.com.ar/estados-unidos/un-ciberataque-a-marcas-de-ropa-famosas-en-estados-unidos-pone-en-riesgo-la-entrega-de-los-regalos-nid18122023/

vulneración a la protección de datos personales, lo que claramente podría repercutir sobre la reputación y el buen nombre de la empresa frente a los consumidores.

A continuación, compartimos algunas de estas estadísticas para ofrecer de manera gráfica la incidencia de la falta de seguridad de la información:



Fuente: BA-CSIRT. Jornadas de concientización. Fuerza Aérea Argentina

II. ¿A QUÉ LLAMAMOS SEGURIDAD DE LA INFORMACIÓN?

La información es uno de los activos más valiosos de las empresas. Con la incursión de las Tecnologías de la Información y la Comunicación gran parte de la información de las empresas familiares se encuentra en formato digital. Dependiendo de la cantidad de información que la empresa vincule con el ámbito digital podremos distinguir si tienen una dependencia baja, media o alta a los ámbitos digitales y de acuerdo con la exposición que hagan de sus datos en dicho ecosistema será la calidad de medidas que deberán tomar en consecuencia. Debemos tener en cuenta que los Activos de Información son aquellos bienes o recursos destinados a generar, procesar, almacenar o divulgar información. Forman parte de

estos sistemas la información de los empleados, clientes y proveedores, los registros de pedidos, informes, proyectos, nóminas o páginas web, la propiedad intelectual, los sistemas y aplicaciones, los procesos de negocios, las patentes industriales, y en el plano material las oficinas donde las empresas llevan a cabo sus tareas. Por ello resulta fundamental estructurar y jerarquizar la información de cada empresa para determinar cuál es el valor que aquella le aporta y qué medidas deben llevarse a cabo para protegerla.

Ahora bien, definimos a la Seguridad de la Información como el conjunto de medidas destinadas a impedir la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios no autorizados al sistema.

Advertimos a través de esta definición estos tres elementos esenciales que configuran a la seguridad de la información:

Estos tres elementos también aparecen en la definición de seguridad de la información que nos aporta el estándar normativo ISO/IEC 27.001:2022 cuando dice: “La seguridad de la información es la preservación de su confidencialidad, integridad y disponibilidad”.

Hablamos de confidencialidad como la propiedad que posee la información de encontrarse accesible solo a entidades autorizadas, sólo a aquellas personas u organizaciones que puedan acreditar un interés legítimo para tener acceso y conocer el contenido de dicha información. A título de ejemplo las historias clínicas de los pacientes son confidenciales y sólo pueden ser accedidas por aquellos médicos o instituciones médicas a los que el paciente haya autorizado con su consentimiento.

Respecto de la Integridad hace a la propiedad que posee la información en cuanto a su precisión y completitud, de manera tal que la misma no pueda ser alterada y/o manipulada de forma alguna. En la práctica cuando se adulteran programas o documentos digitales, agregando, quitando o sustituyendo el contenido de estos se está vulnerando la integridad de la información.

Finalmente, la disponibilidad remite a la propiedad de que la información se encuentre en estado accesible y usable cada vez que sea requerido su uso. El ciberataque conocido como "Ransomware" efectivamente vulnera esta propiedad de la información ya que encripta todo su contenido y no permite que los usuarios puedan acceder a la misma, todo ello además caracterizado con el pedido de pago de un rescate que normalmente se expresa en criptoactivos.

A su vez, la seguridad de la información presenta las siguientes características:

- TRAZABILIDAD
- PROTECCION A LA DUPLICACIÓN
- NO REPUDIO
- LEGALIDAD

Los elementos que conforman el Sistema de Seguridad de la Información -SGSI- son las personas, los procesos y las tecnologías. Es por ello que abordamos tanto factores objetivos -como las herramientas tecnológicas de monitoreo y de ciber defensa o de seguridad ofensiva de los sistemas de información- así como otros de carácter más subjetivo como el entrenamiento en la concientización de los equipos de trabajo y las conductas de los miembros de la empresa, y finalmente los de carácter organizacional en donde se delimitan las políticas y procesos a ser implementados y cumplidos dentro de la organización, quien será la que defina y

estructure la misma, la jerarquice determinando su valor y, en consecuencia determine, las pautas y medios de protección más adecuados.

Los sistemas de Seguridad de la Información tienen un sinfín de aplicaciones en la vida cotidiana de la empresa. Elementos como smartphones, notebooks, memorias USB, discos rígidos, routers, servidores, software y aplicaciones comerciales o desarrolladas a medida, datos en aplicaciones empresariales, página web, bases de datos de clientes, controles de acceso, productos, informes, documentos, etc. conforman el universo de temáticas en los cuales ejerce injerencia el cuidado de la información y la preservación de su confidencialidad, integridad y disponibilidad.

Veamos a continuación la relación que existe entre la información, los riesgos, su impacto en la organización y cómo debemos analizar los conceptos de vulnerabilidad, amenaza e incidente.

Sabemos que el riesgo implica la probabilidad de que una amenaza se concrete, en combinación con el impacto que ello podría producir.

Representan riesgos para la información de la empresa familiar los siguientes presupuestos:

- Robo de información privilegiada o esencial
- Intrusiones al sistema - información sensible desprotegida
- Falta de resiliencia - back up - copias seguridad
- Ciberataques - Ingeniería Social – Catástrofes naturales
- Ataques de denegación de servicio.

A su vez estos riesgos pueden producir determinados impactos en la información de la empresa familiar:

- Pérdida de la información
- Exposición de datos personales /sensibles
- Pérdida de operatividad / productividad - Interrupción de actividades.
- Pérdidas económicas (datos bancarios /billeteras digitales)
- Incumplimiento normativo y/o contractual. Contingencias legales y pérdida de reputación.

Veamos ahora cómo se vinculan estos riesgos con los conceptos de Vulnerabilidad, Amenaza e Incidente.

Vulnerabilidad: es una debilidad o ausencia de los mecanismos de seguridad que puede poner en peligro la información. El empleado que no ha asistido a la capacitación y que luego acepta que en su computadora de la empresa otra persona introduzca un dispositivo USB. La no implementación de antivirus con licencia o la utilización de programas informáticos sin licencia -crackeados- constituyen también otros factores de vulnerabilidad de los sistemas de información.

Amenaza: Es un evento cuya ocurrencia podría impactar en forma negativa en una entidad. Aprovecha la existencia de una vulnerabilidad.

Incidente: Cuando una amenaza ha conseguido su objetivo, comprometiendo la seguridad de la información. Representa una debilidad o ausencia de los mecanismos de seguridad que puede poner en peligro a la información.

Estos conceptos representan los contenidos mínimos que deben ser internalizados por las empresas familiares y los profesionales que la circundan.

III. ¿QUÉ NOS HACE VULNERABLES? - MEDIDAS PROTECTORIAS Y CONTROLES.

Sistemas operativos sin licencia

Antivirus gratuitos

Factores Humanos

Falta de implementación de Permisos / Privilegios y Controles de Acceso.

No actualizar las aplicaciones.

Celulares y tablets sin adecuada protección.

Uso de redes gratuitas sin VPN

No poseer cortafuegos.

¿Cómo podemos robustecer la seguridad de la información en las empresas familiares?

Podemos sugerir las siguientes medidas protectorias y controles:

- Utilizar Antivirus para todos los dispositivos extendiendo el uso de estos tanto a celulares como a tablets o similares.

- Actualizar el sistema operativo y las aplicaciones de internet.

- Formar a los empleados. Aumentar el nivel de concientización en seguridad de la información.

- Prestar atención a mensajes de dudosa procedencia. Verificar las direcciones de mail de los remitentes.

- Utilizar contraseñas seguras que contengan caracteres alfanuméricos y signos de puntuación combinados. Evitar la repetición de contraseñas en las diferentes aplicaciones. También podrá utilizar un llavero de contraseñas que puede ser provisto por el mismo sistema operativo del teléfono o del programa de antivirus. Utilizar doble o triple factor de autenticación. Crear una cuenta de mail específico para la recuperación de contraseñas y solo abrirla en un dispositivo que sea seguro, nunca en nuestro celular, pues los ciberatacantes tienen como práctica pedir con nuestro usuario una nueva contraseña -como si el usuario la hubiera olvidado- con el fin de recuperarla en el correo electrónico disponible en el celular y así lograr iniciar sesión en nuestras aplicaciones.

- Realizar copias de seguridad de aquellos archivos sin los cuales no podría realizarse la actividad de la empresa.

- Descargar aplicaciones de confianza. Analizar previamente a su descarga la reputación y comentarios realizados al desarrollador por los usuarios. Verificar qué datos personales nos requieren y su pertinencia, al igual de con cuáles aplicaciones de nuestro celular requerirá actuar y si las mismas comprometen o no nuestra privacidad, nuestros datos biométricos o algún otro dato personal de carácter sensible.

- Velar por el buen uso de la información personal y de la organización.

- Conectarse a redes seguras. Evitar en lo posible el uso de redes públicas. Habilitar la implementación de una VPN (Virtual Private Network).

- Evitar contactos en redes sociales de origen dudoso. Bloquear comentarios. Verificar previamente la cuenta de la red social antes de comenzar cualquier interacción. Ser cautos con los servicios de venta on line que ofrecen en las redes sociales sus productos y servicios.

- Implementar controles de acceso a la información de carácter sensible. Estructurar previamente la información de la organización y jerarquizarla. Proteger bajo el esquema de "Joyas de la Corona" aquella información imprescindible para la operatividad de la empresa familiar.

- Utilizar herramientas técnicas de monitoreo de amenazas, trackeo de navegación e instaladores de cookies. Instalar un sistema de cortafuegos.

IV. AMENAZAS EXTERNAS E INTERNAS DE LA INFORMACIÓN.

Aquí podemos apuntar un listado de potenciales amenazas que pueden presentarse en la actividad cotidiana de la empresa familiar.

Software malicioso: Es un programa diseñado para tener acceso a sistemas informáticos específicos, robar información o interrumpir las operaciones de nuestra computadora.

Exploit: Secuencia de comandos que se aprovecha de una falla o de una vulnerabilidad del sistema provocando un comportamiento no deseado o imprevisto. Existen los denominados Zero Day Exploits que son aquellas fallas introducidas por primera vez en un sistema y que no ha podido ser advertida o prevista por el desarrollador que inutiliza o causa un daño importante en el uso del programa.

Phishing: Entra dentro de los mecanismos conocidos como "Ingeniería Social", en donde se intenta convencer al usuario para que confíe en el contenido de un mail o mensaje de texto o por mensajería instantánea recibido con la intención de obtener información -contraseñas o claves de acceso- pero que es libremente aportada por la víctima a raíz de la confusión en el que la coloca el ciberatacante. Normalmente requiere de una acción positiva de la víctima ya sea aportando verbalmente un código -WhatsApp- o haciendo clic en un enlace que la lleva a una página web similar a la web oficial que cree estar usando, home banking.

Denegación de servicios: Es el conjunto de métodos técnicos que se utilizan con el fin de inhabilitar un servidor y que a raíz de ello no se pueda acceder a la información del sitio. Afecta a la disponibilidad de la información. Cuando esta denegación de servicios se realiza entre varios equipos a la vez decimos que estamos en presencia de una denegación de servicios distribuido (DDoS). En este caso el ataque consiste en que varios equipos -computadoras-

envían solicitudes simultáneas a un mismo servidor para inhabilitarlo. Normalmente utilizan herramientas denominadas botnets.

Amenaza persistente avanzada: Son un conjunto de amenazas complejas ejecutadas a través de ataques técnicos coordinados y dirigidos específicamente a una determinada entidad u organización específica.

Ransomware. Es una especie dentro de los malware o código malicioso, mediante el cual se secuestra la información del dispositivo de la víctima, solicitándole simultáneamente un pedido de rescate, normalmente criptoactivos, para poder recuperar la información. En nuestro país la administración pública ha recibido varios de estos ataques pudiendo citarse a la Dirección Nacional de Migraciones y a la Comisión Nacional de Valores entre algunos de los organismos afectados.

Fuga de información: Se produce cuando la información almacenada en una red interna o en dispositivos es publicada en Internet por un atacante malintencionado para consulta libre de esa información por un tercero sin autorización alguna. En estos casos vemos vulnerado el principio de confidencialidad de la información. En algunas ocasiones esta es la práctica utilizada por hacktivistas quienes unidos por una causa ideológica proceden a llevar adelante este tipo de ataques. Cabe recordar las publicaciones efectuadas en la red por el grupo activista Anonymous para representar este tema.

Botnets: Los botnets son una serie de dispositivos informáticos que realizan tareas programadas en forma conjunta, algunas con fines lícitos y otras ilícitos, es decir, que son maliciosas. Las de fines lícitos se pueden utilizar por ejemplo para tareas de seguridad informática, como la realización de pentests, que son manejadas desde el comando y control por un especialista o profesional del sector. Las botnets usadas para fines ilícitos se arman sin el conocimiento de que varios dispositivos (computadoras, celulares, tablets, etc) son parte de estas. Entonces, una botnet es una red de dispositivos capaces de conectarse a Internet, que es controlada de manera remota y funciona de forma autónoma y automática. En las de uso malicioso, funcionan sin la autorización ni el conocimiento de las personas usuarias de esos dispositivos. Las botnets también son conocidas como redes de computadoras zombis que se utilizan para realizar tareas rutinarias, pesadas y automáticas que le son asignadas por quien las controla. En la actualidad, las botnets tienen entre sus blancos a dispositivos de Internet de las

Cosas (IoT). Un claro ejemplo es la botnet Mirai, que genera un interés cada vez mayor por parte de aquellos atacantes que apuntan a vulnerabilidades más antiguas en productos de IoT para el mercado consumidor dado que los ciberdelincuentes saben que los dispositivos de IoT están menos protegidos y buscan aprovechar esa vulnerabilidad. Además, existen otras botnets que siguen activas en la región como lo son los casos de Gh0st y Andrómeda, también conocidas como Gamaru y Wauchos. El funcionamiento de una botnet consiste en utilizar parte de la capacidad de procesamiento de los dispositivos que la componen para realizar diversas tareas que van desde el envío de correo masivo, la denegación de servicio (DDoS), minar Bitcoins o cualquier otra actividad que genere un beneficio para el "Bot herder".

Amenazas internas:

Además de las amenazas externas debemos prestar especial atención a las amenazas que pueden plantearse en el ámbito interno de una organización. Las personas que trabajan en una organización representan uno de los principales recursos que poseen las organizaciones. Sin embargo, la seguridad de la información puede verse comprometida en algunos casos como veremos a continuación.

Usuarios internos malintencionados:

Tienen el potencial de ocasionar daños considerables por su capacidad de acceso interno. Pueden ser empleados descontentos o despedidos, cuyas credenciales no se han eliminado, y si tenían permisos como administradores con privilegios, pueden provocar situaciones de riesgo más elevadas.

Usuarios internos engañados:

Pueden ser engañados por terceros (ciberdelincuentes) a través de técnicas de ingeniería social para proporcionarse de datos y/o contraseñas que no deberían compartir. Pueden caer bajo el ardid o el engaño de personas que se hacen pasar por personal del departamento de sistemas de la empresa y otorgar claves de acceso a programas de acceso remoto de la computadora del empleado desde donde acceden a la información de la empresa.

Usuarios internos descuidados.

Pueden simplemente tener un fallo no intencionado, como seleccionar una opción errónea y manipular o eliminar información esencial de forma equivocada.

V. LOS 10 MANDAMIENTOS PARA LA CIBERSEGURIDAD DE LA EMPRESA FAMILIAR.

1.- Formación y Concientización.

2.- Políticas de Seguridad y Normativas de uso.

3.- Convenios de Confidencialidad.

4.- Administración adecuada de roles y perfiles con privilegios.

5.- Gestión y permisos de exempleados.

6.- Establecer un sistema de clasificación de la información.

7.- Soluciones tecnológicas antimalware y antifraude.

8.- Actualización constante de los equipos y de las credenciales de acceso.

9.- No ejecutar programas o ficheros de origen dudoso.

10. No conectar a los dispositivos una memoria USB desconocidos.

Hasta aquí hemos visto que las personas, los procesos y las tecnologías son los elementos más importantes de los Sistemas de Seguridad de la Información (SGSI). En el plano de las personas hemos también entendido la importancia de los procesos de concientización del personal y la necesidad de atribuir roles y funciones para sectorizar el acceso a la información. Además, resulta imprescindible la necesidad de ejercer controles y supervisión de las conductas de las personas en los equipos de trabajo asegurando el entrenamiento efectivo con pruebas especialmente diseñadas para comprobar la internalización de las medidas de protección. Por último, el personal externo a la empresa deberá también contar con diferentes privilegios de acceso y restricciones diseñadas por defecto a los sistemas de información.

En el plano técnico resulta conveniente la incorporación, instalación, configuración y actualización de hardware y software licenciado pues las empresas trabajan constantemente en

la provisión de parches del sistema que protegen de las amenazas más recientes, circunstancia de la que se carece cuando el software no responde a una licencia oficial, sin perjuicio de las contingencias legales por el uso de software crackeado y las infracciones a la Ley 11.723 de Derecho de Autor y de Propiedad Intelectual. La implementación de herramientas criptográficas que permitan el cifrado de información que deba ser circulada ya sea en mails o en la intranet de las organizaciones aporta una barrera más a diversos ataques. Existen herramientas de cifrado gratuitas como VeraCrypt que consiste en un software de código abierto para cifrar archivos, carpetas, unidades USB extraíbles, discos duros completos, e incluso el disco duro donde se encuentra el propio sistema operativo instalado. ("Veracrypt: Cifra y oculta tus archivos gratis - Redes Zone") VeraCrypt es multiplataforma, actualmente es compatible con sistemas operativos Microsoft Windows, cualquier sistema basado en Linux, y también es compatible con macOS. Otra herramienta de cifrado es BitLocker. Esta es una herramienta de Microsoft para Windows completamente gratuita y no necesita de ningún tipo de licencia para ser utilizado. Posee buen nivel de seguridad. Si el disco o unidad USB son robados no podrán acceder a la información que contiene sin la contraseña de recuperación. Otra de sus principales ventajas a nivel de seguridad, es que es muy complicado de desencriptar y tampoco se puede acceder desde otros sistemas operativos como Linux, Mac o Ubuntu entre otros. Brinda protección total contra ataques fuera de línea. ("BitLocker: Tutorial completo para cifrar discos en Windows - Redes Zone")

En el plano organizacional veremos de redactar las políticas, normativa interna y procedimientos para resguardar la información de la empresa familiar. Resulta de interés la implementación de "códigos de conducta digital" en donde se redacten los derechos y obligaciones que ostentan los miembros de la organización permitiendo aportar un marco operativo en donde las reglas del trabajo son claras y facilitan el esquema de cumplimiento y/o sanciones dentro de la empresa. También resultará de suma importancia la elaboración de los planes de contingencia ante eventuales ataques por parte de ciberdelincuentes en donde se designarán las personas autorizadas a cargo del procedimiento de contingencias y respuestas a incidentes, como así también, los pasos de contención y mitigación de los eventuales ataques. Asimismo, luego de superadas las etapas del incidente se abordarán las tareas de aprendizaje y reorganización para afrontar eventuales nuevos ataques en función de la experiencia adquirida.

El dato de color lo aportan los datos personales que se pudieran haber encontrado comprometidos en el incidente de seguridad. Las tendencias en el marco del compliance indican la necesidad de reportar el incidente a los usuarios comprometidos con el fin de advertirles que sus datos personales han sido pasibles de un ciberataque. Estas conductas resultan esenciales si la empresa familiar se encuentra interactuando con clientes o proveedores que se encuentren bajo la jurisdicción de la Unión Europea, ya que en dicha demarcación se encuentra vigente el Reglamento General de Protección de Datos Personales, lo que hace obligatoria la denuncia de filtraciones de datos personales.

Para acompañar la interacción de estos elementos -personas, procesos y tecnologías- aparece en escena el marco regulatorio que nos permite encuadrar jurídicamente las acciones relativas a la seguridad de la información llevadas a cabo dentro del ámbito de la empresa familiar. En este ámbito será fundamental asegurar el cumplimiento tanto de la normativa interna -generada por las políticas organizacionales- como del cuadro normativo imperante en la legislación de la jurisdicción donde opere la empresa familiar y de la legislación aplicable de los contratos celebrados.

VI. MARCO NORMATIVO DE LA SEGURIDAD DE LA INFORMACIÓN.

Dentro del ámbito de la República Argentina la empresa familiar deberá tener en cuenta el cumplimiento respecto a la legislación vigente en materia de Protección de Datos Personales -Ley 25.326- y a las resoluciones emitidas por la Autoridad de Aplicación, la Agencia de Acceso a la Información Pública (AAIP)- en donde deberá prestar especial atención en materia de datos biométricos, datos genéticos y el tratamiento de datos automatizados por la intervención de herramientas que contengan Inteligencia Artificial. Siguiendo esta línea normativa la citada ley prescribe en su artículo 9°: … "El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado…".

Dentro del ámbito del Derecho Penal la Ley 26.388 del 4 de junio de 1988 de Delitos Informáticos modificó el texto del Código Penal Argentino receptando en su articulado diversas figuras como el acceso indebido, el daño informático, el daño informático agravado y la violación de la privacidad entre otros. En tal sentido dejó tipificadas las siguientes conductas:

• ACCESO INDEBIDO (Artículos 153 y 153 bis CP).

La norma sanciona las conductas típicas de abrir o acceder indebidamente a una comunicación electrónica, carta, pliego cerrado, despacho telegráfico, telefónico o de otra naturaleza que no le esté dirigido a esa persona.

Abrir o acceder indebidamente a una comunicación electrónica, carta, pliego cerrado, despacho telegráfico, telefónico de otra naturaleza que no le esté dirigido esa persona. ("Código Penal Nacional - Legislación Argentina 2021") Apoderamiento indebido de información o de otro papel privado, aunque no esté cerrado. Borrar / suprimir indebidamente o desviar el contenido de correspondencia comunicación electrónica que no le esté dirigida. Interceptar / captar comunicaciones electrónicas o telecomunicaciones provenientes de sistemas de carácter privado o de accesos restringidos. El artículo 153 bis agrega los casos en que el autor del delito a sabiendas accediere por cualquier medio sin la debida autorización o excediendo la que posea a un sistema o dato informático de acceso restringido.

• DAÑO INFORMÁTICO (Artículo 183 CP).

La tipificación general apunta a la acción de destruir, inutilizar, hacer desaparecer, dañar de cualquier modo. La tipificación específica del daño informático hace referencia a la alteración, destrucción, inutilización de datos, documentos, programas, o sistemas informáticos. Hace punible la venta, distribución, circulación o introducción de un sistema informático a cualquier programa destinado a causar daños. Actividad de Ransomware, introducción de "bugs" (gusanos) en programas informáticos.

• REVELACIÓN DE DATOS (Artículo 157 y 157 bis del CP)

El funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos. Acceso y violación de sistemas de confidencialidad y seguridad de datos o bancos de datos personales. Proporcionar o revelar a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. Inserción de datos en un archivo de datos personales.

• TRATADOS INTERNACIONALES. EL CONVENIO 108 y 108 +

En tanto el Derecho Internacional también ha sancionado normas atinentes a la protección de los datos personales resulta primordial destacar que en virtud de la aplicación del artículo 75 inciso 22 de la Constitución Nacional Argentina, los Tratados Internacionales de los que el Estado Argentino forme parte en virtud de la adhesión a dicha normativa internacional tiene como efecto la adjudicación de rango constitucional a estas normativas del Derecho Internacional. En tal sentido es necesario destacar que nuestro país ha ratificado la implementación en el territorio de la República Argentina del Convenio 108 que versa sobre el tratamiento automatizado de datos personales a través de herramientas de inteligencia artificial. La República Argentina en el año 2019 mediante la Ley 27.483 aprobó el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal suscripto en la ciudad de Estrasburgo, Francia, el 28 de enero de 1981, así como también el protocolo adicional al Convenio.

El Convenio 108 posteriormente fue modificado en el mes de mayo de 2018 resultando en su continuador, el Convenio 108 +, aguardando a que nuestro país hiciera nuevamente adhesión a esta modificación.

Finalmente, la República Argentina adhirió al Convenio 108 + a través de la Ley 27.699 sancionada con fecha 10 de noviembre de 2022. Si bien como ya dijimos nuestro país ya era un Estado - Parte de este convenio aún quedaba pendiente ratificar su modificación que respondía, según así surge del mismo convenio, a razones de "diversificación, intensificación, globalización del tratamiento de datos y el flujo de los datos personales".

En su articulado el Convenio 108 + establece que "El tratamiento de datos genéticos, datos personales relativos a delitos, procesos y condenas penales y medidas de seguridad relacionadas, datos biométricos que identifiquen de manera exclusiva a una persona, datos

personales para la información que se divulgue relativa a origen racial o étnico, opinión política, afiliación a gremios, creencias religiosas o de otra índole, salud o vida sexual, sólo se permitirá cuando la ley establezca salvaguardas adecuadas que complementen las previstas en el presente Convenio. Dichas salvaguardas brindarán protección contra los riesgos que el tratamiento de datos sensibles pueda generar para los intereses, derechos y libertades fundamentales del titular de los datos, especialmente el riesgo de discriminación.

• UNESCO. RECOMENDACIÓN SOBRE LA ÉTICA DE LA IA.

Por su parte dentro del seno de la UNESCO surgió una Recomendación sobre la Ética de la Inteligencia Artificial. Esta recomendación fue aprobada por la Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) con fecha 23 de noviembre de 2021 y con respecto a la temática que nos ocupa establece respecto a los datos sensibles lo siguiente:

"Ámbito de Actuación 3: Política de Datos. Acápite 74: Los Estados Miembros deberían establecer sus políticas de datos o marcos equivalentes, o reforzar las políticas y marcos existentes, para garantizar la seguridad total de los datos personales y los datos sensibles que, de ser divulgados, puedan causar daños, lesiones o dificultades excepcionales a las personas. Cabe citar como ejemplos los datos relativos a infracciones, procesos penales y condenas, así como a las medidas de seguridad conexas; los datos biométricos, genéticos y de salud; y los datos personales como los relativos a la raza, el color, la ascendencia, el género, la edad, el idioma, la religión, las opiniones políticas, el origen nacional, étnico o social, la condición económica o social de nacimiento, la discapacidad o cualquier otra característica".

Se hace especial mención de la consideración de cuestiones éticas y lo concerniente al impacto de la Inteligencia Artificial en el ámbito de los Derechos Humanos, en tal sentido establece que se presta especial atención a:

"…La identidad y la diversidad culturales, ya que las tecnologías de la IA pueden enriquecer las industrias culturales y creativas, pero también pueden dar lugar a una mayor concentración de la oferta de contenidos, los datos, los mercados y los ingresos de la cultura en manos de unos pocos actores, lo que puede tener consecuencias negativas para la diversidad y

el pluralismo de las lenguas, los medios de comunicación, las expresiones culturales, la participación y la igualdad…"

• NORMAS DE CALIDAD INTERNACIONAL.

Tal como ya mencionamos en materia de seguridad de la información encontramos las normas de la Familia ISO / IEC 27.000 comenzando por la ya citada 27.001:2022 de Certificación de la Seguridad de Información y la 27002:2022 de mejores prácticas y estándares en la Gestión de la Seguridad de la Información y la ISO/IEC 27005:2022 sobre Gestión de Riesgos de Seguridad de la Información que implica la evaluación de la probabilidad de que un riesgo particular se materialice y la medición del impacto que tendría en la organización si ese riesgo se realiza. También resulta de especial aplicación la norma ISO/IEC 27701:2019 e ISO/IEC 27018:2014 en materia de procesamiento de datos personales y la ISO/IEC 29100:2011 de referencia de Alto Nivel para la Protección de Datos Personales. Por su parte en materia de Gestión de Riesgos contamos con la normativa ISO /IEC 31000:2018 que delinea las directrices en la materia incluyendo el diseño, la implementación, valoración, mejora, proceso y evaluación de los riesgos, entre otros parámetros.

• MARCO NIST 2 (Cybersecurity Framework 2.0)

El Marco de Ciberseguridad (CSF) 2.0 del NIST proporciona orientación a la industria y a las agencias de gobierno y otras organizaciones para gestionar los riesgos de ciberseguridad. Ofrece una alta taxonomía de resultados de ciberseguridad de nivel que pueden ser utilizados por cualquier organización, independientemente de su tamaño, sector o madurez, para comprender, evaluar, priorizar y comunicar mejor sus esfuerzos de ciberseguridad. Provee de enlaces a recursos en línea que brindan orientación adicional sobre prácticas y controles que podrían utilizarse para lograr esos resultados.

• NORMATIVA ADMINISTRATIVA REPÚBLICA ARGENTINA

A continuación, se enumeran las normativas de carácter administrativo que rigen las temáticas de ciberseguridad en nuestro país.

Decisión Administrativa 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos.

Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras.

Disposición 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.

Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.

Disposición ONTI 3/2013. Aprobación de la Política Modelo de Seguridad de la Información.

Resolución 1523/2019. Definición de Infraestructuras Críticas.

Decreto 577/2017. Creación del Comité de Ciberseguridad.

Decreto 480/2019. Modificación del Decreto 577/2017.

Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.

Resolución 141/2019. Presidencia del Comité de Ciberseguridad.

VII. CIBERSEGURIDAD Y CIBERINCIDENTES REGISTRADOS CONTRA LA ADMINISTRACIÓN PÚBLICA.

- Dirección Nacional de Migraciones, ocasionado por el Ransomware Netwalker, que afectó al Sistema Integral de Captura Migratoria (SICaM) que opera en los pasos internacionales, dónde se exfiltraron 22 carpetas con diverso material. (27/08/2020).

- El presunto y dudoso hackeo a la base de datos completa del Renaper, donde a través de consultas de su propio sistema el atacante logró teóricamente hacer un dump (vuelco) de la base de datos íntegra, compuesta por los datos de 45 millones de argentinos. El atacante hizo una primera publicación mostrando los datos de 44 figuras públicas y prosiguió dando algunas otras muestras y entrevista al respecto, en la que se jactaba de sus acciones. (12/01/2021).

- El incidente que afectó a Gendarmería, Ejercito, Prefectura Naval, Armada, Fuerza Aérea, Ministerio de defensa, donde se exfiltraron 1.193.316 registros de la base de datos de la obra social de las Fuerzas Armadas (IOSFA), Gendarmería, Prefectura y el Ministerio de Defensa. (25/09/2021).

- La presunta y dudosa venta de datos del gobierno argentino, que fueron ofrecidos por u$s 200.000.- doscientos mil dólares por el Grupo Cibercriminal Everest Ransomware Team, quien tuviera antecedentes similares en Perú, Brasil y los EEUU. (23/11/2021)

- Los incidentes y data leaks de la Policía Federal Argentina conocido como el escándalo de «La Gorra Leaks» y «La Gorra Leaks 2.0», que se extendieron de 2017/2019, el que fue el mayor incidente sufrido por esta fuerza, en la que se llevaron 700 gigabytes de archivos de la Policía Federal y de la Policía de la Ciudad de Buenos Aires, al mismo tiempo que también se vulneró la cuenta de la red social Twitter de la Prefectura Naval Argentina.

- El ataque de Ransomware al Poder Ejecutivo de la Provincia de San Luis, dónde se vieron comprometidos 350 gigabytes de información en noviembre de 2019.

- El ataque al Ministerio de Salud de San Juan de agosto de 2020.

- El ataque de Ransomware a la Agencia Nacional de Seguridad Vial en noviembre de 2020, en el que se vieron comprometidos 50 gigabytes de información.

- El ataque a la página web de la empresa estatal de agua de la Provincia de Buenos Aires ABSA en el mes de enero de 2021.

- El ataque de Ransomware al sistema informático del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires en el mes de noviembre de 2021, por el que se vulneró información administrativa confidencial y por el que, mientras se extendió, ninguna fiscalía federal de la Argentina tenía internet ni podía entrar a ver sus causas.

- El ataque al Senado de la Nación en las primeras semanas de enero 2022, por el grupo Vice Society, en el que se exfiltraron datos como números de DNI, CUIL, números de trámite de documentos, fotocopias de DNI de frente y dorso, domicilios, firmas a mano alzada, licencias de conducir, entre otros datos sensibles.

- El ataque de Ransomware al sistema del Poder Judicial de Chaco a principios de enero de 2022 por el grupo Hive, por el que debieron declarar la suspensión de términos y audiencias y extender la feria judicial.

- El ataque al sistema de historias clínicas del Hospital Perrando, de Chaco en junio de 2022.

- El Data breach del Hospital Garrahan de Julio 2022, con compromiso de información y datos de pacientes y médicos, por 5.5 gigabytes de datos, que se vendían por u$s 1500.-, que contenían 12 M de registros.

- El Data breach de la Corte Suprema de Justicia de la Provincia de Buenos Aires en el mes de Julio de 2022 donde se comprometieron 15.000 registros de carácter sensible entre los que se encontraban nombres de usuarios, direcciones de correo electrónico, nombre completo, DNI (u otros documentos más antiguos como Libreta de Enrolamiento), claves, e incluso direcciones IP y navegador utilizado por el usuario.

- El Data breach del Hospital Municipal Lucero de Bahía Blanca en Julio 2022, con compromiso de acceso a historias clínicas, estudios y documentos de 346 474 pacientes.

- El ataque de Ransomware al Poder Judicial de Córdoba en el mes de agosto de 2022, por el que quedaron comprometidos sus servicios, debiendo establecer un sistema de emergencia y declarando inhábiles a los fines procesales y administrativos por cuatro días consecutivos.

- El ataque al Poder Judicial de Neuquén en el mes de agosto de 2022, dónde se vulneró información de más de 3000 funcionarios.

- El ataque al Poder Judicial de la Provincia de Santa Cruz en septiembre de 2022, en el que se exfiltraron presuntamente y pusieron a la venta los archivos y usuarios de cada sector del poder judicial, hasta el acceso a cada máquina remota de cada sector.

- El ataque a la Legislatura de la Ciudad Autónoma de Buenos Aires, que afectó la página oficial de la misma y sus sistemas en el mes de septiembre de 2022.

- El ataque al Ministerio de Economía en el mes de septiembre de 2022, donde presuntamente se exfiltraron y pusieron a la venta por el grupo Everest claves de accesos.

- El ataque a la base de datos de la Autoridad del Agua de la Provincia de Buenos Aires ADA, en el mes de septiembre de 2022, en el que se sufrió además una pérdida relevante de datos ya que no se efectuaba backup diario y el último con el que se contaba databa aproximadamente de 15 días antes de la ocurrencia del incidente.

- El ataque al Estado Mayor Conjunto de las Fuerzas Armadas en el mes de octubre de 2022, donde se detectó la presencia de malware y se informó que presuntamente no hubo exfiltración de información sensible de dicha institución.

- El ataque a la empresa estatal Aerolíneas Argentinas en el mes de octubre de 2022, dónde se exfiltró y puso a la venta presuntamente entre otras cosas información técnica, contraseñas, emails, casi 65 mil direcciones de correos de clientes de Aerolíneas, aunque la empresa sostuvo que no se filtró información confidencial de la misma.

- El ataque al Ministerio de Salud de octubre de 2022, donde se envió información falsa, mails en cadena y se exfiltraron presuntamente datos de carácter sensible, a raíz de lo cual el Ministerio salió a informar que se desestimaran por el momento todas las comunicaciones provenientes de sus correos electrónicos).

- La pérdida de millones de datos del Censo conocida en octubre de 2022.

- Incidente en la Legislatura de la Ciudad de Buenos Aires. Ransomware. 10/09/22.

Por su parte durante el transcurso del año 2023 se registraron, entre otros, los siguientes incidentes:

- Incidente en el Poder Judicial de San Juan. Filtración de datos en la Suprema Corte. Se filtraron 1983 registros vinculados al concurso interno de ascensos del año 2019. (2/1/23)

- Incidente en la Superintendencia de Seguro de la Nación. El ataque afectó a las aplicaciones Mi Argentina y Mi Seguro. No aparecía ningún certificado. Debieron suspender el uso del Sistema Único de Notificaciones (SUN). (4/4/23).

- Incidente en la Administración Nacional de Medicamentos, Alimentos y Tecnología Médica. Hackeo de los servidores del organismo. (ANMAT) 21/04/23

- Incidente en el Instituto Nacional de Tecnología Agropecuaria (INTA) con fecha 2/5/23. Quedaron varios días sin poder funcionar tres radares producto del hackeo que aportan información al Servicio Meteorológico Nacional.

- El incidente a la Comisión Nacional de Valores ocurrido a mediados del mes de junio de 2023 y que se le adjudicara al ransomware "Medusa" y la cantidad de 1,5 TB de datos e información sensible.

- Incidente en el Hospital Castro Rendón, el más grande de la Provincia de Neuquén. Exfiltraron las bases de datos del Hospital produciendo una fuga de más de 100.000 pacientes con sus datos sensibles causado por factores humanos a través de los cuales se comprometieron credenciales de acceso al sistema. (7/6/23).

- Incidente en el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (PAMI). El grupo ciberatacante Rhysida ostentó poseer un terabyte (1TB) de datos que incluyen presupuestos, gastos, documentos personales extraídos del Sistema de Gestión Administrativa del Sector Público Nacional. El precio del rescate solicitado por los ciberatacantes fue de veinticinco Bitcoins equivalentes en dicha fecha a la suma de U$S. 735.000. (2/8/23)

- Incidente en la Universidad de Buenos Aires. Se trató en este caso de un ransomware en sus sistemas que impidió a los docentes y alumnos gestionar notas, inscribirse a cursos de verano y proceder a la realización de pagos de títulos y otros trámites arancelados. (19/12/23)

En lo que va del año 2024 se registraron los siguientes incidentes:

- Fuga de información de Licencias de conducir. Se exfiltraron datos como firma de las personas, tipo de sangre, restricciones del conductor, direcciones, etc. Salieron a la venta 6 millones de licencias de conducir en la internet profunda. (16/04/24).

- Incidente de exfiltración de datos de RENAPER. Se accedió indebidamente a código fuente, API, contraseñas, fotos y huellas digitales. (17/4/24)

En estos aspectos se han trabajado políticas públicas al efecto. Tal es así que El Banco Interamericano de Desarrollo (BID) aprobó un préstamo para Argentina de US$30 millones para la implementación del Programa de Ciberseguridad para Infraestructuras Críticas de Información (ICI), iniciativa que mediante la detección temprana de incidentes en este terreno contribuiría a la reducción de los costos que generan los ciberataques en el país.

El programa aumentará la seguridad cibernética de Argentina reforzando la protección de la infraestructura tecnológica de sus instituciones públicas, lo que beneficiará tanto a los ciudadanos como al sector privado y a la administración pública.

Para ello fortalecerá las capacidades institucionales y tecnológicas de la Secretaría de Innovación Pública (SIP), consolidará el talento humano en ciberseguridad y mejorará la protección del ecosistema de Gestión Documental Electrónica (GDE).

Durante el año 2023 el Estado Argentino proyectó el Segundo plan estratégico sobre CIBERSEGURIDAD: El 6 de enero de 2023, por medio de la Resolución N° 1 del 2 de enero de 2023 de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS, se declaró la apertura del procedimiento de consulta pública respecto de la SEGUNDA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD incluida como Anexo IF-2022- 133944871- APN- SSTI#JGM. En la misma norma, se encomendó a la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, impulsar los actos administrativos y demás acciones necesarias para la implementación de la SEGUNDA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD. El documento puesto a consideración de la ciudadanía mediante el proceso de elaboración participativa de normas fue confeccionado por el Grupo de Trabajo del Comité de Ciberseguridad creado a tal fin. Este grupo estaba conformado por representantes de los Ministerios de Defensa; Seguridad; Relaciones Exteriores, Comercio Internacional y Culto y Justicia y Derechos Humanos y las Secretarías de Innovación Pública y Asuntos Estratégicos. Participaron también, en calidad de invitados, funcionarios de la Sindicatura General de la Nación, el Banco Central de la República Argentina, ARSAT, la Administración Federal de Ingresos Públicos, la Agencia de Acceso a la Información Pública, la Secretaría Legal y Técnica y la Agencia Federal de Información.

VIII. LA RESOLUCIÓN 87/2024 DE LA SECRETARÍA DE COMERCIO.

Esta resolución estableció que todos los comercios que operen con tarjetas de compra, crédito o débito deberán poner a disposición de los usuarios una terminal de pago inalámbrica a la vista del cliente. Esto implica que los clientes puedan mantener bajo su estricto control y en permanente contacto sus tarjetas de débito o crédito al momento de efectuar un pago, lo que redundará en reducir la posibilidad de maniobras de vulneración de datos y estafas, como tomar fotografías de números de tarjetas, código de seguridad de éstas y DNI del usuario, circunstancia que habilitaba a la sustitución de la identidad digital.

Ya en el mes de Julio de 2023 la Provincia de Río Negro sancionó en igual sentido la Ley 5648. Neuquén y Santa Fe también implementaron estas medidas en sus legislaciones exigiendo a los comercios proveer a los usuarios de medidas de seguridad al momento de realizar los pagos de productos y/o servicios.

Para permitir una correcta adecuación la Secretaría de Comercio previó que los comercios tengan a partir de la sanción de la norma el plazo de 180 días para implementar la normativa y, en caso de incumplimiento, podrán ser sancionados de acuerdo con las penas que prevé la Ley de Defensa del Consumidor. De acuerdo con estadísticas de la Secretaría de Comercio, en 2023 hubo casi 7 mil denuncias ante la Dirección Nacional de Defensa del Consumidor por fraudes y estafas en servicios financieros. Según fuentes del sector de Tarjetas de Crédito, en los mercados en los cuales el comerciante no manipula las tarjetas, y por lo tanto no tiene acceso a la información que estas contienen, el fraude es cuatro veces menor que en el resto de los mercados. Esta medida mejora la experiencia de pago del usuario, dándole celeridad para pagar y, por sobre todas las cosas, mejora la seguridad ya que el usuario nunca pierde control sobre sus tarjetas.

Al mismo tiempo, la Secretaría de Comercio ha informado que realizará una campaña de educación en consumo para concientizar a los ciudadanos sobre la importancia de pedir el POS a la hora de pagar. Promover la transparencia de las transacciones es un objetivo compartido por asociaciones de consumidores, autoridades provinciales y especialistas en la materia.

IX. EL FUTURO DE LAS EMPRESAS FAMILIARES Y LA SEGURIDAD DE LA INFORMACIÓN.

Las Empresas Familiares para poder crecer y ofrecer sus productos y servicios a nuevos mercados deberán ajustarse paulatinamente a las normativas y estándares internacionales en materia de gestión de sistemas de seguridad de la información. No sólo para conquistar nuevos mercados sino también para poder interactuar con otras empresas de mayor envergadura que la propia, las que tienen como parámetro que sus clientes y/o proveedores lleven delineadas políticas claras en materia de seguridad de la información. Esto se debe a que podría resultar riesgoso contratar con una empresa que no disponga de medidas diligentes en la seguridad de

la información, pues los datos de la empresa y de las transacciones efectuadas entre ellas podrían quedar comprometidos por un ciberataque que producirá mayor daño a la empresa que no se encuentre preparada para defenderse del mismo y en consecuencia queden comprometidos datos de empleados, clientes o proveedores de ambas empresas.

La capacitación para fortalecer el eslabón más débil que son las personas definirá la diferencia entre una empresa familiar robusta en materia de cumplimento de protección de datos personales y gestión del riesgo en materia de seguridad de la información de aquellas que no apliquen recursos a fortalecerse en la materia.

Siguiendo las experiencias europeas con el Reglamento General de Protección de Datos (RGPD), la Ley de Mercados Digitales y la Ley de Servicios Digitales, se puede vislumbrar que la exfiltración de datos personales será en un futuro no muy lejano el nuevo derecho de daños en la práctica profesional. Es por ello por lo que las Empresas Familiares deberán ir adecuando paulatinamente sus procesos para evitar futuras contingencias legales, lo que además redundará en beneficios a la hora de efectuar contrataciones con empresas internacionales o en el caso en que la misma empresa familiar inicie su proceso de internacionalización desplegando sus actividades en nuevas jurisdicciones.

REFERENCIAS BIBLIOGRÁFICAS.

Instituto Nacional de Ciberseguridad de España (INCIBE). (n.d.). Guía de Ciberataques. https://www.incibe.es/ciudadania/formacion/guias/guia-de-ciberataques (Recuperado el 20 de abril de 2024).

Burgueño, M. R. (Dir.). (2023). Ciberseguridad. Nociones básicas de Seguridad de la Información. En Innovación e Inclusión Digital (Capítulo VI). Editorial Di Lalla.

Faliero, J. C. (2023). Infosecurity, Seguridad Informática, Ciberseguridad & Hacking. "To hack and not to jail". Editorial AdHoc.

Hernández Ramos, J. L., Karopoulos, G., Nai Fovino, I., Spigolon, R., Sportiello, L., Steri, G., Gorniak, S., Magnabosco, P., Atoui, R., & Crippa Martinez, C. (2024). Cyber Resilience Act Requirements Standards Mapping. Publicación de la Oficina de la Unión Europea. https://data.europa.eu/doi/10.2760/905934 (Recuperado el 29 de abril de 2024).

Instituto Nacional de Ciberseguridad de España (INCIBE). (n.d.). Cumpliendo con la NIS2: recursos y servicios para la pyme. https://www.incibe.es/empresas/blog/cumpliendo-con-la-nis2-recursos-y-servicios-para-la-pyme (Recuperado el 17 de abril de 2024).

Escudo Digital. (2024, marzo 23). ¿Qué pueden hacer las pymes para reducir las ciberamenazas? https://www.escudodigital.com/ciberseguridad/que-pueden-hacer-pymes-reducir-ciberamenazas_57906_102.html (Recuperado el 23 de marzo de 2024).