Universidad de SanAndrés

Escuela de Administración y Negocios

Trabajo de Graduación de Contador Público y Licenciatura en Administración de Empresas

Ciberseguridad en PyMEs de la industria de *retail* farmacéutico: estudio de los casos Zona Vital y FarmaBelén

Autor: Agustín Spinelli Riso

Legajo: 25.202

Mentor: Gabriel Aramouni

Victoria, Agosto de 2018

Agradecimientos

En primer lugar, agradecer a Dios su eterna compañía, sin la cual nada de esto sería posible.

Luego, quiero expresar mis más profundos agradecimientos, a ellos que me guiaron desde pequeño. A mi papá, José Luis, mi mamá, Virginia, a mis hermanos, Ramiro, Juan y Nicolás y, muy especialmente a mi abuelo, el 'Nono' y mi abuela, la 'Abu '.

Seguidamente, agradecer a mi fiel compañera Sofía. A mis amigos de toda la vida y a los que se sumaron en esta experiencia universitaria.

Gracias a mi mentor, Gabriel Aramouni, por su compromiso, tiempo y conocimientos. Y gracias a todos los profesores con los que tuve la suerte de compartir una materia, un aula, un rato… especialmente, agradecerle a Matías Wersocky por sus consejos y ayuda constante.

Resumen Ejecutivo

Las PyMEs representan un eslabón fundamental en el plano socio-económico de Argentina. Son la principal fuente de creación de empleo y ocupan un rol esencial en el crecimiento del producto nacional. Sin embargo, los distintos obstáculos (de índole financiero, legal y social) que se presentan como un freno para su desarrollo las coloca en una situación de alta vulnerabilidad. En este contexto, Drucker (1999) plantea que, dado el continuo avance de la digitalización e innovación, la tecnología se ha vuelto un *commodity* y el enfoque se ha colocado sobre la información. En otras palabras, debido a que cada vez más personas y organizaciones tienen acceso a las nuevas tecnologías, el diferencial se encuentra en la información. En este escenario, la gestión eficiente de la ciberseguridad para la protección de este activo crítico adquiere una gran importancia dentro del ámbito organizacional, como un elemento clave para impulsar el crecimiento de las compañías.

La presente investigación tiene como principal objetivo analizar la relevancia que las PyMEs que desarrollan sus actividades dentro de la industria de *retail* farmacéutico, en particular Zona Vital y FarmaBelén, otorgan al tratamiento de la ciberseguridad en el ámbito corporativo. De este modo, el trabajo se encuentra estructurado en los siguientes cinco capítulos.

En el **primer capítulo** se presentan la problemática y justificación que motivan y fundamentan la realización del trabajo. Luego, se enuncian las preguntas y objetivos generales y específicos en base a los cuales se desarrolla el estudio. Posteriormente, se abordan los conceptos teóricos y referencias claves para la delineación de los ejes de análisis. Por último, se configuran los aspectos relacionados a las decisiones metodológicas de la investigación, en donde se enuncian dichos ejes.

El **segundo capítulo** se divide en dos secciones. Con el objetivo de enmarcar la problemática planteada en el contexto local, se lleva a cabo una descripción de la situación general de la ciberseguridad en Argentina, tanto en el sector público, como en el privado. Luego, se efectúa el análisis de la seguridad informática en el ámbito de las PyMEs de *retail*, en donde se profundizan las

distintas medidas que se recomiendan implementar en dichas compañías para el tratamiento eficiente de la ciberseguridad.

En el **tercer capítulo** se implementa la técnica de *benchmarking* para describir la forma en que la ciberseguridad se circunscribe en Estados Unidos y Chile. Allí, se hace referencia a los principales aspectos que caracterizan el contexto de la seguridad informática en dichos países.

En el **cuarto capítulo** se lleva a cabo el análisis de la ciberseguridad en Zona Vital y FarmaBelén respectivamente. En ambos casos, en primera instancia, se describe a las compañías en términos generales y, luego, son analizadas a la luz de los ejes oportunamente establecidos. Finalmente, se incluyen algunas conclusiones y reflexiones del capítulo, y se realiza una comparación entre los casos de estudio abordados.

Por último, en el **quinto capítulo**, se presentan las conclusiones generales del trabajo, se resalta el aporte profesional de la investigación y, finalmente, se exponen algunos lineamientos, alrededor de la temática tratada, que pueden ser abordados en futuros trabajos.

Palabras clave: ciberseguridad, seguridad informática, información digital, activos de información, ciberincidentes, incidentes informáticos, PyMEs, *retail*, farmacias.

Índice General

CAPÍTULO 1: INTRODUCCIÓN

1. Problemática y justificación del estudio

1.1 Planteamiento de la problemática

> "El único sistema verdaderamente protegido es aquél que está apagado, encerrado en un bloque de hormigón y sellado en una habitación forrada de plomo con guardias armados —y aun así tengo mis dudas—"[1], Eugene Howard Spafford. (Dewdney, 1989, p. 110)

El continuo desarrollo tecnológico genera nuevas oportunidades de crecimiento para las organizaciones, al mismo tiempo que plantea un escenario complejo y desafiante, al que deben responder de manera eficiente para mitigar la ocurrencia de situaciones no deseadas. En otras palabras, "la dinámica del permanente cambio observado en las tecnologías de información y las comunicaciones, han impulsado de múltiples formas y, al mismo tiempo, condicionado las grandes transformaciones de las organizaciones" (Ojeda-Pérez *et al.,* pp. 42-43). Estos cambios generan, simultáneamente, oportunidades y beneficios, amenazas y riesgos para las organizaciones que se desenvuelven en esta era digital, en donde las tecnologías informáticas (*hardware*, *software*, bases de datos, redes y telecomunicaciones) poseen un rol central para el desarrollo y crecimiento de aquellas. Debido a que cada nueva oportunidad de negocio, apalancada en el empleo de dichas tecnologías abre, también, una nueva puerta para la ocurrencia de ciberincidentes[2], la proactividad de las firmas para prevenir y responder oportunamente a este tipo de sucesos, resulta de gran importancia.

La gestión eficiente de los distintos riesgos y peligros que implican la utilización de recursos tecnológicos para el desarrollo de sus negocios debe tratarse de una actividad estratégica prioritaria para las organizaciones, evaluada con el mismo grado de importancia que sus esfuerzos destinados, por ejemplo, en la

[1] Frase textual: "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards -- and even then I have my doubts."

[2] Ciberincidentes: concepto que engloba los incidentes relacionados con la seguridad de las tecnologías informáticas (incluye los ataques informáticos). Ver *4.3 Ciberincidentes* para mayor detalle al respecto.

innovación continua para mantenerse competitivas en el mercado. En este contexto volátil, incierto, complejo y ambiguo (conocido en inglés como V.U.C.A —*Volatility, Uncertainty, Complexity & Ambiguity*—), en el cual el cambio permanente es lo único estable, los incidentes informáticos constituyen una gran amenaza para las empresas y, particularmente, para aquellas en las que la dependencia de sus modelos de negocio al empleo de herramientas informáticas, resulta incuestionable. Principalmente, este es el caso de las entidades de servicios financieros y compañías de seguros y, por ello, se tratan de las industrias más reguladas del mundo.

Según sostiene la firma de consultoría internacional Price Waterhouse Coopers (más conocida como PwC) en su informe anual, a medida que aumenta la dependencia de la sociedad y las organizaciones respecto de los datos y la interconectividad, el desarrollo de la capacidad de hacer frente a los incidentes cibernéticos se vuelve cada vez más importante (Encuesta Mundial sobre el Estado de la Seguridad de la Información, 2017). Más aún, al tomar conocimiento acerca de la constante evolución en la cantidad y sofisticación de estos sucesos. Sin embargo, tal como señala el reporte desarrollado por la *Information Systems Audit and Control Association* (en adelante, ISACA[3]), a pesar de que el presupuesto que las empresas destinan al ámbito de la seguridad informática aumenta anualmente, su ratio de crecimiento se reduce año a año (*State of Cyber Security,* 2017). En pocas palabras, el presupuesto en ciberseguridad se encuentra desfasado respecto del aumento de los ataques e incidentes cibernéticos a nivel global. A pesar de ello, el informe destaca que cada vez más organizaciones cuentan con un responsable en la administración de la seguridad informática en sus nóminas de empleados.

“El valor de la información en nuestra sociedad, y sobre todo en las empresas, es cada vez más importante para el desarrollo de negocio de cualquier organización” (Canedo Estrada, 2010, p. 82). En la actualidad, la información representa uno de los activos más importantes, si no el más importante, de cualquier tipo de entidad. Constituye un recurso central para la toma de decisiones y, la calidad de estas decisiones depende de la calidad de la

[3] ISACA: es una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

información, lo que contribuye a mejorar la competitividad de las empresas. La información provee innumerables oportunidades de nuevos negocios para las empresas, al mismo tiempo que representa una gran responsabilidad en su empleo, almacenamiento y protección. En resumidas palabras, implica asumir el compromiso de aprender a gestionar de manera eficiente los riesgos asociados al manejo de este recurso crítico. En este sentido, la información posee un valor económico explícito e implícito para las organizaciones. Por un lado, puede ser monetizada a través de su intercambio por bienes, servicios o dinero. Por otro lado, su utilización puede generar un aumento de las utilidades, una reducción de gastos y/o riesgos, al mismo tiempo que su gestión puede favorecer la imagen y el reconocimiento del negocio. En definitiva, la información es un pilar estratégico fundamental en las organizaciones y, por tal motivo, el resguardo de este activo resulta de principal relevancia para garantizar su calidad y generar confianza en el mercado.

El constante incremento de los ciberincidentes que avanza paralelamente al exponencial desarrollo tecnológico, puede ocasionar grandes pérdidas en las empresas, no solo del tipo económicas sino que también puede deteriorar su imagen y confiabilidad. Por un lado, en términos de impacto económico, según el expresidente de la INTERPOL (*International Criminal Police Organization*), los ciberincidentes generan pérdidas estimadas de 400 mil millones de dólares a nivel global por año, lo cual representa alrededor de un 0,5% del PBI global (Centro Criptológico Nacional, 2017). Esta cifra se compone del daño directo ocasionado (robo de información, destrucción de servidores, etc.), la interrupción de las operaciones y los costos derivados de la recuperación, notificación del hecho y el retorno a la actividad. Asimismo, un estudio realizado por PwC Argentina revela que las empresas de todo el mundo sufren, en promedio, cuatro incidentes de ciberseguridad al año (Encuesta Global de Seguridad de la Información, 2017). Por otro lado, el daño en la reputación de la compañía representa un costo inmensurable e irreparable en términos de la pérdida comercial en la que puede derivar. Un incidente de tales características es capaz de generar una brecha de confianza, difícil de revertir, entre los clientes y la organización y, entre los líderes empresariales y los inversores.

Con el fin de dimensionar la problemática abarcada en la presente investigación en el ámbito local, cabe destacar algunos datos estadísticos brindados por el Ministerio de Modernización de la Nación en torno a la ciberseguridad (El panorama de la ciberseguridad en números, 2017). En un lapso de dos años y medio se registró un aumento exponencial del 224% de incidentes cibernéticos (2.252 en 2015, 422.000 en 2016 y 947.598 tan solo al 31 de mayo de 2017). Durante ese período, el 29% de las empresas en Argentina sufrió un incidente informático al menos una vez. Asimismo, las pérdidas generadas por ciberincidentes ascendieron a 5.400 millones de dólares entre agosto de 2015 y agosto de 2016. En esta línea, el trabajo publicado por la Unión Internacional de Telecomunicaciones (UIT)[4] sobre el estado de la ciberseguridad en el mundo, ubica a la Argentina en el puesto 63 sobre 134 naciones analizadas (*Global Cybersecurity Index,* 2017). Asimismo, el estudio sostiene que Singapur es el país con el enfoque más completo y avanzado en la materia y que América Latina es la segunda peor región del mundo en seguridad informática.

Tal como sostiene un experto en ciberseguridad: “en vías de una rápida digitalización y un mundo conectado por redes hacia una explosión de datos motorizada por el creciente ritmo de transformación que posee la tecnología, la importancia de la ciberseguridad es incuestionable” (Ramachandran, 2018). Sin embargo, a pesar de los perjuicios económicos y de imagen, y los distintos problemas en los que puede derivar un incidente cibernético, la mayoría de las firmas “prefieren no denunciarlo y hacen lo imposible por ocultarlo” (Kantor, 2016). ¿Cuál es el motivo de ello? La principal razón es que las empresas no quieren revelar sus vulnerabilidades frente a la competencia y, aún menos, a los clientes, quienes han depositado su confianza en ellas. Las organizaciones suelen justificar su actitud de evitar dar a luz lo ocurrido, ante un ataque o incidente informático, para no generar temor en sus clientes y/o usuarios. No obstante, detrás de esta intención de “cuidarlos”, subyace el verdadero motivo económico (reducir daños por pérdida de clientes, sanciones financieras,

[4] UIT: organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

suspensión de operaciones, investigaciones, etc.) que lleva a resolver internamente, con la menor repercusión posible, los ciberincidentes.

En el caso de Argentina, la problemática señalada en el párrafo precedente se profundiza debido a que el sector privado no se encuentra obligado por ley a reportar las violaciones a la seguridad cibernética. Sin embargo, la falta de denuncia ante incidentes informáticos es una práctica que no se limita al territorio nacional (ni tampoco al ámbito de la ciberseguridad), sino que se trata de una (mala) costumbre de larga data a nivel internacional. De esta manera, lo que las empresas aún no logran observar —colocando sus intereses individuales por encima de todo— es que, a través de estas decisiones, están desaprovechando una gran oportunidad: construir una comunidad colaborativa y constructiva, en donde circule información confiable y valiosa para concientizar sobre los riesgos cibernéticos y direccionar los esfuerzos en la mejora de los mecanismos de ciberseguridad para prevenir futuros sucesos. Tal como remarca PwC en su reporte: "*Across organizations, sectors, countries, and regions, building the capability to withstand cyber shocks is a team effort, the effectiveness of which will be diminished without greater and more significant participation*"[5] (Encuesta Global de Seguridad de la Información, 2018). El cambio de la mentalidad en este aspecto representaría un signo de madurez en el campo de la ciberseguridad corporativa. En este sentido, cabe destacar que no toda la responsabilidad recae sobre las organizaciones, sino que la falta de denuncia ante brechas de ciberseguridad también se debe al desconocimiento que existe respecto de su funcionamiento: ¿a quién se tiene que reportar?, ¿por qué es importante denunciar?, ¿qué se debe informar? Todos estos interrogantes son producto de la falta de información generalizada que existe en materia de seguridad informática. Por ello, el compromiso y la responsabilidad para cambiar esta situación son tanto de las organizaciones, como de las instituciones gubernamentales, quienes deben trabajar en conjunto para generar información precisa al respecto y, darla a conocer mediante canales de comunicación efectivos. Porque

[5] "A través de organizaciones, sectores, países y regiones, desarrollar la capacidad para resistir los shocks cibernéticos es un esfuerzo de equipo, cuya efectividad se verá disminuida sin una participación mayor y más significativa." (traducción propia)

solamente comprendiendo los riesgos y dimensionando las posibles consecuencias, se logra tomar consciencia de la situación.

Ahora bien, es importante resaltar que ninguna organización es invulnerable a los ciberincidentes, pues la seguridad absoluta no existe bajo ninguna perspectiva de análisis. Los incidentes informáticos son una realidad que amenaza de manera constante al mundo de los negocios, sin hacer distinción del tamaño o tipo de organización, ni del lugar físico en el que se encuentre ubicada. Basta con mencionar algunos de los casos de mayor repercusión en los últimos años para observar la diversa gama de usuarios que pueden verse afectados (Perazo, 2017). En el ámbito internacional, Yahoo admitió el acceso de terceros a las cuentas de más de 32 millones de usuarios entre 2015 y 2017. Por su parte, Uber dio a conocer que ciberatacantes accedieron a datos de 57 millones de usuarios. En el plano local, el Ministerio de Seguridad de La Nación —paradójicamente— sufrió el robo y filtración en internet de documentos privados en mayo del 2017. Asimismo, a través de un aviso falso en Google mediante la modalida*d phishing*[6]*,* el pueblo de 25 de Mayo (Buenos Aires) padeció el robo de 3,5 millones de pesos. La municipalidad local y algunas pequeñas y medianas empresas fueron las principales afectadas.

Luego de haber desarrollado un primer acercamiento hacia las principales nociones y problemáticas en torno al valor de la información en la sociedad actual y, la imponente amenaza que representan los ciberincidentes en ella, este trabajo se focalizará en el análisis de la relevancia asignada al tratamiento de la ciberseguridad en el ámbito de las Pequeñas y Medianas Empresas (en adelante, “PyMEs”) argentinas del sector de *retail* farmacéutico[7], a través de un estudio comparado de dos casos representativos de dicha industria, por las razones que se enuncian en el siguiente apartado. El estudio de esta temática resulta de particular relevancia en el contexto actual de negocios digitalizados y la constante amenaza que acarrea la utilización de tecnologías informáticas en el desarrollo de las organizaciones.

[6] *Phishing*: es un tipo de fraude informático que busca adquirir credenciales de un usuario (robo de contraseñas, números de tarjetas de crédito, datos bancarios, etc.) mediante el engaño. Ver *Anexo 3: Ejemplo de Phishing* para mayor detalle.

[7] *Retail* farmacéutico*:* hace referencia a las farmacias como puntos de comercialización de los productos ofrecidos a los clientes finales (medicamentos, productos para la salud y otros afines), diferenciándose de la actividad desarrollada por la industria farmacéutica (elaboración de medicamentos).

1.2 Justificación del estudio

La protección de la información, como se ha mencionado, es un pilar fundamental dentro de las organizaciones y, más aún, en aquellas compañías donde el empleo de herramientas de tecnología informática resulta esencial para el desarrollo del negocio. La decisión de llevar a cabo el presente estudio se encuentra fundamentada por diversos aspectos que se presentan a continuación.

En primer lugar, se ha seleccionado como unidad de análisis a las PyMEs debido al papel preponderante que ocupan en el escenario nacional, en cuanto al desarrollo y crecimiento de la economía. En Argentina, las PyMEs poseen una significativa predominancia en el mercado, pues, según el Ministerio de Producción de la Nación, representan el 99,7% de las empresas de bandera nacional. Constituyen la espina dorsal del aparato productivo nacional, ya que generan el 70% del empleo privado formal y contribuyen al producto bruto interno en aproximadamente un 30%. En este sentido, el Estado tiene el deber de proteger estas organizaciones y promover su crecimiento, a través de distintas herramientas económico-financieras y políticas de apoyo, necesarias para construir compañías más competitivas, innovadoras y comprometidas con el desarrollo nacional. Por tal motivo, en 2016 se sancionó una ley (Ley Nº 27.264) que brinda una serie de beneficios exclusivos para las pequeñas y medianas empresas (alivio de la presión fiscal, mejora del acceso al financiamiento, incentivo a la inversión y simplificación administrativa) que buscan crear condiciones para que estas organizaciones logren desplegar toda su fuerza emprendedora. Ante la necesidad de la Argentina de ganar competitividad y lograr diferenciación para una inserción inteligente al mundo, es fundamental que las pequeñas y medianas empresas creen valor agregado en las actividades económicas, en donde el tratamiento de la ciberseguridad representa un aspecto fundamental. En este sentido, dentro del marco de la progresiva globalización que presenta cambios radicales y constantes, las PyMEs se encuentran frente al gran desafío de lograr posicionarse en un mercado cada vez más competitivo.

Con el objetivo de enfocar la presente investigación en el ámbito de las pequeñas y medianas empresas, se ha decidido abordarla a partir del análisis

de dos casos de estudio de la industria de *retail* farmacéutico. Dicha elección se asienta, principalmente, en dos pilares: por un lado, estas compañías forman parte de una industria muy importante para el país, en términos del aporte al producto bruto interno y el nivel de competitividad que la caracteriza. Además, las farmacias son el eslabón final de la industria farmacéutica, es decir, son la imagen visible y el nexo final entre las empresas productoras de medicamentos y los clientes. En este sentido, las farmacias manejan datos e información relevante y sensible de pacientes, tratamientos especiales, médicos, medicamentos, recetas electrónicas y relaciones con obras sociales, organismos públicos y laboratorios. Estos recursos críticos deben ser administrados con el cuidado que merecen, debido a que su robo, manipulación o alteración puede generar grandes problemas en las compañías. Por lo tanto, las farmacias representan un sector relevante para el análisis de la problemática planteada en materia de ciberseguridad. Por otro lado, en relación a la viabilidad de la investigación, el acceso a fuentes de información en dicho rubro impulsó su selección. Cabe destacar que, en la siguiente sección, se retoman y amplían los argumentos que permiten justificar la elección del *retail* farmacéutico como unidad de análisis.

En segundo término, la relevancia del estudio de la ciberseguridad en cuanto a la gestión de la información digital adquiere, cada vez, una mayor trascendencia debido al continuo crecimiento de la cantidad de datos e información clave administrada por las organizaciones para el desarrollo de sus negocios. El permanente avance de la tecnología, impulsado por el uso eficiente de la información disponible, le brinda a las empresas la posibilidad de acceder a nuevos oportunidades de mercado (tal como el comercio electrónico), al mismo tiempo que genera nuevos desafíos. Actualmente, el crecimiento de las compañías y su posicionamiento en el sector que participan, se encuentran estrechamente vinculados a la oportuna adopción de las tecnologías emergentes, lo cual deriva en que la mayoría de los procesos realizados cuenten con el soporte de sistemas y tecnologías informáticas. Ello, como toda acción, conlleva numerosos riesgos inherentes a la actividad desarrollada. En este sentido, las PyMEs que operan dentro de la industria del *retail* se encuentran en una posición de alta vulnerabilidad, ya que, además de

la información corporativa, la constante interacción con sus clientes genera que manejen datos e información confidencial brindada por ellos (domicilio, números de tarjeta de crédito, datos bancarios, patrones de compra, entre otros). Por lo tanto, la implementación de medidas de ciberseguridad en las PyMEs de *retail* resulta fundamental para transmitir confianza en los consumidores, quienes, en última instancia, determinan el éxito o fracaso de la organización. En otras palabras, las firmas que actúan dentro de este segmento del mercado necesitan generar un vínculo de cercanía y credibilidad con sus clientes, asegurando el modo en que su información es utilizada y protegida. En este sentido, un ciberincidente que atente sobre las bases de datos podría ocasionar una pérdida de confianza (difícil de recuperar) y debilitamiento institucional de la empresa, lo que llevaría a una inminente caída de su imagen y, en consecuencia, generaría grandes pérdidas económicas.

Por los motivos anteriormente mencionados, resulta relevante estudiar el tratamiento de la seguridad informática dentro de la estructura organizacional y, el modo en que las pequeñas y medianas empresas se preparan (si es que lo hacen) para evitar la ocurrencia de incidentes informáticos o, en su defecto, para reducir el impacto negativo de sus consecuencias. Además, cabe destacar que estos hechos se van desarrollando, ampliando y aumentando su grado de sofisticación a medida que la tecnología avanza; por lo cual, el análisis de las acciones de ciberseguridad llevadas a cabo por estas entidades adquiere, diariamente, una mayor trascendencia. De este modo, cabe preguntarnos: ¿existe concientización acerca de la relevancia de la implementación de medidas de seguridad informática en el ámbito PyME?, ¿se encuentran estas compañías capacitadas para afrontar este escenario de amenazas crecientes?

En tercer lugar, si bien los ciberincidentes afectan a todo tipo de organizaciones y empresas en el mundo, las PyMEs se encuentran en un escenario de mayor exposición y hostilidad frente a estos sucesos. Ello se debe a que cuentan con una capacidad de recursos más limitada (en relación a las grandes compañías) para realizar inversiones eficientes en materia de ciberseguridad y, generalmente, no reciben el apoyo estatal adecuado para posicionarse de una mejor manera frente a las amenazas en general, y mucho menos de las derivadas del ámbito informático. De esta manera, los ejecutivos de dichas

organizaciones se encuentran frente al desafío de hacer “menos con más”. Asimismo, la falta de conocimiento por parte de las firmas acerca de lo fundamental que resulta la implementación de medidas de ciberseguridad, radica en la ausencia de información sobre el estado de la (in)seguridad existente, derivado de una práctica que se ha vuelto habitual en este contexto: la no denuncia de incidentes informáticos, puesto que ello significaría revelar fallas y debilidades de la empresa, tanto a los competidores, como a los clientes, las cuales podrían dejarla al margen del negocio. Así, ocultando sus debilidades, las organizaciones pierden la posibilidad de generar una cultura de cooperación para tratar este tipo de hechos y poner el foco en la protección de su información, su principal activo. Este mecanismo, por ejemplo, posee resultados positivos en la industria bancaria, en donde el “Club de CISO´s” funciona como un espacio para compartir experiencias, mejores prácticas y opiniones acerca de la ciberseguridad en la banca comercial.

En línea con la desinformación generalizada que caracteriza al ámbito PyME, existe una marcada creencia de “falsa exención” o mito de la irrelevancia de este tipo de organizaciones frente a la ocurrencia de ciberincidentes y, particularmente, ciberataques. En otras palabras, los directivos no consideran que sus empresas sean objetivos de gran valor para los ciberatacantes. En este entorno parece razonable pensar que los atacantes cibernéticos no tienen motivación alguna para direccionar sus operaciones en el mundo de las PyMEs porque ¿quién quisiera obtener ganancias de una organización pequeña, cuando en el mundo existen grandes compañías de las cuales los ciberatacantes pueden obtener mayores beneficios? Sin embargo, “casi la mitad de todos los ciberataques se cometen contra pequeñas empresas”, ya que quienes llevan a cabo estos actos se aprovechan de la gran cantidad de brechas de seguridad informática y, del mínimo esfuerzo y habilidades requeridas para vulnerar las defensas (si es que existen) impuestas por las compañías (Varela, 2017). El exceso de confianza o desinterés provoca que estas organizaciones se encuentren aún más expuestas a padecer incidentes informáticos. Por lo tanto, podríamos sostener que la mayor amenaza que afrontan las empresas es pensar que “lo digital” no atraviesa sus estructuras y repercute en sus procesos y operaciones. El desafío que poseen los líderes de

las organizaciones en este sentido, consiste en desmitificar estas creencias, como así también inculcar el verdadero valor estratégico de la ciberseguridad.

Por último, el aporte que se pretende generar a partir de la presente investigación, motiva y justifica su desarrollo. Se busca brindar una herramienta de valor profesional, académico e institucional. En primer lugar, el trabajo procura aportar una mirada sistémica acerca del escenario actual de la ciberseguridad en las PyMEs argentinas de *retail* farmacéutico, la cual pueda resultar útil para que dichas empresas logren comprender la importancia de la implementación de medidas efectivas de seguridad informática para la protección de su información, la preservación de sus clientes y, en última instancia, la sustentabilidad del negocio. Buscaremos brindar un documento de utilidad para que los ejecutivos de PyMEs argentinas, principalmente del sector de *retail* farmacéutico —pero también aplicable a las industrias que se encuentran en similares condiciones de exposición frente a los ciberincidentes y para aquellas que lo consideren pertinente—, comprendan la relevancia del tratamiento de la ciberseguridad y logren poner en marcha planes de acción de acuerdo a las mejores prácticas del mercado. En segundo término, nos proponemos proveer un instrumento de utilidad para el ámbito académico, es decir, que pueda ser utilizado para la enseñanza y formación de profesionales en ciberseguridad en las instituciones educativas (secundarias, terciarias y universitarias) del país. En última instancia, se busca generar un aporte institucional que impacte en las estructuras socio-económicas, con el fin de destacar la relevancia del tratamiento de la ciberseguridad a nivel nacional.

En síntesis, la elección del enfoque mencionado para el desarrollo del trabajo se fundamenta en la relevancia, novedad y actualidad creciente de la temática seleccionada, en función de los procesos de transformación en la era digital. Además, al tratarse la ciberseguridad de una materia poco abordada y, en especial, al aplicarla al estudio de las PyMEs (particularmente, de la industria de *retail* farmacéutico) se podría generar una herramienta con un valor agregado para dichas organizaciones. Finalmente, el interés personal respecto del tema en cuestión y, por profundizar el conocimiento al respecto, motiva la elección de dicho abordaje.

1.2.1 Justificación del *retail* farmacéutico

Para el desarrollo de la presente investigación se han seleccionado empresas de *retail* del rubro farmacéutico argentino como unidad de análisis, debido a diversos motivos que serán desarrollados a continuación. Antes de comenzar, cabe aclarar que las compañías que se desempeñan en dicho segmento son las farmacias que comercializan los medicamentos (y otros productos) elaborados por laboratorios nacionales e internacionales.

Con el objetivo de enmarcar el contexto de las farmacias en el plano local, se mencionan algunos de los aspectos más relevantes de la industria en la que participa. Las compañías que desarrollan sus actividades dentro de este segmento de mercado ocupan un lugar central en la cadena de valor de la industria farmacéutica argentina; son una extensión del sistema de salud nacional. Las farmacias conforman uno de los eslabones del sector farmacéutico, el cual es considerado como una industria estratégica en Argentina por distintos factores, entre las cuales se destacan (Cámara Industrial de Laboratorios Farmacéuticos, 2017):

- Con una larga trayectoria en territorio nacional (más de 100 años) y pionera regional en la fabricación de medicamentos, es el tercer sector industrial más grande de Argentina.
- Es una industria de alto contenido tecnológico y conocimiento científico que genera una producción con alto valor agregado, la cual representa alrededor de un 5% del valor agregado industrial del país.
- Se trata de una industria competitiva (más de 180 jugadores de capital nacional superan la presencia y participación de laboratorios extranjeros) que garantiza el normal abastecimiento de medicamentos de calidad internacional a precios accesibles.

Dada la relevancia que posee la industria farmacéutica para el país y, el rol de intermediario que desarrollan las farmacias entre los laboratorios y los consumidores finales, la ciberseguridad debería considerarse un tema a tratar en las agendas de los empresarios —no solo de las farmacias, sino también de los laboratorios— y los organismos públicos competentes. Ello se debe a que, muchas veces, un incidente o un ataque informático perpetuado en el eslabón

más débil de la cadena (como es el caso de las farmacias PyME) es capaz de expandirse hacia los sistemas de sus socios estratégicos. Por lo tanto, la conformación conjunta de un tejido empresarial ciber-seguro entre las partes interesadas, adquiere un alto grado de importancia.

En lo referido específicamente al mercado de las farmacias, tal como lo remarca un reporte del sector, este ha experimentado un fuerte crecimiento en los últimos años (Eduardo Tchouhadjian & Asociados, 2018). No obstante, al igual que sucedió con la mayoría de las empresas de consumo masivo, el mercado en cuestión evidenció una caída del volumen de ventas en 2017: las unidades vendidas cayeron un 0,7% respecto del año anterior. Si bien no se trató de un descenso significativo, señala el informe, marca un quiebre de la tendencia creciente en el consumo de medicamentos desde el 2002 (con excepción del 2014). En este sentido, cabe destacar que, históricamente, la disminución de volúmenes de venta en el mercado farmacéutico ocurrió producto de una profunda crisis (2002), o de un período en el que la economía no creció (2014). En 2017, estos factores no explican la caída de las ventas de productos farmacéuticos. De esta manera, el reporte indica que los principales motivos fueron: a) nuevas restricciones impuestas sobre las recetas de afiliados PAMI[8] con cobertura al 100% y; b) el desfasaje entre los incrementos de precios de los medicamentos (22,1%) respecto de la evolución de la inflación general (24,6%). La brecha existente entre ambos aspectos representó una pérdida de rentabilidad en las farmacias y, consecuentemente, la necesidad de realizar una mayor inversión y optimización del capital de trabajo para mantener el nivel de stock (factor calve para las farmacias) y buscar recuperase. Asimismo, la insignificante evolución de venta de los productos de perfumería y dermocosmética, los altos plazos de cobro, las elevadas bonificaciones en obras sociales y privadas (crecimiento de productos con cobertura al 100%), y la presión impositiva, contribuyeron a disminuir el nivel de rentabilidad y efectivo.

A pesar de todo ello, el estudio remarca que las cámaras del sector farmacéutico proyectan para el 2018 un alza del segmento de un 1% en

[8] PAMI (Programa de Asistencia Médica Integral): obra social de jubilados y sus familiares a cargo, discapacitados, pensionados y veteranos de Malvinas que opera en Argentina.

unidades vendidas y, aproximadamente, un 20% en facturación. Estas perspectivas estarán muy ligadas a lo que ocurra en el marco económico en general y, a lo que suceda con la renegociación del Convenio PAMI (reducción del precio de lista de los medicamentos cubiertos por dicha entidad). De esta manera, el informe finaliza sosteniendo que se deberá asignar una gran importancia a las actividades de gestión y control continuo de gastos, recursos disponibles y todas aquellas variables que afecten la rentabilidad del negocio para retomar a los niveles de actividad deseados.

A partir de la situación en la que se encuentran inmersas las empresas farmacéuticas, descripta en los párrafos anteriores, es posible advertir algunos desafíos relacionados a la ciberseguridad. Por un lado, el crecimiento esperado del sector puede suponer una mayor cantidad de las transacciones llevadas a cabo, lo cual incrementa las posibilidades de ocurrencia de ciberincidentes que afecten los datos e información empleada en las operaciones comerciales (información de ventas, datos de clientes, negociaciones con proveedores, etc.). Esto evidencia la relevancia de la existencia de un ámbito de seguridad informática activo en estas organizaciones, capaz de mitigar los riesgos de la manera más eficiente posible. Por otro lado, desde el entorno farmacéutico, tal como revela el reporte mencionado anteriormente, aseguran que una de las principales medidas a tomar para retornar a los niveles de rentabilidad deseados, es la gestión profesional del negocio que permita desarrollar actitudes proactivas, crear valor agregado al servicio brindado y controlar para optimizar los gastos y recursos. Diseñar y analizar la información necesaria para la toma de decisiones estratégicas es el elemento clave de gestión en tiempos de negocios con rentabilidad compleja. En este sentido, la información del negocio ocupa un rol crítico para apalancar dichas actividades; por lo tanto, se refuerza la importancia de la temática abordada en la presente investigación.

Por último, la diversidad de agentes que participan en este rubro: farmacias, clientes, proveedores (laboratorios o droguerías), médicos, obras sociales y prepagas, PAMI, hacen que la investigación en este sector del mercado, en torno al ámbito de la ciberseguridad, adquiera una mayor relevancia. En otras palabras, la construcción de un espacio seguro desde las perspectivas

abordadas en el trabajo resulta trascendental dada la cantidad de transacciones y operaciones de todo tipo que tienen lugar en este negocio. En tal sentido, cabe mencionar que, como señala el *Executive Director* en Ciberseguridad de EY en Argentina (Nicolás Ramos)[9], el *retail* en el país, a diferencia de la industria bancaria por ejemplo, no cuenta con ninguna regulación que obligue a las compañías a implementar mecanismos de seguridad informática.

2. Preguntas de investigación

2.1 Pregunta general

- ¿Cuál es la relevancia que las PyMEs de la industria de *retail* farmacéutico, en particular Zona Vital y FarmaBelén, le otorgan a la ciberseguridad para la protección de sus activos de información frente a los ciberincidentes?

2.2 Preguntas específicas

- ¿Cuál es el conocimiento del significado e impacto de la ciberseguridad y los ciberincidentes en el ámbito corporativo?
- ¿Cómo es el diseño de la ciberseguridad en la estructura organizacional de las compañías?
- ¿Cuál es el nivel de desarrollo de las funciones de ciberseguridad en las firmas?
- ¿Cómo se encuentra instrumentada la protección de los activos de información en las empresas (políticas, mecanismos y soluciones de seguridad informática)?

3. Objetivos

3.1 Objetivo general

- Comprender la relevancia que las PyMEs de la industria de *retail* farmacéutico, en particular Zona Vital y FarmaBelén, le otorgan a la

[9] Entrevista personal. Ver *Anexo 1: Entrevistas* para mayor detalle.

ciberseguridad para la protección de sus activos de información frente a los ciberincidentes.

3.2 Objetivos específicos

- Estudiar el conocimiento del significado e impacto de la ciberseguridad y los ciberincidentes en el ámbito corporativo.
- Identificar cómo es el diseño de la ciberseguridad en la estructura organizacional de las compañías.
- Conocer el nivel de desarrollo de las funciones de ciberseguridad en las firmas.
- Caracterizar la instrumentación de la protección de los activos de información en las empresas, a través de políticas, mecanismos y soluciones de seguridad informática.

4. Marco de referencia

En esta sección se describen los principales conceptos que se emplean en el trabajo, en función de la problemática y los objetivos planteados en la presente investigación.

4.1 Pequeñas y Medianas Empresas en Argentina

Una pequeña y mediana empresa (PyME) es una entidad cuya dimensión y envergadura de negocio se encuentran delimitadas por los criterios que impone la legislación de cada país. Las variables para encuadrar a una empresa dentro de la categoría PyME pueden ser de carácter cuantitativo (según el nivel de facturación, el volumen de producción, la cantidad de personal) o cualitativo (según la propiedad del capital, la independencia de la administración de la empresa respecto de los propietarios, entre otros). De este modo, una PyME que supera o no cumple con los parámetros preestablecidos, califica como una gran empresa y se encontrará sujeta al cumplimiento de otras leyes y normas.

En Argentina, una PyME es toda unidad productiva que genera bienes o servicios en el país, cuya facturación anual es inferior a un monto determinado, según la actividad del negocio y el personal empleado. En este sentido, es importante aclarar que la legislación argentina incluye el concepto de micro

empresa; no obstante, a los fines de simplificar la nomenclatura, vamos a hacer referencia a las PyMEs como unidad inclusiva de todas las categorías mencionadas en la ley. La Resolución 154-2018 (publicada en mayo de 2018 por la Secretaría de Emprendedores y de la Pequeña y Mediana Empresa del Ministerio de Producción) dispone la clasificación de una empresa como PyME según las ventas totales anuales, el sector del mercado en el que opera la entidad y la cantidad de empleados, tal como se puede observar en el siguiente cuadro:

CATEGORÍA	ACTIVIDAD				
	Construcción	Servicios	Comercio	Industria y minería	Agropecuario
Micro	12	7	7	15	5
Pequeña	45	30	35	60	10
Mediana tramo 1	200	165	125	235	50
Mediana tramo 2	590	535	345	655	215

CATEGORÍA	ACTIVIDAD				
	Construcción	Servicios	Comercio	Industria y minería	Agropecuario
Micro	$ 5.900.000	$ 4.600.000	$ 15.800.000	$ 13.400.000	$ 3.800.000
Pequeña	$ 37.700.000	$ 27.600.000	$ 95.000.000	$ 81.400.000	$ 23.900.000
Mediana tramo 1	$ 301.900.000	$ 230.300.000	$ 798.200.000	$ 661.200.000	$ 182.400.000
Mediana tramo 2	$ 452.800.000	$ 328.900.000	$ 1.140.300.000	$ 966.300.000	$ 289.300.000

Fuente: Ministerio de Producción de la Nación, Secretaría de Emprendedores y PyMEs.

A través de dicha norma se elevan (respecto de la Resolución 103E-2017) los límites de facturación anual, contemplando las especificidades propias de los distintos sectores y su evolución, con el objetivo de impulsar el crecimiento y desarrollo de las pequeñas y medianas empresas en el país. Las ventas totales anuales surgen del promedio de los últimos tres ejercicios comerciales o años fiscales, excluyendo el Impuesto al Valor Agregado (IVA), los impuestos internos que pudieran corresponder y, deduciendo hasta un 75% de los montos por ventas correspondientes a exportaciones, con el fin de estimular las ventas al mercado externo. Además, no se consideran PyMEs aquellas empresas incluidas en el anexo 2 y las entidades de intermediación financiera, servicios de seguros y servicios inmobiliarios que superen los 100 millones de pesos en activos. Por último, cabe señalar que, para aquellas empresas que perciban ingresos provenientes de más de una actividad, se tomará la de mayores

ingresos para su clasificación y, si al menos una de ellas supera el límite establecido, dejará de ser clasificada como PyME.

4.2 Ciberseguridad

Antes de comenzar, cabe destacar que los términos “ciberseguridad”, “seguridad informática” y “seguridad cibernética” son utilizados como sinónimos en la presente investigación.

La ciberseguridad es abordada por la literatura especializada en el tema desde dos perspectivas diferentes, pero complementarias. Por un lado, el organismo ISACA define la ciberseguridad a partir de su función y objetivos dentro de un entorno organizacional. De esta manera, establece que la seguridad cibernética hace referencia a la “protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados” (Mendoza, 2015). Así, los activos de información o activos digitales constituyen todos aquellos datos e información en formato digital que tienen un valor añadido para una organización. En otras palabras, la seguridad informática tiene como objetivo la protección de la propiedad intelectual e información que gestionan y administran las organizaciones contra su robo y el uso indebido. Por el otro lado, la ciberseguridad es comprendida como un medio o herramienta para cumplir los propósitos mencionados anteriormente. En consecuencia, se define como “el conjunto orgánico y coordinado de acciones y recaudos específicos que posibilitan eliminar o atenuar los efectos adversos de las múltiples vulnerabilidades que atentan contra todos los elementos componentes de los sistemas informáticos” (Clase Sistemas de Información UdeSA, Módulo VI: Auditoría, seguridad y delito informático, 2017). En otras palabras, la seguridad informática es el conjunto de tecnologías, procesos y prácticas diseñadas e implementadas para proteger redes, computadoras, programas, datos e información de los incidentes y ataques informáticos que pueden generar daños.

En síntesis, la ciberseguridad es la capacidad que poseen las organizaciones para defender y anticipar amenazas y vulnerabilidades internas y externas, minimizando las consecuencias dentro del ecosistema en el que operan, a

través de la implementación de un conjunto de soluciones tecnológicas, procesos y prácticas. Su eficiente gestión constituye un valor agregado, ya que tiene como objetivo la protección de la información que es un recurso vital para el crecimiento y desarrollo de las organizaciones. Es un factor diferencial clave para generar sólidos vínculos de confianza tanto con los clientes y usuarios, como con los proveedores y socios estratégicos. En definitiva, la seguridad informática genera confianza y esta, al mismo tiempo, crea oportunidades de negocio.

Resulta pertinente aclarar que el concepto de ciberseguridad o seguridad informática se diferencia del de seguridad de la información, el cual es más amplio, ya que incluye el resguardo de toda la información, más allá del medio en el que se encuentre almacenada (incluye la información en papel, la que se presenta de manera oral, entre otras fuentes). En cambio, la ciberseguridad se focaliza en el resguardo de la información del tipo digital que se encuentra comprendida en las tecnologías informáticas (*software, hardware*, bases de datos y redes) que la procesan, transmiten y almacenan. En resumidas palabras, es importante destacar que la seguridad informática se encuentra comprendida dentro de la seguridad de la información que posee un mayor alcance. Asimismo, cabe aclarar que la investigación no abordará los temas relacionados a la seguridad física de la infraestructura tecnológica (computadoras, celulares, unidades de USB, servidores), sino a los activos digitales que se encuentran almacenados en ella.

4.2.1 Marcos de referencia en ciberseguridad

Un marco de referencia o *framework* en materia de ciberseguridad es un conjunto de procesos documentados que son utilizados para definir políticas, mecanismos y procedimientos en torno a la implementación y gestión de los controles de seguridad informática dentro del ámbito corporativo, con el objetivo de medir el riesgo de robo y/o pérdida de activos y reducir las vulnerabilidades. Estos estándares de ciberseguridad son conjuntos de ideas, definiciones, sistemas de evaluación y clasificación y procedimientos que responden a las mejores prácticas, los cuales se encuentran enfocados en la construcción de estrategias y planes de acción que pueden ser adaptados a los riesgos, situaciones y necesidades de cada organización. Asimismo, los

frameworks representan una herramienta para que las empresas puedan evaluar su situación actual en seguridad informática respecto de un estándar de buenas prácticas, para así poder plantear un estado objetivo en dicho ámbito, capaz de ser alcanzado a través de la implementación eficiente del marco de referencia seleccionado.

Existen distintos tipos de *frameworks*, los cuales adoptan enfoques similares, pero difieren en el alcance de sus objetivos. Por lo tanto, es tarea de la organización evaluar cuál se adapta mejor a las necesidades y condiciones de la empresa. Dada la gran variedad de marcos de referencia que presentan las mejores prácticas en cuanto a la aplicación de medidas de seguridad informática, a continuación, se desarrollan aquellos que se encuentran más alineados al contexto y a las necesidades del negocio de las PyMEs, debido a su claridad y sencillez tanto en la explicación como en la aplicación del modelo propuesto. En primer lugar, se desarrolla el *Cybersecurity Framework* elaborado por el *National Institute of Standards and Technology* (en adelante, NIST) de los Estados Unidos. Su brevedad y simpleza lo convierten en un buen marco a ser adoptado en las organizaciones sin experiencia previa en la evaluación de riesgos de ciberseguridad. Posteriormente, se presentan las principales consideraciones del apartado *Risk IT* del, reconocido internacionalmente, documento *Control Objectives for Information and related Technology* (en adelante, COBIT) elaborado por ISACA. En tercera instancia, se desarrollan los aspectos más relevantes que presenta la norma internacional ISO 27001, en cuanto a la conformación de ámbitos de ciberseguridad organizacional. Una de las mayores ventajas de ISO 27001 sobre los demás marcos, es que las empresas pueden certificarse por su cumplimiento, demostrando a sus clientes (actuales y potenciales), proveedores y demás socios del negocio que la protección de los activos informáticos es una prioridad. Finalmente, se presentan los lineamientos más importantes abordados por la ISO 27032 que, a diferencia de la ISO 27001, no es certificable. De todas maneras, representa un marco de referencia que reúne las mejores prácticas para la toma de decisiones en torno a la ciberseguridad.

Cybersecurity Framework

El *Cybersecurity Framework* (en adelante, CSF), como marco de referencia modelo para conformación de ámbitos de ciberseguridad organizacionales, provee las herramientas, no solo para responder a las amenazas y recuperarse de los incidentes informáticos, sino también para prevenirlos antes de que se materialicen. El CSF reúne lo mejor de los marcos más reconocidos en el plano mundial de la ciberseguridad (COBIT e ISO), las mejores prácticas y metodologías del mercado y la experiencia de profesionales que colaboraron en su elaboración. Este documento, desde su primera publicación en 2014, se ha convertido en un estándar para la delineación de programas de ciberseguridad en las organizaciones. De hecho, para el 2015, el 30% de las entidades estadounidenses se encontraban utilizando el CSF y, según una proyección realizada por Gartner, el 50% lo estará empleando en el 2020 (National Institute of Security and Technology, s.f.).

Los objetivos principales que plantea el CSF son:

- Identificar estándares de ciberseguridad y guías aplicables de forma trasversal a todo tipo de organización (sin distinción de tamaño, sector, exposición a riesgos cibernéticos y sofisticación del entorno de seguridad informática).
- Ayudar a las organizaciones en la identificación, gestión y reducción de riesgos de seguridad informática (tanto internos como externos), a través de distintos planes de acción, según el nivel de madurez en ciberseguridad que posea.

De esta manera, el trabajo propone cinco funciones fundamentales que toda organización debe llevar a cabo para el desarrollo de un ambiente de ciberseguridad: identificar, proteger, detectar, responder y recuperar. Dado el dinamismo que caracteriza al mundo cibernético, estas actividades han de actualizarse constantemente para cubrir las necesidades de ciberseguridad, en función de los cambios que sucedan en el entorno. En primer lugar, se deben identificar los sistemas utilizados, activos de información físicos y digitales, y todos aquellos recursos que le permiten a la organización alcanzar sus objetivos. Asimismo, es necesario evaluar si existen políticas y procedimientos

definidos en materia de seguridad informática para la protección de cada uno de ellos, según su nivel de importancia en el cumplimiento de dichos propósitos.

En segunda instancia, resulta esencial proteger los sistemas informáticos a través de la implementación de medidas (capacitaciones, limitación del acceso a los recursos digitales, actualización de los programas, entre otras) para atenuar el impacto de incidentes cibernéticos. Para ello, cada miembro dentro de la organización debe tener conocimiento de los riesgos asociados al mundo digital y comprender cuáles son sus responsabilidades al respecto. Los datos e información deben ser gestionados de manera consistente con los riesgos del negocio, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.

Luego, se deben detectar situaciones de vulnerabilidad en la infraestructura de ciberseguridad mediante el monitoreo continuo (mediante un antivirus, por ejemplo), para poder anticiparse a la ocurrencia de situaciones no deseadas. En este sentido, conocer el potencial impacto de incidentes informáticos es sustancial para resaltar la importancia de las medidas de seguridad informática en la entidad.

En cuarto lugar, las organizaciones deben responder frente a las amenazas a través de un conjunto de actividades establecidas para reaccionar de manera oportuna y mitigar las consecuencias negativas de su materialización. Además, se destaca la relevancia de compartir la información respecto del incidente informático, en vistas a la generación de una cultura de concientización colaborativa en términos de la ciberseguridad y poder mejorar las prácticas en función de las lecciones aprendidas.

Finalmente, una vez concluido el incidente, las entidades deben implementar procesos de recuperación y restauración de los sistemas y activos afectados, para así poder retornar a la situación normal de trabajo. En este caso, el mecanismo de copias de seguridad constituye una buena práctica a implementar.

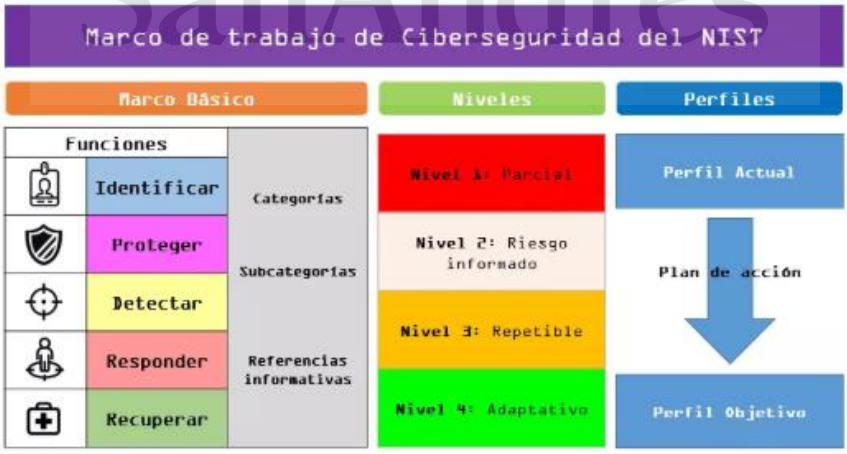
Después de definir las principales funciones a desarrollar dentro de las estructuras organizacionales en materia de seguridad cibernética, el CSF

delinea cuatro niveles de madurez informática para adecuar la implementación de las medidas propuestas al estado de la ciberseguridad correspondiente. El objetivo de esta categorización consiste en que las organizaciones puedan encuadrarse dentro de alguno de los niveles para identificar su posición frente a la ciberseguridad y evaluar las acciones a tomar con el fin de alcanzar el nivel de madurez deseado, teniendo en cuenta su viabilidad y alineación con los objetivos del negocio. Para llevar a cabo la clasificación se tienen en consideración diversos aspectos, tales como, las prácticas existentes de gestión de riesgos de ciberseguridad, el contexto amenazante en el que se desarrollan las actividades, los requerimientos legales y regulatorios y los objetivos y restricciones que posee cada entidad. Estos niveles describen de manera creciente el grado de rigor y sofisticación en las prácticas de gestión de los riesgos de seguridad cibernética.

1) Parcial: en este nivel inicial, las prácticas de gestión de riesgos de ciberseguridad no se encuentran formalizadas y las actividades para la conformación de un ámbito de seguridad informática no son una prioridad dentro de la agenda organizacional. En otras palabras, existe una baja consciencia de los riesgos asociados al uso de tecnologías informáticas y, por lo tanto, se caracterizan por tener una acción reactiva frente a los incidentes ocurridos.
2) Riesgos informados: las prácticas de gestión del riesgo en materia de ciberseguridad se encuentran alineadas a los objetivos del negocio. Se cuenta con procedimientos y procesos formales definidos e implementados y con personal capacitado.
3) Repetible: en esta categoría, se le brinda un alto grado de importancia a las medidas de seguridad informática, debido a que se comprende el impacto que puede generar en el negocio. Las prácticas de gestión del ciber-riesgo son formalizadas, a través de políticas que se actualizan regularmente como parte de la aplicación de análisis en cambios en requerimientos de negocio, amenazas o tecnologías.
4) Adaptativo: en este nivel, las organizaciones cuentan con una cultura de ciberseguridad fuertemente arraigada a los valores institucionales. Por ello, ninguna decisión se toma sin tener en cuenta los riesgos que implican en

cuanto a la seguridad informática. Las prácticas en este ámbito están basadas en lecciones aprendidas, a través de un proceso de mejora continua de adaptación a los cambios. Además, se le otorga gran importancia a la colaboración activa con terceros, compartiendo información de eventos de seguridad cibernética.

Posteriormente, a partir del análisis de las funciones necesarias para el desarrollo de un ámbito de ciberseguridad, los requerimientos del negocio, los recursos disponibles y el nivel de madurez en las organizaciones, el *framework* establece un perfil de la compañía. En él se describe el estado presente en seguridad informática y, otro en función del estado objetivo que se pretende alcanzar. El análisis de las diferencias entre ambos momentos permitirá identificar las brechas de seguridad informática que posee la organización y llevará al diseño de un plan de acción para reducirlas, en función de las necesidades del negocio. Cabe mencionar que, debido a la complejidad estructural que presentan las grandes corporaciones, una entidad puede asignar un perfil por cada sector. De esta manera, en el siguiente esquema se puede observar el armado de la arquitectura global al que arriba el CSF para la conformación de un entorno de seguridad cibernética, el cual debe ser monitoreado continuamente para evaluar su funcionamiento y perfeccionar las prácticas realizadas.



Fuente: Isec Auditors. Recuperado de: http://blog.isecauditors.com/2016/12/guia-rapida-para-entender-marco-trabajo-de-ciberseguridad-del-NIST.html

En conclusión, este documento aporta una herramienta de gran valor para la gestión de la ciberseguridad que puede ser aplicada en cualquier tipo de

organización. El CSF las ayuda a comprender los riesgos de ciberseguridad y provee un conjunto de medidas y prácticas para reducirlos a un nivel de tolerancia aceptable. El mencionado *framework* no busca reemplazar las prácticas y procesos existentes llevados a cabo por las compañías en dicha materia, sino que fue diseñado para mejorarlos, fortalecerlos e incluso servir como pilar para la creación de programas de gestión de los ciber-riesgos.

COBIT 5 y Risk IT Framework

El COBIT representa un trabajo de gran valor —reconocido y empleado a nivel internacional— para comprender la criticidad de la administración adecuada de los datos e información en un marco organizacional. La primera edición fue publicada en 1996 y COBIT 5, lanzada en 2012, es la versión más reciente del *framework*. Allí se hace principal énfasis en la importancia del alineamiento entre la estrategia de la organización y *IT*[10], puesto que ello promueve el crecimiento, incrementa el valor de la entidad y crea ventajas competitivas, al mismo tiempo que se fortalece la estructura organizacional contra los riesgos y amenazas emergentes. El documento promueve la alineación del gobierno corporativo con el gobierno de *IT*, integrados en una sola figura para gobernar la tecnología de la empresa, como una actividad crítica para eficientizar todos los procesos de negocio. Ello no quiere decir que se da mayor preponderancia a los aspectos tecnológicos, sino que la función de la tecnología e información debe ser tratada como cualquier otro activo clave para la organización. Las herramientas que brinda COBIT 5 pueden ser aplicadas para organizaciones de cualquier tamaño, industria, mercado, bien sea pública o privada, con o sin fines de lucro.

El principal aporte de COBIT 5, en función de los objetivos de la presente investigación, es la publicación *Risk IT*. Se trata de un *framework* para la gestión de riesgos relacionados con las tecnologías informáticas. Destaca la importancia del balance entre riesgo y valor, es decir, que los esfuerzos por reducir los riesgos informáticos no limiten las oportunidades de generación de valor de negocio para la empresa. Este trabajo hace énfasis en la integración de la evaluación del riesgo asociado con el uso, propiedad, ejecución,

[10] IT (*Information Technology* o Tecnología de la Información -TI-): se refiere a la utilización de *hardware, software,* redes y telecomunicaciones para almacenar, procesar y transmitir datos e información.

participación, influencia o adopción de tecnologías informáticas con las prácticas existentes de gestión del riesgo corporativo, debido a que en muchos casos es subestimado por los directivos y tratado como un aspecto estrictamente técnico. En otras palabras, la organización debe otorgarle al riesgo de *IT* la jerarquía que caracteriza al resto de los riesgos del negocio, tales como el riesgo de mercado, riesgo financiero, riesgo operacional, entre otros.

En definitiva el riesgo asociado al empleo de tecnologías informáticas existe, sea reconocido o no como tal por los miembros de una organización. Aquí adquieren importancia las herramientas brindadas por el *Risk IT Framework*, con el objetivo de lograr identificar y gestionar los potenciales problemas derivados del riesgo de *IT*, como un elemento más de la gestión integral de riesgos corporativos. Cabe destacar que el proceso de evaluación de riesgos de *IT* debe ser analizado constantemente, a través del establecimiento de ciertos indicadores o métricas adecuadas que permitan reconocer si los controles y mecanismos aplicados para mantener dicho riesgo a niveles aceptables, continúan siendo efectivos. Se trata de un trabajo continuo, y no de una actividad puntual y estática. De esta manera, la organización podrá conformar su propio perfil de riesgo y elaborar una estrategia acorde al nivel de tolerancia al riesgo determinado, a partir de un análisis de costo-beneficio. Dicha estrategia establecerá un plan de acción de medidas a llevar a cabo para alcanzar el nivel de ciberseguridad deseado (previniendo incidentes y ataques informáticos), al mismo tiempo que se aseguran las condiciones para promover el crecimiento organizacional. Para ello, este marco de referencia considera fundamental la creación de un plan de respuesta ante incidentes informáticos que permita a la empresa retornar a sus actividades diarias en el menor tiempo y al menor costo posible. Por último, se le asigna una gran importancia a la comunicación efectiva del estado presente de la ciberseguridad, los riesgos de *IT* y las acciones a llevar a cabo a todos los miembros de la organización, con el propósito de lograr alinear los comportamientos. En definitiva, el fin último de la implementación de este *framework* es la protección de, probablemente, el activo más valioso de toda organización: la información.

ISO

ISO/IEC 27001:2013

El estándar ISO 27001 —emitido por *International Organization for Standardization* fue publicado por primera vez en 2005— se rige sobre el principio de proteger la confidencialidad, integridad y disponibilidad de la información. Para ello define un sistema de gestión de seguridad informática, que, si bien tiene en cuenta la existencia de múltiples soportes en los que se encuentra la información, hace hincapié en los aspectos relacionados a la información que se sustenta en las tecnologías informáticas. Este sistema de gestión se basa en un enfoque de mejora continua, el cual se apoya en cuatro funciones: planificar, hacer, controlar y actuar (conocido como PDCA, por sus siglas en inglés —*Plan, Do, Check, Act*—).

1) Planificar: implica realizar un análisis de los riesgos de la seguridad informática, seleccionar los controles a aplicar y definir las autoridades y responsabilidades en torno a la seguridad informática, asignando una gran importancia al involucramiento de los altos directivos.
2) Hacer: implementación de los controles de ciberseguridad seleccionados.
3) Controlar: verificar la eficiencia de los controles puestos en marcha, a través de indicadores y métricas.
4) Actuar: adoptar acciones de mejora para mantener el nivel de seguridad cibernética deseado.

El objetivo del sistema es garantizar el conocimiento de los riesgos asociados a la utilización de tecnologías de la información para poder ser gestionados y minimizados por la organización, a través de un conjunto de controles (medidas y acciones) debidamente documentados.

De la misma manera que los *frameworks* desarrollados anteriormente, ISO 20701 puede ser utilizado como guía para la construcción o mejora de un ámbito de ciberseguridad en cualquier empresa u organización, independientemente de su tamaño o sector.

ISO/IEC 27032:2012

La norma ISO 27032 define un marco de gestión de riesgos de ciberseguridad que se complementa con el estándar ISO 27001 emitido por la misma

institución, y hace foco en el resguardo de los activos digitales. Los principales objetivos de una gestión eficiente de los riesgos de ciberseguridad se pueden resumir de la siguiente manera:

- Comprender el nivel de riesgos de ciberseguridad y seleccionar los controles adecuados a implementar.
- Involucrar y educar a la alta gerencia en cuestiones de ciberseguridad para que logren comprender la relevancia de su tratamiento.
- Realizar un plan de respuesta ante incidentes informáticos, el cual incluya compartir la información relevante del hecho en tiempo y forma a las autoridades que corresponda.

Para concluir, este apartado tuvo como finalidad exponer las principales características de los marcos de referencia en materia de ciberseguridad más reconocidos e implementados en todo el mundo. Como se pudo observar, cada uno de los *framework* tiene sus particularidades que lo diferencian de los demás, pero todos comparten el principal objetivo de generar un entorno organizacional en donde la ciberseguridad sea una prioridad, en vistas a resguardar un activo crítico para el funcionamiento de cualquier tipo de empresa u organización: la información. Por ello, los criterios, medidas, herramientas y procedimientos adoptados por cada marco de referencia no son excluyentes y, en muchos casos, de la integración de ellos se puede lograr un mejor resultado. En este sentido, el aspecto más importante es la consistencia en la utilización del documento seleccionado. El verdadero valor se encuentra en su aplicación efectiva en todos los niveles de la organización para la gestión de los riesgos orientados a las tecnólogas informáticas, en donde se relacionen las vulnerabilidades técnicas con el impacto en el negocio. Asimismo, la implementación de un *framework* para la creación u optimización de un entorno de ciberseguridad permite resaltar la importancia del tema y justificar las inversiones a realizar en dicho aspecto.

4.2.2 Marco regulatorio: *General Data Protection Regulation*

La regulación y legislación cada vez más estricta sobre el empleo de la información de terceros (datos de los empleados y consumidores, por ejemplo)

para fines comerciales impulsa una mayor concientización acerca de la importancia de la conformación de un ambiente corporativo ciber-seguro, eficientemente gobernado y administrado.

El *General Data Protection Regulation* (en adelante, GDPR), es un marco legal desarrollado por la Unión Europea, que comenzó a ser exigible a partir del 25 de mayo de 2018, tanto a las organizaciones, como a las grandes, medianas y pequeñas empresas. Se trata del cambio más importante en regulación de privacidad de datos en las últimas dos décadas. El principal objetivo de este marco legislativo es retornar el control de los datos personales a su propietario, de manera de limitar el uso que las organizaciones hacen de los datos, sin la autorización del titular. A diferencia de los *frameworks* desarrollados en la sección anterior, la aplicación de los lineamientos establecidos por el GDPR es de carácter obligatorio. No obstante, los marcos de referencia pueden ser empleados para alinearse a la regulación europea, ya que recomiendan una gran cantidad de controles, herramientas y procedimientos a llevar a cabo en el ámbito de la ciberseguridad.

Con el fin de acentuar la relevancia otorgada al tema en cuestión, la Unión Europea determinó que las organizaciones que no cumplan con los requisitos establecidos podrán recibir multas de hasta 20 millones de euros o hasta un 4% de los ingresos anuales del ejercicio financiero anterior, lo que resulte mayor. En este sentido, el cumplimiento de los puntos referidos en el GDPR deberá ser una prioridad en las agendas de las organizaciones, no solamente europeas, sino de cualquier organización que administre datos de residentes de la comunidad política del viejo continente. Una de las principales medidas que busca aportar claridad para la conformación de una cultura consciente de los riesgos asociados a la utilización de tecnologías informáticas, impone a las organizaciones reguladas la notificación de incidentes cibernéticos y robo o fuga de datos, tanto a los usuarios afectados como a las autoridades competentes dentro de las siguientes 72hs de ocurrido el incidente. En este reporte, la entidad que ha sido vulnerada deberá informar la procedencia del hecho, los datos afectados y las medidas que han sido adoptadas para resolver la brecha de ciberseguridad en cuestión. Es decir, la denuncia ya no se trata de una alternativa con la que cuentan las empresas para salvaguardar su

reputación e imagen ante un hecho de tales características, sino que deberán incorporar esta práctica a sus procedimientos de negocio.

La regulación indica que las organizaciones deben notificar a los usuarios de manera clara y explícita los datos que está procesando (previo consentimiento) y almacenando, cuál es su finalidad y con qué otras organizaciones pueden compartir esos datos. Asimismo, se añade el derecho del usuario a reclamar la eliminación de sus datos en cualquier momento. Con todo ello, cada vez adquiere mayor importancia que las empresas conozcan con exactitud la información y datos personales que administran de terceros. El análisis de estos recursos permitirá que las firmas se desprendan de datos que carecen de utilidad por ser redundantes, innecesarios u obsoletos. Por lo tanto, la inversión necesaria para alinearse a los requerimientos del GDPR, lejos de ser considerada un costo, se traducirá en ganancias en el corto-mediano plazo: al realizar la limpieza de los datos, se observará que menos datos, significan menores costos para protegerlos y menores riesgos asociados a la pérdida de información. En el caso de las pequeñas empresas —a diferencia de las grandes compañías que cuentan con altos volúmenes de datos almacenados hace tiempo— representa una gran oportunidad para comenzar a crecer, minimizando la cantidad de información confidencial que administran, de tal manera de reducir al máximo posible los riesgos asociados a ello.

Se trata de un gran desafío para todas aquellas organizaciones objeto de la regulación —y para las que aún no lo son, pero en vías de la globalización y crecimiento de los negocios podría ser alcanzadas por ella— y, más aún para las PyMEs. La ya mencionada escasez de recursos y el desconocimiento de los requerimientos tecnológicos para adaptarse, representan los mayores retos para este tipo de organizaciones. No obstante, a pesar del carácter compulsivo del Reglamento General de Protección de Datos (por su traducción al español), representa una oportunidad para que las pequeñas y medianas empresas fortalezcan sus controles de seguridad informática y desarrollen planes de respuesta ante incidentes cibernéticos. De esta manera, no solo estarán cumpliendo con la nueva normativa, sino que también se encontrarán mejor preparadas para afrontar los nuevos desafíos de la economía digital. Del mismo modo, la adaptación al marco GDPR mejorará la imagen de marca,

demostrando a sus clientes y demás socios de negocio su compromiso con la protección de los datos. En conclusión, el principal estímulo para adoptar los requisitos impuestos por el marco regulatorio no debería ser evitar las sanciones e infracciones financieras, sino el hecho de que a través de ello, la gestión de los datos e información será más eficiente, segura y así, poder responder de manera eficiente a las expectativas del cliente.

4.2.3 Responsable en ciberseguridad

La definición de los roles y responsabilidades es una tarea esencial si se pretende lograr un ámbito de ciberseguridad capaz de velar por la integridad, confiabilidad y disponibilidad de la información. La conformación de posiciones dentro de la estructura organizacional dependerá de su tamaño y de las necesidades del negocio en cuanto a la gestión de la seguridad informática. En este sentido, un rasgo característico de las PyMEs es la ausencia del diseño de un puesto jerárquico responsable de garantizar la seguridad de la información contenida en medios digitales. Por el contrario, la mayoría de las veces, esta suele ser una de las tantas tareas de los empleados del "área de sistemas"[11] de la compañía. En otras palabras, en este tipo de organizaciones la ciberseguridad es un aspecto exclusivamente abordado desde una perspectiva técnica. Aún más, generalmente no existen procesos y prácticas de seguridad informática establecidas, sino que las distintas tareas de carácter operativo desarrolladas por el personal asignado, generan un efecto sobre la protección de los activos informáticos (como por ejemplo, mantener actualizados los programas utilizados).

En cambio, las empresas que perciben del valor agregado de contar con procesos y procedimientos sólidos en torno a la gestión estratégica de la ciberseguridad tienden a incorporar la figura del CISO (*Chief Information Security Officer*). El director de la seguridad de la información se desempeña en el nivel ejecutivo de la compañía y tiene como principal función, la definición de una estrategia de seguridad informática, alineada a la estrategia y objetivos de negocio (Instituto Nacional de Ciberseguridad de España, 2016). El CISO es responsable del establecimiento y aplicación de políticas y prácticas de

[11] El entrecomillado hace referencia a que, muchas veces, ni siquiera existe formalmente un área de sistemas delineada en estas organizaciones.

seguridad cibernética para respaldar los objetivos de la organización y, lo suficientemente flexibles para ser modificados y/o actualizados según las necesidades del negocio y los cambios generados en el entorno. A medida que la complejidad de las operaciones y procesos del negocio aumentan, las necesidades de contar con personal especializado se hacen visibles y, entonces, se delinean nuevos puestos que se complementan en el desarrollo de un ámbito corporativo ciber-seguro. Por ejemplo, en las grandes compañías se encuentra la persona responsable de la seguridad de la organización: el CSO (*Chief Security Officer*). Este se caracteriza por tener una visión más integral de los riesgos a los que se encuentra expuesta la organización, en comparación con el CISO que se centra en los riesgos de seguridad de la información. Cuando coexisten ambas posiciones, el CISO reporta al CSO y este último a la dirección. El CIO (*Chief Information Officer*), otra de las posiciones presentes en las grandes empresas, es el encargado de alinear las estrategias de la organización con la tecnología informática para lograr los objetivos planificados. Asimismo, cabe señalar que en estas compañías, el CIO y el CISO son dos grandes posiciones de nivel ejecutivo (el denominado *C-level*) que responden de manera directa al CEO (*Chief Executive Officer*). Tradicionalmente, el responsable de la seguridad informática corporativa se encontraba debajo de la figura del CIO, es decir, respondía a los intereses de este último. Sin embargo, el crecimiento de las empresas provocó que se desvincule al CISO de la dependencia del CIO, para así poder generar un mayor ámbito de control recíproco entre ambas posiciones.

En cuanto a la figura del CEO, el reporte directo del responsable en seguridad informática al director general, es un indicador que demuestra el carácter prioritario que posee la ciberseguridad en la organización. En estos casos, los líderes de ciberseguridad suelen participar en reuniones de directores corporativos, por lo cual deben contar con el adecuado conocimiento del negocio para ser capaces de ejercer influencia en las decisiones. De esta manera, deben evitar adoptar una postura exclusivamente técnica, presentando las soluciones tecnológicas que se requieren abordar para abastecer las necesidades del negocio, en vez de plantear la manera en que se crean oportunidades de negocio a través de aquellas soluciones. El tipo de antivirus o

software de encriptación de documentos que se implementará debería ser el resultado de una conversación enfocada en los desafíos que tiene la empresa, en un lenguaje de negocios y de la manera en que la ciberseguridad puede impulsar su innovación y crecimiento. En otras palabras, vincular las iniciativas de seguridad cibernética a los resultados comerciales que proporcionan valor más allá de proteger a la organización, es una buena manera de demostrar la alineación de la ciberseguridad con el logro de los objetivos del negocio.

En síntesis, el encargado en seguridad informática puede recibir distintos nombres, tener asignadas más o menos responsabilidades, pero lo importante es que exista una persona cuya principal actividad consista en adoptar las medidas necesarias para la protección de los activos informáticos de la organización y el resguardo de la información. Los líderes en ciberseguridad deben complementar sus conocimientos y capacidades técnicas con el entendimiento integral del negocio para poder desarrollar su función de manera eficiente y, principalmente, para contar con los fundamentos necesarios para lograr convencer a la alta dirección acerca de la relevancia del tratamiento de la seguridad informática. "*A CISO's role today is primarily risk management, where they are more of an advisor and strategist, while being technologist behind the scenes*" (Roy, 2018)[12]. En resumidas palabras, el líder de ciberseguridad debe resaltar la función habilitadora del negocio que poseen las actividades desarrolladas en torno a la conformación de un espacio de seguridad informática, ayudando a las organizaciones a responder de manera más eficiente a las necesidades cambiantes del entorno y obtener una ventaja competitiva, estimulando la innovación y el crecimiento.

Métricas de ciberseguridad

Como toda actividad desarrollada con determinado objetivo, el ámbito de ciberseguridad y las tareas llevadas a cabo para su conformación deben ser evaluadas y controladas para poder ser mejoradas y adaptadas a las nuevas necesidades del negocio. De esta manera, algunas de las métricas de performance más empleadas en este campo son:

- Tiempo para detectar y resolver o mitigar una vulnerabilidad crítica.

[12] "El papel de un CISO hoy en día es principalmente la gestión de riesgos, donde es más un consejero y estratega, mientras que es un técnico detrás de escena" (traducción propia).

- Tiempo para detectar un incidente de ciberseguridad.
- Tiempo para resolver un incidente y retornar a la actividad operativa del negocio.
- Costo de los incidentes de ciberseguridad respecto del presupuesto asignado a esta área.
- Costo de la recuperación ante un ciberincidente.
- Ahorro (operativo, legal, etc.) obtenido por evitar la materialización de un incidente.
- Indicador de reducción de ciberincidentes luego de la adopción de medidas de seguridad informática.

A través de la medición, la organización podrá evaluar el grado de cumplimiento de los objetivos de ciberseguridad preestablecidos y tomar decisiones al respecto, ya que lo que no se mide, no se gestiona y, lo que no se gestiona, no se puede mejorar. Los indicadores y las métricas efectivas de ciberseguridad deben ser utilizadas para identificar debilidades en los procesos evaluados, determinar mecanismos para optimizar el empleo de recursos de seguridad informática y analizar el funcionamiento de las soluciones implementadas.

Además, las métricas constituyen una buena forma de justificar las inversiones en seguridad cibernética brindando visibilidad sobre su efectividad, a través de indicadores relevantes para el negocio. En este sentido, el ROI (*Return on Investment*) puede ser utilizado para evaluar el beneficio obtenido respecto de la inversión realizada en seguridad informática, la cual puede ser medida a través del TCO (*Total Cost of Ownership*) que permite visualizar el costo total de la inversión llevada a cabo, teniendo en cuenta los gastos en *software* y *hardware*, el entrenamiento del personal, los tiempos de implementación, el soporte y mantenimiento, entre otros costos.

4.3 Ciberincidentes

Los ciberincidentes (o incidentes informáticos/cibernéticos) es el término general que abarca a aquellos incidentes y ataques relacionados con la seguridad de las tecnologías informáticas. De esta manera, pueden clasificarse de distintas maneras en función de varios factores, como por ejemplo, el tipo de

incidente (*ransomware*[13]*, phishing*, virus informático, etc.), el objetivo (robo, alteración de la información, destrucción de redes, sistemas, etc.), el perfil de los usuarios afectados (su posición dentro de la organización), entre otras variables. En función de los objetivos planteados en la presente investigación —y debido a la inviabilidad que significaría abordar la gran cantidad de incidentes cibernéticos que existen y que continúan surgiendo de manera constante— nos focalizamos en el tratamiento de los siguientes ciberincidentes, según el origen e intencionalidad de la amenaza, cuyo objetivo sea el robo, alteración o manipulación de la información digital. De esta manera, podemos clasificarlos en:

1) Ataques informáticos externos: son aquellos actos llevados a cabo por agentes ajenos a la infraestructura, aplicaciones, servicios y red corporativa que lograron vulnerar los controles de seguridad informática e ingresar a la red, con el objetivo de generar un daño a la organización.
2) Ataques informáticos internos: generados por empleados, proveedores o socios estratégicos desleales con acceso autorizado a la red corporativa e intención de causar un daño.

Los mencionados hasta aquí comparten la intencionalidad del acto realizado y el objetivo y, se diferencian en el origen del ataque. Cabe agregar que aquellas personas que realizan ataques informáticos externos se conocen como *crackers* en el ámbito informático. Estos se diferencian de los conocidos *hackers*, los cuales utilizan sus conocimientos y habilidades técnicas para introducirse en sistemas informáticos ajenos con el objetivo de poner a prueba sus capacidades y demostrar las brechas de ciberseguridad existentes en determinado contexto. En cambio, los *crackers* emplean sus habilidades para producir daños, muchas veces con fines delictivos, en los sistemas que logran vulnerar.

Por último, en función de la clasificación mencionada, se encuentran los:

3) Incidentes informáticos internos: cuando se trate de un suceso accidental causado por negligencia, desinformación o mal uso de un

[13] *Ransomware*: es un código malicioso utilizado para secuestrar datos, es decir, un tipo de ciberataque en la cual el atacante cifra los datos de la víctima y exige un pago (recompensa) por la clave de descifrado.

recurso tecnológico, por parte de miembros de la organización, en donde se demuestre que no existió motivación de causar ningún tipo de daño.

"*Information is data made meaningful*" (*Information Systems Audit and Control Association*, 2017, p. 5)[14]. Por lo tanto, la gestión eficiente de los datos, en todas sus formas (texto, número, sonido, gráfico, video, etc.), es una cuestión fundamental dentro de cualquier tipo de organización. Pues, los datos procesados bridan información valiosa para la toma de decisiones, tanto operativas, como estratégicas. En otras palabras, "*the successful use of data drives the accomplishment of enterprise goals*" (*Information Systems Audit and Control Association*, 2017, p. 5)[15]. Asimismo, la información puede ser utilizada para generar conocimiento clave dentro de la compañía. En este sentido, los ciberincidentes analizados en la presente investigación son aquellos que representan una amenaza contra las principales cualidades que brindan calidad a la información y limitan la posibilidad de optimizar las decisiones tomadas a partir de ella:

a) Disponibilidad: garantizar el acceso a la información a quienes estén autorizados, cuando sea necesario. La principal amenaza contra la disponibilidad es la eliminación de datos, información o recursos.
b) Confidencialidad: consiste en que solamente aquellos que estén autorizados puedan acceder a la información. Por lo tanto, el acceso no autorizado a ella representa la principal amenaza.
c) Integridad: solo los autorizados pueden realizar modificaciones en la información para garantizar su fiabilidad. Los cambios, alteraciones o ingreso de información falsa amenazan la integridad de los recursos.

En la siguiente tabla, con el objetivo de enmarcar las distintas vulnerabilidades que afectan a los sistemas informáticos y, en consecuencia, a los datos e información contenida en estos medios, se puede observar la correlación que existe entre los tipos de vulnerabilidades y las diferentes medidas que se pueden implementar en este sentido:

[14] "La información son datos provistos de significado" (traducción propia).

[15] "El uso exitoso de datos impulsa el logro de los objetivos de la empresa" (traducción propia).

Vulnerabilidades	Descrpción	Ejemplos	Medidas			
			Preventivas[1]	Detectivas[2]	Correctivas[3]	Disuasivas[4]
Naturales	Daños ocasionados por causas del ambiente o desastres naturales sobre la infraestrucutra tecnológica.	Incendios, inundaciones, cortes de electricidad, excesiva humedad, picos de temperatura, huracanes.	Sistema de prevención de incendios, UPS, sistema de regulación de temperatura y humedad.	N/A	Extintor, Póliza de seguro.	N/A
Personas	Errores humanos no intencionales e intencionales que derivan en un daño a la infraestrucutra tecnológica.	Errores y/o omisiones en el ingreso de datos, acceso no autorizado, fraude, robo y alteración de información.	Autenticación de usuarios (contraseñas seguras), permisos de acceso a recursos, segregación de funciones.	Antivirus, antispam.	Reparación del daño efectuado, Plan de respuestas.	Selección y capacitación del personal, políticas y normas de ciberseguridad, sanciones administrativas y penales.
Hardware	Situaciones en las que las herramientas de *hardware* se encuentran expuestas a sufrir un daño.	Cortes y alta tensión eléctrica, errores de configuración, daño por uso inapropiado, robo de equipos.	Control de acceso (claves, autenticación biométrica), cámaras de seguridad, personal de seguridad.	Alarmas, personal de seguridad.	*Back-up,* Restauración del hardware afectado, Plan de contingencias.	Políticas y normas referidas a la gestión del *hardware.*
Software	Consiste en la posibilidad de que el sistema sea accesible debido a fallas en el software.	Errores de programación, de instalación, cambios sin autorización.	Control de acceso (contraseñas), encriptación de datos, actualización del software.	Notificaciones de aviso sobre actualizaciones disponibles.	*Back-up,* Recuperación de los sistemas afectados, Plan de contingencias.	Políticas y normas referidas a la gestión del *software.*
Redes y comunicaciones	Daño causado mediante el acceso o manipulación indebido de las redes corporativas.	Robo de información, intersección indebida de datos en una comunicación.	Encriptación de datos, *Virtual Private Network* (VPN), restricción de acceso a sitios web.	Sistema de detección de intrusos, *Firewall*.	Restauración de las comunicaiones, Plan de contingencias.	Políticas y normas referidas a la gestión de las redes y la información que circula a través de ella.

[1] Preventivas: actúan antes de que un hecho ocurra con el objetivo de detener la materialización de situaciones no deseadas.

[2] Detectivas: actúan antes de que ocurra un hecho y su función es identificar y revelar la presencia de situaciones no deseadas para evitar que sucedan.

[3] Correctivas: tienen efecto luego de que suceda el hecho y, se encuentran orientadas a recuperar la capacidad de operación normal.

[4] Disuasivas: su propósito es desalentar las acciones que puedan derivar en una situación no deseada.

Fuente: elaboración personal.

Los ataques informáticos o ciberataques (tanto internos como externos) pueden ser clasificados como ciberdelitos o delitos informáticos, si el hecho llevado a cabo es susceptible de sanción penal, de acuerdo a la legislación que correspondiera aplicarse.

El Convenio sobre la Ciberdelincuencia del Consejo de Europa define a los ciberdelitos como “actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos” (2001, p.1). En otras palabras, un delito informático es un acto intencionado llevado a cabo por una o más personas, en el que:

a) los sistemas informáticos constituyen el objetivo del hecho (por ejemplo: acceso ilegítimo a un sistema, destrucción de una red) o;

b) los sistemas informáticos son utilizados como medio o instrumento para provocar daños contra terceros (por ejemplo: fraude informático, falsificación de datos digitales).

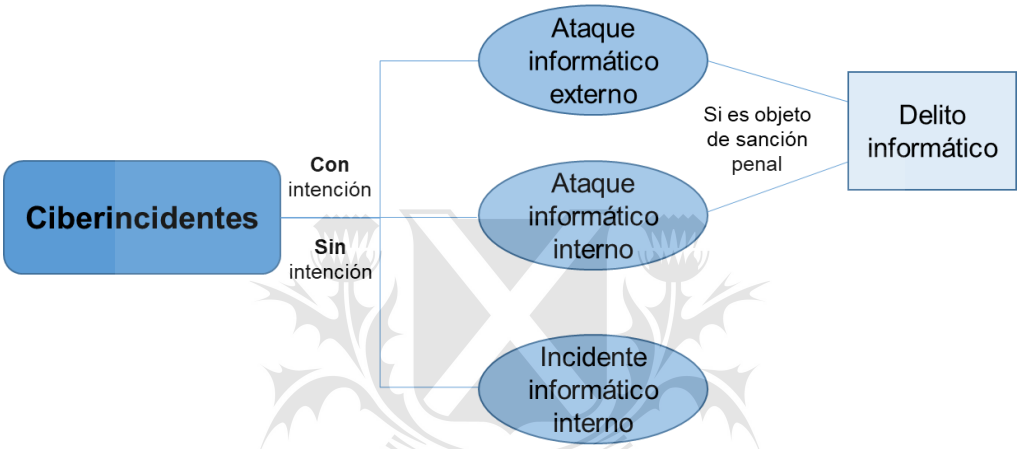
En palabras de especialistas en auditoría de sistemas, lo delitos informáticos pueden definirse como:

> “toda conducta ilícita que puede ser sancionada a la luz del Derecho Penal, por hacer uso indebido de la información y de cualquier medio informático empleado para su manejo, o de la tecnología electrónica o computarizada, como método, como medio o como fin, en perjuicio de la libertad de las personas y organizaciones, o de su patrimonio, o propiedad (activos), o de su derecho a la vida, a la intimidad, al crédito y buen nombre”. (Ojeda-Pérez *et al.*, 2010, p. 51)

En este sentido, resulta pertinente remarcar —a fin de evitar confusiones— la diferencia entre la noción de ataque informático/ciberataque del concepto de delito informático/ciberdelito, puesto que este último hace referencia a todos aquellos ciberataques que se encuentran tipificados como hecho delictivo en la normativa jurídica que rige en el país. La legislación en materia de delitos informáticos varía según la relevancia brindada a dicho aspecto por cada nación. Por lo tanto, con lo enunciado hasta aquí, es posible afirmar que todos los ciberdelitos son ciberataques pero, generalmente, no todos los ataques

informáticos se encuentran tipificados como delitos y, por ello, no pueden ser considerados como tales. Esto sucede debido a que el avance de estos actos contrarios a las buenas costumbres, aumenta constantemente a una velocidad sin precedentes, de manera tal que la legislación se encuentra atrasada por el proceso mismo que constituye sancionar una norma que regule y sancione una nueva conducta antijurídica.

El gráfico a continuación refleja, a modo de esquema, los conceptos abordados en la sección:



Fuente: elaboración personal

4.3.1 Legislación argentina en ciberdelitos

En el caso de la normativa argentina, existen tres leyes que encuadran las distintas figuras delictivas del ámbito de la ciberseguridad, las cuales resultan pertinentes enunciar en función de los objetivos planteados en la presente investigación.

En primer lugar, la Ley de Protección de Datos Personales (Ley 25.326), tal como establece el artículo 1, tiene como objetivo “la protección integral de los datos personales asentados en archivos, registros, banco de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas”. En segundo término, la Ley de Propiedad Intelectual (Ley 11.723) establece la protección del derecho de propiedad sobre obras científicas, literarias y artísticas, incluyendo “los escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto”. Luego, la

Ley de Delito informático (Ley 26.388) sustituye, modifica e incorpora figuras delictivas a diversos artículos del Código Penal con el fin de regular las nuevas formas de cometer delitos a través de medios tecnológicos. De esta manera, establece sanciones por el acceso ilegítimo a sistemas o datos informáticos, violación de correos electrónicos, daño informático y distribución de códigos maliciosos, e interrupción de las comunicaciones. Por último, cabe remarcar que Argentina se adhirió al Convenio sobre la Ciberdelincuencia del Consejo de Europa, a través de la Ley 27.411 del 2007.

5. Estrategia Metodológica

5.1 Tipo de investigación

La presente investigación se desarrolló en base a los lineamientos de un estudio descriptivo, cuyo principal objetivo es "especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis" dentro de su propio contexto, a través de la observación de sus principales características (Sampieri *et al.*, 2010, p. 80). En este sentido, se llevó a cabo una investigación descriptiva de la situación actual de la relevancia otorgada a la seguridad informática en las PyMEs argentinas de *retail* farmacéutico, cuyo propósito consiste en brindar una visión integral y precisa respecto del fenómeno abordado.

Asimismo, se adoptó una orientación cualitativa para analizar el objeto de estudio con el propósito de obtener información de calidad, relevancia y profundidad que permita arribar a conclusiones con las mismas características. En los estudios cualitativos "se trata de captar el núcleo de interés y los elementos clave de la realidad estudiada, facilitándose de esta manera el entendimiento de los significados, los contextos de desarrollo y los procesos" (Tonon, 2011, p. 2).

5.2 Método de investigación

El estudio descriptivo se encuentra complementado por un análisis comparativo de casos, con el objetivo de investigar las particularidades de la temática desarrollada dentro de las empresas seleccionadas.

El método de estudio comparado tiene como fin la búsqueda de similitudes y disimilitudes entre los casos estudiados (Tonon, 2011). Por lo tanto, el empleo de este método debe asegurar la selección de casos que realmente puedan ser comparados, es decir, que presentan variables similares que pueden ser consideradas constantes y variables disimilares susceptibles de contrastar. La comparación se basa en el criterio de homogeneidad de las unidades de análisis, siendo la identidad de clase el elemento que legitima dicha comparación. En nuestra investigación, el sector de las pequeñas y medianas empresas del sector de *retail* farmacéutico argentino justifica la comparación de los dos casos de estudios a abordar. En conclusión, el método comparativo sirve para confrontar dos o varias propiedades (variables o ejes de análisis) enunciadas en dos o más objetos, en un momento preciso o en un arco de tiempo más o menos amplio. El núcleo del estudio en una metodología de análisis de casos lo constituye un fenómeno contemporáneo, como resulta el caso de la ciberseguridad, dentro de un contexto particular, es decir, en el campo de las PyMEs de la industria *retail* farmacéutico en Argentina.

En síntesis, el presente trabajo se plantea desde la perspectiva de un estudio de casos descriptivo, cuyo objetivo es abordar de la forma más completa posible el objeto de estudio dentro de su propio contexto. Por último, resulta importante señalar, como una de las principales características del estudio comparado de casos, que las conclusiones de la investigación se encuentran acotadas a los casos abordados en ella, a las fronteras de las organizaciones analizadas. En este sentido, al momento de exponer las conclusiones del presente trabajo, se debe tener en cuenta su limitación, ya que no podemos suponer que representan al resto de la población de PyMEs del *retail* farmacéutico y, aún menos, del ámbito PyME en general. No obstante, resaltamos su valor como punto de contraste para otras investigaciones, con el objetivo de comprobar si estas conclusiones pueden ser aplicadas para otros casos de estudio.

5.3 Ejes de análisis

La ciberseguridad puede ser abordada desde múltiples perspectivas de análisis. Algunas de ellas serán presentadas como líneas futuras de investigación más adelante. En función de los objetivos establecidos en el

trabajo efectuado y del enfoque seleccionado para su tratamiento, se definen los siguientes ejes de análisis a aplicar en los casos de estudio seleccionados:

- Dimensiones generales de la ciberseguridad en la empresa: conocimiento del significado e impacto de la ciberseguridad y los ciberincidentes en el ámbito corporativo, presupuesto asignado a la ciberseguridad y diseño de la ciberseguridad en la organización;
- Análisis del estado de las funciones de la ciberseguridad;
- Implementación de políticas, mecanismos y soluciones para la protección de los activos de información del negocio.

5.4 Técnicas de recolección de datos

El análisis bibliográfico se realizó a partir de la lectura selectiva, comprensiva, estratégica y crítica de libros y artículos profesionales, a fin de obtener insumos teóricos, conceptos y datos relevantes para la presente investigación.

En el trabajo se utilizan fuentes de información primaria y secundaria. En el primer caso, se empleó una metodología de entrevistas a actores con influencia dentro del campo de la ciberseguridad. Se realizaron entrevistas abiertas a miembros clave de las PyMEs seleccionadas para indagar sobre los aspectos más relevantes, en función de los objetivos de investigación y variables planteadas anteriormente. Asimismo, se llevó a cabo una entrevista con un consultor especialista en ciberseguridad que aportó su visión sobre dicha disciplina. En el anexo 1 se encuentran las preguntas guía que enmarcaron las entrevistas mencionadas.

En el caso de los recursos de información secundaria, se acudió a artículos de revistas, *papers*, libros y conferencias, tanto de origen académico como profesional, y documentos publicados por organismos internacionales y entidades gubernamentales. Asimismo, se dio relevancia a los informes y reportes en materia de ciberseguridad realizados por consultoras y empresas proveedoras de infraestructura tecnológica de renombre en el plano internacional (tales como Gartner, McKinsey, Forbes, PwC, Ernst&Young, entre otras), los cuales brindan información valiosa, ejemplos de casos reales y datos del escenario complejo que presenta la ciberseguridad a nivel global.

Finalmente, con el objetivo de brindar una contextualización internacional acerca del tema abordado en un marco global, se presenta el estado de la seguridad informática en los casos de Estados Unidos y Chile. En este sentido, se establece qué se hace en otro lugar del mundo respecto de la seguridad informática: ¿existe una mayor consciencia sobre la (in)seguridad informática?, ¿qué medidas se llevan a cabo para atenuar las vulnerabilidades ante eventuales ataques informáticos?

5.5 Justificación de los casos de estudio

Para la presente investigación, se han seleccionado las siguientes PyMEs argentinas de la industria de *retail* farmacéutico como unidades de análisis: Zona Vital y FarmaBelén. Además de la viabilidad (acceso a fuentes de información), requisito excluyente para desarrollar el trabajo, a continuación se delinean diversas razones por las cuales se han seleccionado dichas organizaciones.

En primer lugar, ambas encuadran dentro de la clasificación legal para ser tratadas como PyMEs. Por un lado, Zona Vital es una sociedad en comandita simple que se encuentra conformada por catorce locales, los cuales poseen personería jurídica independiente (presentan balances y tributan como sociedades independientes) y se categorizan como PyME. No obstante, la administración se encuentra centralizada. Por otro lado, FarmaBelén es una sociedad anónima que se encuentra alcanzada por la resolución que clasifica a las pequeñas y medianas empresas. Además, desde la perspectiva jurídica, ambas compañías se encuentran sujetas al cumplimiento de la Ley de Protección de Datos Personales (Ley 25.326), debido a que administran datos e información de terceros.

En segundo término, tanto Zona Vital como FarmaBelén son compañías referentes, con una vasta trayectoria en el mercado farmacéutico argentino. Además, desde el punto de vista metodológico, resultan compañías comparables en cuanto a sus estructuras y operatoria de negocio: poseen cantidades similares de locales, tienen una fuerte presencia en la Provincia de Buenos Aires, segmentación del negocio en dos actividades, entre otras características. Asimismo, ambas empresas registran, procesan y almacenan

datos de clientes de distintas maneras (datos que surgen de las transacciones físicas y *online* —números de tarjetas de crédito, nombre y apellido, domicilio, etc.—) y cuentan con información crítica para el negocio respaldada en sus tecnologías informáticas. Finalmente, a modo de contraste entre las firmas, cada una ha avanzado de una manera distinta en cuanto al desarrollo de herramientas que le permitan ofrecer nuevos servicios de excelencia al cliente. Mientas Zona Vital ha desarrollado su tarjeta de puntos para recopilar datos de los clientes y obtener información valiosa del comportamiento del consumidor, a partir de su análisis, FarmaBelén ha iniciado su experiencia de venta a través de su sitio web.

CAPÍTULO 2: CIBERSEGURIDAD EN ARGENTINA

En el siguiente capítulo se lleva a cabo una descripción del ámbito de la ciberseguridad en Argentina que va de lo general al ámbito particular de las PyMEs de *retail*, con el objetivo de dar a conocer el contexto en el que estas organizaciones se encuentran desarrollando sus negocios. Primero, se describe el estado de la seguridad informática en el ámbito nacional, tanto en el sector público, como en el privado y, luego, se delinean las principales características de dicha temática en las pequeñas y medianas empresas del sector de *retail*.

1. Situación general de la ciberseguridad nacional

La ciberseguridad es un tema que preocupa a nivel global. El Estado tiene la obligación de involucrarse en el despliegue de los mecanismos de difusión de los recaudos que los ciudadanos deben tomar al respecto, como así también establecer medidas de prevención de incidentes informáticos. Cabe destacar que, a pesar de que la mayoría de los datos estadísticos reflejan un panorama complejo en torno a los desafíos de la ciberseguridad, el gobierno ha tomado conciencia de la problemática existente en torno a la seguridad informática y ha comenzado a tomar algunas medidas. En este sentido, se creó el Comité de Ciberseguridad que tendrá como principal objetivo desarrollar una estrategia nacional de seguridad informática, enfocada en la mejora de los marcos normativos existentes para abarcar la creciente aparición de ciberincidentes y el desarrollo de medidas técnicas, políticas y procedimientos que permitan establecer una cultura de ciberseguridad en el país. Por ello, tal como expresó el Subsecretario de Tecnologías y Ciberseguridad de la Nación, Álvarez Prado:

> “La Ciberseguridad […] es un nuevo Paradigma que nos compete a todos, ya que la vida se trasladó allí. Hay una vida social, económica, financiera y comercial, todo pasa por el ciberespacio, ya que es un sitio común. No hay un único gobierno ni una única ley que lo regule, tampoco fronteras. Es una realidad que llegó para quedarse.” (Comisión de Ciberseguridad, 2017, p. 1)

El grado de madurez de la ciberseguridad en Argentina puede ser analizado a partir de los diferentes ejes de análisis propuestos por el Observatorio de la Ciberseguridad en América Latina y el Caribe[16]. De esta manera, podremos aproximarnos al contexto actual de la ciberseguridad en Argentina y analizar el escenario que se presenta para el crecimiento de las organizaciones.

En primer lugar, desde la perspectiva de la **política y estrategia**, Argentina se encuentra en un período de formación de una estrategia nacional de seguridad cibernética, a través del "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" (ICIC). Dicha estrategia se encuentra focalizada en la creación de consciencia en el público acerca de los riesgos asociados, la mitigación de la ciberdelincuencia y la capacidad de respuesta ante este tipo de hechos. Asimismo, se ha comenzado a diseñar y difundir un programa de ciberseguridad de cooperación nacional, el cual busca reunir esfuerzos para la construcción de un cuerpo de conocimiento provisto de experiencias y mejores prácticas en dicho campo. Por último, se ha avanzado en la identificación de los riesgos, las amenazas externas e internas y las vulnerabilidades del sistema nacional de ciberseguridad.

En segunda instancia, en cuanto a la creación de una **cultura de consciencia** e importancia brindada a la seguridad cibernética, el análisis se puede dividir en tres áreas. Desde el gobierno, se ha comenzado a brindarle prioridad a la ciberseguridad, a través de la creación de organismos y proyectos destinados al tratamiento de dicho aspecto (Ministerio de Seguridad Nacional, Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), Subsecretaría para la Protección de Infraestructura Crítica y Ciberseguridad, Comisión de Ciberseguridad). En el sector privado, si bien el nivel de concientización es mayor que en el sector público, aún queda un largo camino por recorrer para establecer una firme mentalidad de seguridad informática y de la importancia de la formación de una cultura de cooperación entre las empresas para afrontar los incidentes. Finalmente, en la sociedad se puede observar la adopción paulatina de una mentalidad de ciberseguridad, a través de los programas y materiales desarrollados desde las entidades

[16] Observatorio de Ciberseguridad en América Latina y el Caribe: institución fundada en conjunto por la OEA -Organización de los Estados Americanos- y el BID -Banco Internacional de Desarrollo-.

gubernamentales para mejorar las prácticas de seguridad cibernética. Sin embargo, aún no se reconoce la necesidad de una política de difusión de la información acerca de casos de delitos cibernéticos en las organizaciones públicas y privadas.

La tercera variable definida por el Observatorio de la Ciberseguridad es la **educación** en seguridad cibernética. En este aspecto, cabe mencionar que existe formación en dicha materia, aunque todavía se encuentra limitada y se requiere incorporarla en una mayor cantidad de programas educativos del país. Asimismo, el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad brinda cursos, talleres y charlas en materia de seguridad informática. En el ámbito empresarial, las cuestiones de seguridad cibernética suelen ser delegadas al Director de Información o CISO (*Chief Information Security Officer*), quien tiene la responsabilidad de proveer niveles de seguridad acordes a las necesidades del negocio. La formación de profesionales en ciberseguridad es un punto de partida para poder gestionar de manera más eficiente la seguridad informática, ya que no es posible reaccionar y defenderse de lo que no se conoce. En consecuencia, en la actualidad, la gestión de la ciberseguridad es en gran medida reactiva, es decir, que se desarrollan mecanismos de respuesta ante incidentes cibernéticos, en vez de anticiparse a su materialización.

En cuarto lugar, los **marcos legales** implementados en Argentina respecto de la seguridad informática protegen los derechos de los individuos y las organizaciones en el entorno digital. En este sentido, la legislación vigente tipifica una serie de delitos relacionados con pruebas electrónicas que pueden ser abordados en el código penal. No obstante, cabe mencionar que hay pocos jueces con la capacidad para presidir un caso sobre delito cibernético y, actualmente, no se destinan recursos a la formación judicial en delincuencia cibernética. Por su parte, la Subsecretaría de Tecnologías y Ciberseguridad del Ministerio de Modernización brinda una guía para la realizar denuncias frente a delitos informáticos. Asimismo, ofrece una serie de recomendaciones básicas para el resguardo de la información que se encuentra expuesta a los riesgos de seguridad informática y cursos de capacitación en dicho ámbito.

Por último, según el Observatorio de la Ciberseguridad en América Latina y el Caribe, las **tecnologías** de información utilizadas a nivel nacional cumplen los estándares internacionales y están alineados con las mejores prácticas. Por ejemplo, en el comercio electrónico se implementan medidas y procesos de autenticación de las transacciones. No obstante, como se ha señalado anteriormente, es necesario adherirse a normas internacionales de ciberseguridad para aumentar el nivel de seguridad en el ámbito digital, tal como se con el Convenio sobre la Ciberdelincuencia del Consejo de Europa, lo cual representa un avance en el proceso de concientización sobre los riesgos del mundo digital. Asimismo, cabe resaltar que el mercado local de la seguridad informática ofrece productos genéricos, no especializados y se encuentra bastante retrasado respecto de la oferta internacional de *software* destinado a la ciberseguridad. A su vez, se ha identificado la necesidad de creación de un mercado de seguros de delincuencia informática que ofrece distintas alternativas según la evaluación de riesgos financieros para el sector privado y público. Al momento, este negocio se encuentra en desarrollo y en búsqueda de las mejores prácticas para la evaluación de los riesgos mencionados. La aparición de estos productos demuestra la importancia de la adopción de medidas de ciberseguridad en los negocios. De hecho, muchas instituciones financieras y crediticias ya han incorporado la variable cibernética entre los parámetros evaluados para la valuación crediticia de las organizaciones.

Los ejes de análisis definidos por el Observatorio de la Ciberseguridad en América Latina y el Caribe se encuentran estrechamente relacionados con los puntos propuestos por la Comisión de Ciberseguridad en 2017 para mejorar el ámbito de la seguridad informática: desarrollo de marcos regulatorios, formación y cooperación. Actualmente, en Argentina, la problemática de la ciberseguridad es un punto central en la agenda del Estado y, por ello, se ha dispuesto el trabajo conjunto del Ministerio de Modernización, el Ministerio de Defensa y el Ministerio de Seguridad de la Nación en el desarrollo y elaboración de una estrategia nacional de ciberseguridad para responder al crecimiento exponencial de los incidentes informáticos. En la siguiente tabla se exhibe el estado de madurez de la ciberseguridad en Argentina, a partir del nivel de desarrollo de los ejes mencionados:

Observatorio de la CiberSeguridad en Latinoamerica y el Caribe	Argentina (escala del 1 al 5)
Política y estrategia	
Estrategia nacional de seguridad cibernética oficial o documentada	
Desarrollo de la estrategia	2
Organización	2
Contenido	3
Cultura y sociedad	
Mentalidad de seguridad cibernética	
En el gobierno	2
En el sector privado	3
En la sociedad	2
Conciencia de seguridad cibernética	
Sensibilización	2
Educación	
Disponibilidad nacional de la educación y formación cibernéticas	
Educación	3
Formación	2
Desarrollo nacional de la educación de seguridad cibernética	
Desarrollo nacional de la educación	1
Formación e iniciativas educativas públicas y privadas	
Capacitación de empleados	2
Gobernanza corporativa, conocimiento y normas	
En las empresas estatales y privadas	3
Marcos legales	
Marcos jurídicos de seguridad cibernética	
Para la seguridad de las TIC	3
Privacidad, protección de datos y otros derechos humanos	3
Derecho sustantivo de delincuencia cibernética	3
Derecho procesal de delincuencia cibernética	3
Divulgación responsable de la información	
Divulgación responsable de la información	1
Tecnologías	
Adhesión a las normas	
Aplicación de las normas y prácticas mínimas aceptables	2
Adquisiciones	2
Desarrollo de software	2
Mercado de la ciberseguridad	
Tecnologías de seguridad cibernética	2
Seguros de delincuencia cibernética	2

Fuente: elaboración personal. Recuperado de: http://observatoriociberseguridad.org/

En conclusión, Argentina se encuentra en una etapa inicial de concientización y aprendizaje en el ámbito de la ciberseguridad. Dada la complejidad y relevancia del tema abordado, el cual afecta de manera transversal a todos los sectores de la sociedad, resulta necesaria la participación y colaboración conjunta de los distintos actores (sector público, privado y particulares). En este proceso, el rol del Estado adquiere suma trascendencia para demostrar la importancia de su tratamiento. La cooperación entre el sector público y el privado debe ser un paso inicial para compartir experiencias y generar una comunidad en donde se discutan sobre las mejores prácticas en ciberseguridad. Para ello es fundamental la adopción de normas que primero motiven y luego, obliguen a las organizaciones a denunciar los ciberincidentes, ya que las compañías se resisten a reportar públicamente estos sucesos. Asimismo, es necesario mantener actualizados los cuerpos de normas para abarcar las nuevas tendencias delictivas en el mundo digital y castigar a los responsables. No obstante, a pesar de todos los esfuerzos que se puedan realizar para crear una

cultura de concientización y cooperación, resulta oportuno retomar una de las ideas principales del presente trabajo: la seguridad absoluta no existe y, por lo tanto, lo mejor que se puede hacer es minimizar los riesgos y atenuar el impacto de un eventual ciberincidente. En definitiva, es a esta tarea a la que deben abocarse las organizaciones.

2. Ciberseguridad en PyMEs de la industria de *retail*

Como se ha mencionado en el apartado anterior, en el sector privado existe un mayor nivel de concientización respecto de la ciberseguridad en comparación con el sector público. En este sentido, un estudio realizado por la consultora Frost & Sullivan plantea que la complejidad creciente de los ciberataques es uno de los factores principales que impulsa la inversión en ciberseguridad en las empresas argentinas (Ebizlatam, 2017). De esta manera, sostiene que durante el período 2018-2022, la seguridad informática será una de las áreas en la cual más se focalizarán las empresas del país. Es importante que las organizaciones comiencen a entender las soluciones de ciberseguridad como potenciadores del negocio y generadores de ventajas competitivas. Sin embargo, según PwC, la mayoría de las empresas argentinas (53%) no cuenta con una estrategia para proteger la información (Encuesta Global de Seguridad de la Información, 2018). Del mismo modo, el 54% no posee un programa de capacitación en seguridad informática para sus empleados y el 61% carece de un plan de contingencia ante la ocurrencia de un incidente cibernético.

Una eficiente gestión de la ciberseguridad en el ámbito corporativo cumple, principalmente, dos objetivos de manera simultánea. Mientas que por un lado, genera la reducción de los riesgos y materialización de los ciberincidentes en las organizaciones, por el otro, genera grandes beneficios: el crecimiento del negocio, el impulso por innovar y la construcción de vínculos de confianza con los clientes. En el caso de las compañías de *retail*, este último aspecto resulta de especial importancia para la creación de bases sólidas que estimulen el desarrollo organizacional. Las exigencias de los consumidores han crecido en los últimos años, en función del aumento de la información disponible con la que cuentan para evaluar y comparar las empresas con las que deciden

realizar sus transacciones. Por tal motivo, la seguridad cibernética debe ser abordada como un pilar fundamental en pos del resguardo, no solo de los datos e información confidencial que administra de sus clientes, sino también de los activos digitales críticos del negocio.

En la industria del *retail* obtener el apoyo y ganar la confianza de los consumidores nunca fue una tarea sencilla y, aún menos en la actualidad, donde el cambio es lo único certero y nadie puede escapar a los riesgos que implica operar a través de tecnologías informáticas. El reporte de PwC sobre la protección de los consumidores en esta era digital destaca que la confianza de los clientes en las organizaciones decrece año tras año (*Consumer Intelligence Series: Protect.me.*, 2017). Las compañías que actúan en el segmento de *retail online* se encuentran dentro de los negocios con menor nivel de confiabilidad por parte de los usuarios. Tan solo el 13% de ellos confía en las prácticas de ciberseguridad implementadas en cuanto a la gestión de su información personal. Este aspecto abre un abanico de oportunidades para las empresas, ya que quien logre ganar la confianza de los consumidores (a través de la transparencia en el manejo responsable de la información confidencial), habrá dado un notable paso diferenciándose de sus competidores. En este sentido, las empresas deben adoptar una actitud proactiva respecto de la protección de la información y la construcción de un ambiente de ciberseguridad, al mismo tiempo que buscan nuevas maneras de monetizar este recurso clave para el negocio.

Asimismo, los consumidores aprecian positivamente que las compañías notifiquen las brechas de seguridad informática que detectan. No obstante, como se ha mencionado anteriormente, las organizaciones suelen ocultar lo sucedido cuando padecen un incidente cibernético, pues temen que su comunicación derive en grandes pérdidas económicas. Los consumidores buscan transparencia y responsabilidad; por ello, valoran que las organizaciones (además de recompensarlos) expliquen lo que sucedió y brinden una clara descripción de los cambios que se implementarán en el ámbito de la ciberseguridad para que no vuelva a ocurrir. El empuje del lado de los clientes podría impulsar el progresivo abandono de la (mala) práctica de no comunicar a terceros los incidentes informáticos sufridos y, así, colaborar en la

conformación de una cultura de cooperación entre los distintos agentes del mercado. Las compañías deben comprender las necesidades de los consumidores, no solo en lo que respecta al producto o servicio final ofrecido, sino también en cuanto a los aspectos ligados a la ciberseguridad. La eficiente gestión del espacio de seguridad informática funcionará como una palanca impulsadora del crecimiento organizacional de las pequeñas y medianas empresas. Para ello, la estrategia de seguridad informática y privacidad de la información de los consumidores debe estar contenida y ser parte esencial de la estrategia integral del negocio.

Las PyMEs, como se ha mencionado en la presente investigación, desempeñan un rol fundamental en el desarrollo de las economías nacionales. La vulnerabilidad de estas organizaciones puede significar un gran riesgo dentro del ecosistema empresarial en el cual desarrollan sus operaciones. Ello se debe a que un ciberincidente que tiene lugar en una de estas firmas puede generar consecuencias en su red empresarial, afectando a proveedores y cualquier tipo de socio de negocio que se encuentre interconectado a ella. En este sentido, la ciberseguridad representa un gran desafío, al mismo tiempo que puede significar una fuente creadora de ventajas competitivas para aquellas que logren gestionar un ámbito de ciberseguridad eficiente.

Actualmente, las PyMEs, según Nicolás Ramos (*Executive Director* en Ciberseguridad de EY Argentina), se caracterizan por tener un bajo nivel de adopción de medidas de seguridad informática para el respaldo de sus procesos de negocio soportados por infraestructura tecnológica[17]. Según el profesional, esta conducta suele ser justificada, desde el entorno de las pequeñas y medianas empresas, a partir de las restricciones presupuestarias con las que se encuentran en el día a día para llevar adelante su negocio. Pero, cabe preguntarnos, ¿por qué al tratarse de otros proyectos para potenciar las ventas, a través una campaña de marketing por ejemplo, se cuenta con un presupuesto más holgado? El hecho es que, tal como afirma el director ejecutivo referido anteriormente, la seguridad informática es percibida como un costo y no como una inversión capaz de potenciar el negocio de las PyMEs. Ello radica en la falta de una visión estratégica de los directivos

[17] Entrevista personal. Ver *Anexo 1: Entrevistas para mayor detalle*.

respecto de la conformación de un ámbito ciber-seguro. Asimismo, esa posición se ve potenciada por la falta de concientización sobre los riesgos a los que se encuentra expuesta su organización en ese sentido, la cual refleja la deficiencia en la percepción del panorama de amenazas en el que se desenvuelven. El cambio en estos aspectos resulta primordial para comenzar a inclinar la historia en el ámbito de la ciberseguridad de las PyMEs de la industria de *retail*.

Por su parte, la filosofía del *cost killing*[18] que predomina en estas compañías, señala Ramos, impide analizar a la seguridad informática como una inversión necesaria de realizar. En otras palabras, frente al desafío de obtener ganancias con los estrechos márgenes característicos en el negocio de las firmas de *retail*, la necesidad de reducir costos y el entendimiento de la ciberseguridad como tal, obstaculiza la asignación de un presupuesto destinado a dicha actividad. Por estos motivos, la participación de un agente/consultor externo a la organización podría ayudar a modificar esta creencia, haciendo foco en el estrecho vínculo que existe entre la seguridad informática y la mejora de los resultados financieros. Resaltando los beneficios de una inversión eficiente en ciberseguridad y observando el repago generado (haciendo el cálculo del ROI, por ejemplo), es posible cambiar esta perspectiva en el ámbito PyME.

En las pequeñas y medianas empresas, dada la escasez de recursos, el proceso de evaluación y determinación de prioridades al momento de analizar inversiones en materia de ciberseguridad es fundamental para evitar el derroche de recursos. En este proceso, los altos directivos desempeñan un rol fundamental, pues la inversión en un programa de seguridad para la protección de los activos digitales críticos de la organización exige un compromiso en todos los niveles y áreas. En definitiva, "*cybersecurity investment must be a key part of the business budget cycle"* (Kaminski *et al.*, 2017)[19]. Los programas eficientes de ciberseguridad le brindan la posibilidad a las PyMEs de *retail* a competir en el mercado, a través de la constante innovación y la confianza y

[18] *Cost killing:* hace referencia a la práctica que tiene como objetivo la optimización de los gastos en las empresas. Ver *Anexo 1: Entrevistas* para mayor detalle.

[19] "La inversión en ciberseguridad debe ser una parte clave del ciclo presupuestario de la empresa" (traducción propia)

lealtad brindada por sus clientes, al mismo tiempo que se reducen los riesgos derivados de la utilización de tecnologías informáticas.

2.1 Medidas orientadas a la ciberseguridad

Una de las principales concepciones que el presente trabajo pretende asentar es que ciberseguridad no es una función tecnológica de control, sino que es un proceso que se encuentra integrado a las operaciones del negocio. A partir de ello, el primer paso para la conformación de un ámbito organizacional ciber-seguro es reconocer el hecho de que si hay datos e información contenida en sistemas informáticos, existen riesgos asociados a ello. Luego, se debe analizar cuáles son los activos digitales más valiosos para la organización, para así poder considerar el daño que un incidente informático podría generar. En el caso de las empresas de *retail*, además de la información corporativa, los datos de los consumidores (detalle de tarjetas de crédito y débito, patrones de consumo, etc.) son considerados el activo más crítico. De esta manera, se podrán evaluar los riesgos que afectan a dicho recurso clave y, en este momento, tendrá sentido realizar un análisis de las medidas de ciberseguridad a implementar para mantener estas amenazas al margen de la organización, incluyendo a los empleados en estas actividades. El proceso continuo de proteger la información que se almacena, procesa y transmite en los sistemas representa una tarea desafiante y compleja que demanda tiempo, recursos y conocimiento especializado. En este sentido, la evaluación de las medidas a tomar, con el objetivo de salvaguardar los activos corporativos digitales, al mismo tiempo que se busca optimizar al máximo los recursos empleados, adquiere una gran relevancia. Más aún en el caso de las PyMEs donde el presupuesto se encuentra muy limitado. Uno de los aspectos a considerar al evaluar la introducción o mejora de mecanismos de ciberseguridad es la jerarquización de la información en función de su importancia para la empresa. Antes de comenzar a implementar medidas y políticas, la organización debe clasificar su información. En este sentido, la robustez de los controles será mayor cuanto más crítica y estratégica resulte la información en cuestión. Así, se logrará una eficiente distribución de los recursos y el tiempo atribuido a tales tareas de ciberseguridad.

Muchas veces, para ahorrar tiempos de investigación de las soluciones ofrecidas en el mercado, las organizaciones se deciden por aquellas que tienen mayor popularidad y ratio de uso y, generalmente, suelen tratarse de las medidas más costosas de adquirir, implementar y mantener. De este modo, el software de código abierto (*Open Source Software*) surge como una buena alternativa para aquellas empresas que cuentan con limitados recursos para gestionar la ciberseguridad. Por lo tanto, al momento de realizar un análisis previo a la incorporación de soluciones de seguridad informática efectivas y accesibles, no se deben descartar aquellas que son gratuitas (o parcialmente) y, que pueden llegar a ser más adecuadas a las necesidades de la compañía. La realidad indica que no existe en el mercado un único producto que ofrezca todas las funciones necesarias en pos de brindar un nivel de seguridad informática necesario. De este modo, el estudio de las medidas a establecer debe tener en cuenta la complementariedad de los productos o soluciones a adquirir. Por un lado, desde el punto de vista de soluciones de *hardware* y *software*, el Plan de Esquemas Cibernéticos del Gobierno del Reino Unido (*UK Government's Cyber Essentials Scheme*) recomienda la aplicación de los siguientes cinco tipos de medidas de ciberseguridad en el entorno de las pequeñas y medianas empresas:

1) *Firewalls* e internet *gateways*: estas herramientas representan las primeras defensas para prevenir el ingreso de terceros a través de la red de internet. El *firewall* puede detener ataques e incidentes cibernéticos antes de que se encuentren en lo profundo de la red corporativa. Por el En tanto, el internet *gateway* ayuda a prevenir el acceso de los usuarios internos de la organización a sitios web que no son confiables.
2) Configuraciones básicas de seguridad y copias de seguridad: eliminar *software* y servicios que no sean utilizados para reducir la cantidad de vulnerabilidades innecesarias. Asimismo, se deben configurar todos los elementos de *hardware* y *software* con los que cuenta la organización.

   Las copias de seguridad —en cintas de *back-up*, CD´s o DVD´s, discos externos, unidades de almacenamiento USB, etc.— representan uno de los principales mecanismos de seguridad informática y, su eficiente gestión es capaz de evitar el derrumbe de la organización tras un

ciberincidente o, incluso luego de un desastre (incendio, inundación, cortes de electricidad). Por ello, se debe delinear una estrategia de *back-up* de la información crítica del negocio.

3) Controles de acceso: consiste en la restricción del acceso a los sistemas e información a los usuarios de la organización. Cada usuario debe utilizar su propia cuenta que disponga de una contraseña segura. En este punto, es importante resaltar que los controles de acceso deben ser los suficientemente restrictivos para delimitar el uso deliberado de la información disponible, al mismo tiempo que deben garantizar los permisos necesarios para que cada usuario pueda desempeñar sus tareas sin problemas.
4) Protección de *malware*: es importante que la empresa cuente con antivirus y *antimalware* que escaneen regularmente la red para detectar y eliminar posibles amenazas. Además, es fundamental que estos programas se encuentren actualizados en todo momento, dirigidos al monitoreo de los recursos deseados y que emitan reportes o alertas tempranas al detectar una actividad inusual para prevenir grandes daños.
5) Administración de parches y actualización de *software*: el mantenimiento y actualización de los equipos y el *software* es una tarea elemental para asegurar su correcto funcionamiento.

Por el otro lado, a pesar de las sofisticadas soluciones basadas en tecnología de inteligencia artificial y predictiva en el campo de la ciberseguridad, el principal elemento para proveer seguridad informática en una organización son los empleados. Asimismo, existe la práctica conocida como *hacking* ético, mediante la cual las empresas contratan a *hackers* para poner a prueba sus propias defensas informáticas y, perpetrar los sistemas y redes en busca de vulnerabilidades. Sin embargo, por más *firewalls*, sistemas de detección de intrusos, contraseñas seguras, antivirus y medidas de última tecnología que se implementen en la empresa, el empleado es en definitiva quien gestiona, modifica, elimina, transmite y procesa los datos e información. La capacitación en materia de ciberseguridad es fundamental para la construcción de una cultura de seguridad en el ámbito corporativo. Más aún, el consultor experto en

ciberseguridad —Nicolás Ramos— sostiene que las personas que trabajan en las compañías son el pilar fundamental de la seguridad informática, mucho más importante que los procesos que pudieran existir en dicha materia y que las soluciones tecnológicas[20]. Por ello, la formación de los empleados debería anteceder la implementación de medidas de carácter técnico como las mencionadas anteriormente. La concientización de los usuarios debería ser la base que apalanque la implementación efectiva de estas medidas. En definitiva, los empleados deben conocer sus responsabilidades y ser conscientes de los riesgos asociados a la utilización de tecnologías informáticas, pues son quienes administran y utilizan los activos digitales críticos de la empresa.

En la actualidad es muy habitual la utilización de servicios de almacenamiento en la nube (o *cloud*). La nube ofrece acceso a información, procesamiento y almacenamiento a través de la red o un proveedor de servicios externo. Esta tecnología permite a las empresas comprar espacio de almacenamiento en la nube como un servicio, en lugar de realizar grandes inversiones en servidores y personal de soporte interno. La flexibilidad y escalabilidad que ofrece el *cloud*, lo hace compatible con las necesidades de las PyMEs. Además, optar por esta alternativa significaría un menor costo en comparación con el almacenamiento en servidores internos de la compañía, lo cual implicaría invertir en una sala especialmente preparada (con controles de acceso, cámaras de seguridad, control de temperatura y humedad, sistema de prevención de incendios, etc.) y personal para gestionar el almacenamiento dentro de la infraestructura de la organización.

Por último, la subcontratación en la gestión de funciones de seguridad informática, afirma Ramos, es una gran decisión en aquellas PyMEs donde dicha actividad no representa el *core* del negocio. De esta manera, estas compañías podrán ahorrar valiosos recursos (menores costos de sueldos de personal dedicado a esas actividades, menores costos de mantenimiento y soporte, etc.), al mismo tiempo que se contará con el respaldo de los servicios y soluciones de proveedores especializados en ciberseguridad.

[20] Entrevista personal. *Ver Anexo 1: Entrevistas* para mayor detalle.

Soluciones tecnológicas del mercado

A continuación, a modo de recomendación de los productos de seguridad informática ofrecidos en el mercado, orientados al sector de las pequeñas y medianas empresas, se describen algunos *software* que podrían generar un impacto positivo en el ámbito de seguridad corporativo.

En este sentido, el paquete de antivirus que ofrece la compañía rusa KasperskyLab, denominado "*Small Office Security*", está enfocado en compañías que operan hasta 45 dispositivos y consiste en un sistema de gestión y monitoreo basado en la tecnología de la nube. Es una herramienta sencilla de utilizar, orientada especialmente a aquellas organizaciones con mínima (o, incluso, sin ninguna) experiencia en el ámbito de la seguridad informática. Si bien, como hemos mencionado anteriormente, en el mercado existe una gran multiplicidad de productos, esta solución de Kaspersky brinda una relación precio-prestación muy competitiva. El programa incluye herramientas *anti-malware*, *anti-phishing*, administrador de contraseñas seguras y copias de seguridad, controles web y cifrado de archivos.

En relación a la administración de las contraseñas de los usuarios, el *software "Password Manager Pro"*, comercializado por la empresa nacional de servicios de seguridad informática ZMA, es una herramienta de gestión de las contraseñas. Entre las prestaciones que ofrece, se destacan: el almacenamiento y gestión de todas las contraseñas utilizadas en un repositorio centralizado, el control de acceso a los recursos informáticos basado en roles y responsabilidades de puesto y, el reinicio automático de las contraseñas de acceso a los servidores, bases de datos, dispositivos de red. Para el monitoreo del uso de los recursos informáticos *"Wfilter Enterprise"* controla y archiva las actividades de internet (listado de páginas web visitadas, contenido de los correos electrónicos, transferencia de archivos vía web). Además, cuenta con una herramienta para filtrar el contenido de internet y restringir el acceso a determinados sitios.

El producto *"DESlock+"*, de la compañía de seguridad informática Eset, consiste en un conjunto de herramientas de encriptación de discos rígidos, medios extraíbles, archivos y correos electrónicos, a través de algoritmos impenetrables con el objetivo de proteger la información de la empresa.

Por último, agregamos una solución de ciberseguridad más sofisticada para el ámbito PyME que ofrece el análisis inteligente del tráfico de la red. *"Greycortex"* utiliza métodos de inteligencia artificial, aprendizaje automático (más conocido como *machine learning* en inglés) y *data mining* para la detección oportuna de amenazas y respuesta inmediata a incidentes informáticos.

Capacitación del personal

En este apartado se retoma el rol clave que posee la formación de los empleados en ciberseguridad en las PyMEs de la industria de *retail*, y en las empresas en general.

El acceso de los empleados a la información que administran las compañías es una necesidad para el desarrollo del negocio y esto introduce riesgos derivados, tanto de la falta de conocimiento e información, como de actitudes maliciosas con intención de generar un daño. Sin embargo, las restricciones y controles excesivos tienen consecuencias contraproducentes: se ralentizan los procesos de negocio con pérdida de productividad, se producen quejas en los usuarios por las dificultades para realizar sus actividades cotidianas, entre otras. En este sentido, resaltamos la importancia de trabajar en la concientización de los empleados en materia de ciberseguridad para reducir las amenazas internas carentes de intencionalidad, es decir, para minimizar la ocurrencia de incidentes informáticas internos (según la clasificación de ciberincidentes realizada anteriormente). En consecuencia, los riesgos restantes serán procedentes de usuarios internos y agentes externos a la firma con intención de generar algún tipo de perjuicio en la compañía. En otras palabras, la paliación de las amenazas de ataques informáticos contará con personal debidamente capacitado en seguridad informática, medida a la cual se podrán sumar soluciones tecnológicas (antivirus, *firewalls*, entre otras mencionadas más arriba).

Si bien, en general, los ataques informáticos externos son los que mayor repercusión generan (por ejemplo, el famoso "WannaCry"), cabe resaltar que, en la mayoría de los casos, los problemas relacionados con temas de ciberseguridad se deben a deficiencias en procesos internos y al comportamiento de las personas que trabajan dentro de las organizaciones. Tal es así que un estudio de IBM refleja que aproximadamente el 60% de los

ciberincidentes relacionados a la violación de datos, son causados por los propios empleados de la organización (Fernández, 2018). Los empleados sin formación no solo aumentan las posibilidades de materialización de incidentes informáticos internos, sino representan una oportunidad que para los ciberatacantes que se aprovechan de esta la falta de conocimiento para perpetuar un ataque en la empresa. Tal es así que los ciberincidentes más habituales en el ámbito de las PyMEs tienen al personal como causa raíz:

- Infecciones por *malware* oculto en sitios web;
- Ejecución de programas o archivos con contenido malicioso;
- Descarga de documentos adjuntos al correo electrónico con virus;
- Conexión de terminales USB desconocidas sin revisión previa a los equipos;
- Acceso a recursos por contraseñas débiles;
- *Phishing*[21]: de hecho, según un estudio de la empresa de seguridad informática KasperskyLab, Argentina ocupa el séptimo lugar en la lista de los países que son afectados por esta técnica de engaño en todo el mundo (González Pérez, 2017).

Estas son algunas de las modalidades que se aprovechan del desconocimiento de los empleados en el campo de la seguridad informática. Como se pudo observar, los incidentes informáticos más desafiantes son aquellos que se aprovechan de las vulnerabilidades humanas en lugar de las tecnológicas (como la desactualización de un programa, por ejemplo). Por tal motivo, es de especial relevancia subrayar la importancia de invertir en la capacitación y entrenamiento en ciberseguridad para todos sus empleados —no solo al staff de seguridad informática—. En este sentido, la capacitación generalmente, indica Nicolás Ramos, no se trata de un mecanismo muy costoso[22]. Puede ser abordada a través de múltiples canales: jornadas de concientización para toda la compañía, reuniones informales de debate, charlas sobre temas específicos de seguridad informática (utilización de contraseñas seguras, verificación de los archivos adjuntos recibidos por mail antes de proceder a su descarga, etc.), entre otros mecanismos.

[21] Ver *Anexo 3: Ejemplo de Phishing*.

[22] Entrevista personal. Ver *Anexo 1: Entrevistas* para mayor detalle

Para concluir, la ciberseguridad no es un producto, es un proceso continuo que requiere de la interacción coherente y constante entre los componentes humanos y la infraestructura tecnológica para proteger los activos digitales de la empresa. Por ello, resulta fundamental involucrar a los empleados para enfrentar las distintas amenazas del mundo cibernético y, para ello, es necesario que reciban la formación adecuada y conozcan sus responsabilidades en este contexto.

Auditoría en seguridad informática

La auditoría en seguridad informática tiene como principal objetivo evaluar el nivel de protección del activo corporativo más importante: la información digital. De esta manera, se llevan a cabo pruebas para determinar si los mecanismos de ciberseguridad implementados en la compañía son eficientes en el resguardo de la disponibilidad, confidencialidad e integridad de este activo fundamental. Asimismo, este proceso puede ser realizado para controlar el cumplimiento de las leyes y regulaciones a las que la empresa se encuentra sujeta. La auditoría en ciberseguridad puede ser desarrollada de manera interna, por la misma compañía, o puede ser llevada a cabo por un auditor externo. En este último caso, el o los profesionales pueden ayudar a visualizar problemas relacionados a la gestión de la ciberseguridad que desde adentro no logran identificarse. Además, la auditoría es empleada para analizar si las medidas de seguridad informática se encuentran alineadas al cumplimiento de los objetivos organizacionales, si existe un eficiente empleo de los recursos y, si corresponde, recomendar maneras de optimizar dicha situación.

En cuanto a las empresas que se encuentran obligadas a la presentación de estados financieros auditados por un agente externo, este trabajo puede incluir la auditoría de la seguridad informática, cuando el profesional a cargo lo considere necesario. En este caso, el *Executive Director* en Ciberseguridad de EY señala que los procedimientos de ciberseguridad efectuados por el auditor externo se basan en chequeos técnicos que permitan reunir pruebas válidas y suficientes, con el propósito de brindar un nivel de seguridad razonable para la auditoría principal de los estados financieros[23]. De esta manera, los controles realizados consisten en verificar la configuración segura y actualización de los

[23] Entrevista personal. *Ver Anexo 1: Entrevistas para mayor detalle.*

programas, la seguridad de archivos, la efectividad de las políticas de *back-up*, los límites de acceso a los recursos digitales, entre otros. En definitiva, el auditor busca efectuar las revisiones necesarias sobre los mecanismos de seguridad informática implementados en la organización para poder confiar en la información que se almacena, modifica y circula en los sistemas informáticos. Finalmente, cabe agregar que las auditorías externas en seguridad informática pueden ser realizadas por consultoras (tales como EY y PwC, por ejemplo) o profesionales especialistas en el tema. En este sentido, la certificación CISA (*Certified Information Systems Auditor*) que ofrece ISACA para auditores profesionales, respalda el trabajo realizado por el auditor externo, ya que se trata de una de las certificaciones más reconocidas y avaladas a nivel internacional. Desde su lanzamiento en 1978, más de 130.000 profesionales han conseguido esta prestigiosa certificación (*Information Systems Audit and Control Association*, s.f.).

En síntesis, de acuerdo con ISACA, "el objetivo de una auditoría de ciberseguridad es proveer a la gerencia una evaluación de la efectividad de los procesos de ciberseguridad, de las políticas, procedimientos, gobernanza y otros controles" (Fortino, 2017). Asimismo, añade que la auditoría se encuentra diseñada sobre las funciones críticas de ciberseguridad presentadas por el *Cybersecurity Framework*, abordadas en la presente investigación: identificar, proteger, detectar, responder y recuperar.

Seguros informáticos

La industria de seguros ha visto en la ciberseguridad una ventana para expandir sus negocios, a partir del constante incremento de brechas de seguridad informática en las organizaciones. El servicio de seguros contra ciberincidentes (o ciberseguros) aún se encuentra en una etapa inicial de madurez, pero dadas las condiciones del mercado crecerá en los próximos años. En Argentina, aún no se encuentra reglamentada esta actividad, pero la Superintendencia de Seguros de la Nación se encuentra trabajando en ello para que las compañías aseguradoras comiencen a ofrecer seguros contra ciberincidentes.

Las organizaciones que desarrollan sus procesos de negocio apoyándose en tecnologías y sistemas informáticos, en donde los datos e información

desempeñan un rol fundamental, deberían considerar proteger su negocio con un ciberseguro que se adapte a sus propias vulnerabilidades y riesgos. En este sentido, en los mercados donde este mecanismo se encuentra desarrollado, como sucede en Chile, los distintos seguros ofrecen cobertura por: pérdida, daño o distorsión de datos, soporte técnico para restaurar los activos informáticos dañados, pago de multas, entre otros. Estos seguros ofrecen un gran valor a las compañías que buscan protegerse de los daños y costos de los ciberincidentes. Sin embargo, es probable que la adquisición de un ciberseguro en el ámbito de las pequeñas y medianas empresas no sea viable, a priori, en términos del costo-beneficio. En otras palabras, en la etapa inicial en la que se encuentra el mercado de seguros contra incidentes cibernéticos en el país genera que los costos de su adquisición sean muy elevados de asumir en una PyME que se encuentra en una etapa de aprendizaje y concientización en el ámbito de la ciberseguridad.

2.2 Ciberseguridad en el *e-commerce*

El *e-commerce* o comercio electrónico es definido por Laudon & Laudon (2012) como el empleo de la tecnología de internet para el desarrollo de transacciones de negocio. Esta modalidad de comercio a través de la web comenzó en 1995 y, desde entonces, ha experimentado un crecimiento exponencial, tal como se puede observar en el siguiente gráfico:

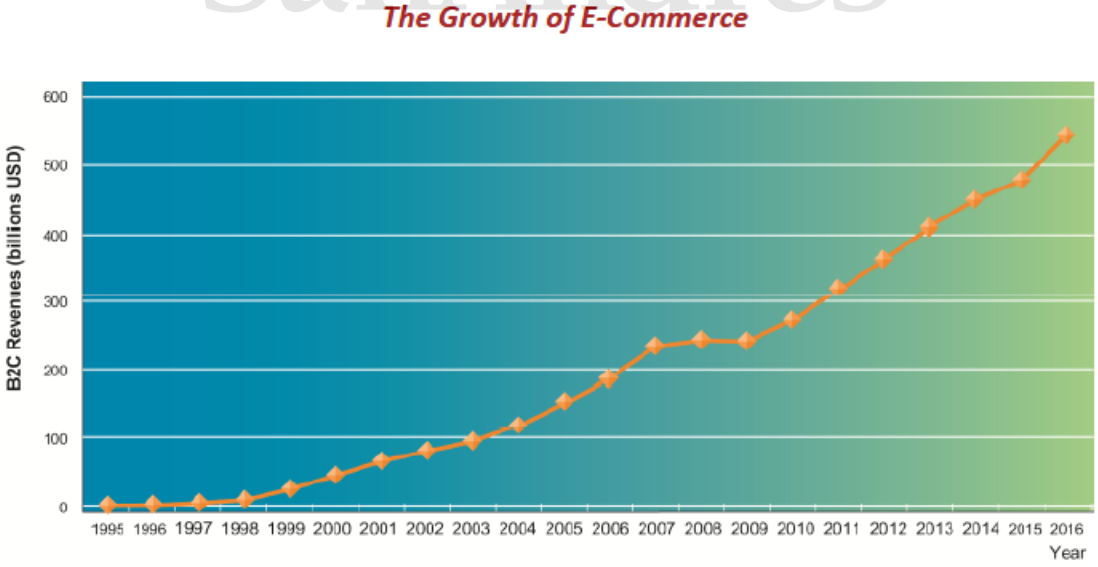


Figure 10-1 Retail e-commerce revenues grew 15–25 percent per year until the recession of 2008–2009, when they slowed measurably. In 2012, e-commerce revenues are growing again at an estimated 15 percent annually.

Fuente: Clase Sistemas de Información (Módulo V – Continuación. E-commerce, E-business, Balanced Score Card), Prof. Gabriel Aramouni. Universidad de San Andrés, 10 de mayo de 2017, Victoria).

El comercio electrónico en Argentina, según las estadísticas de la Cámara Argentina de Comercio Electrónico (CACE), ha facturado 156.300 millones de pesos en el 2017. Ello significó un crecimiento del 52% de la facturación respecto del año anterior. Además, mientras que en los países desarrollados el *e-commerce* representa más del 5% de las ventas minoristas totales, en Argentina esta cifra alcanzó el 2% en 2017.

El *e-commerce* le ha brindado a las compañías tradicionales la posibilidad de extender el alcance de sus negocios y, a las pequeñas compañías y emprendimientos, la oportunidad de crecer a partir del empleo de esta herramienta, aprovechando las infraestructuras tecnológicas creadas por gigantes como Google y Amazon, y los beneficios provistos por los servicios en la nube. Los autores mencionados anteriormente, redefinen el concepto de las empresas de *retail* que vuelcan parte de sus negocios al *e-commerce*, denominándolos “e-tailer´s”, señalando que la propuesta de valor se basa en ofrecer conveniencia, bajos costos de envío y amplios stock para el consumidor quien puede realizar sus compras en cualquier momento. No obstante, a pesar de los múltiples beneficios que tiene tanto para las empresas, como para los consumidores, es importante remarcar la relevancia que adquiere la ciberseguridad en este contexto. Las vulnerabilidades en el *retail online* se multiplican y, en consecuencia, la cantidad de incidentes y ataques informáticos se multiplican. Por lo tanto, lo mismo debería suceder con los mecanismos y controles a emplear para reducir la probabilidad de su materialización, ya que una brecha de seguridad que afecte los datos personales de los clientes puede causar graves daños en la compañía.

Las compañías deben contar con las medidas necesarias que permitan garantizar la protección de la información provista por los clientes en sus sitios web de *e-commerce*. Además, de las soluciones desarrolladas en la sección anterior, a continuación se enuncian algunos mecanismos específicamente empleados para generar confianza en el mercado:

- Utilización de protocolos de seguridad para la autenticación web y la protección de los datos mediante la encriptación, como por ejemplo, el certificado SSL (*Secure Sockets Layer*);
- Mantener una cantidad mínima y suficiente de datos de terceros almacenados, con copia de seguridad;
- Exigir contraseñas seguras a los clientes.

En resumen, a pesar de que el tema tratado en este apartado no constituye el principal objeto de estudio de la presente investigación, se acentuó la importancia de abordar los aspectos relacionados a la ciberseguridad en el *e-commerce* en la industria del *retail*, con el objetivo de proteger la confidencialidad de los datos provistos por los clientes e impulsar el crecimiento de la compañía a través del canal de ventas digital.

CAPÍTULO 3: BENCHMARKING

El objetivo del siguiente capítulo es proveer a los lectores de la presente investigación un documento con un valor, para que puedan abordar la ciberseguridad provistos de más herramientas e información. En este sentido, se empleará la técnica de *benchmarking*[24], con el propósito de desarrollar la situación de la seguridad informática en las pequeñas y medianas empresas en los siguientes países: Estados Unidos, por su avance en la materia y Chile, por su más similar realidad a la de nuestro país.

1. Estados Unidos

"[*P*]*rotecting our digital infrastructure is a national security priority and a national economic priority",* declaró el expresidente Barack Obama en una conferencia en 2015, haciendo énfasis en la trascendencia del tratamiento de la ciberseguridad a nivel nacional. Los Estados Unidos encabezan la lista de las naciones más comprometidas en la construcción de una cultura de concientización en el ámbito de la seguridad cibernética. Tal es así que, al igual que en Europa, en octubre se celebra el mes nacional de la conciencia sobre la ciberseguridad con el fin de promover la importancia de dicho aspecto. La legislación estadounidense en materia de ciberseguridad es abordada con la relevancia que amerita. Las leyes nacionales, por un lado, obligan a las organizaciones (más allá de su tamaño e industria en la que participan) a denunciar frente a las autoridades competentes cuando se produce un ciberincidente que tiene como consecuencia el robo, la pérdida, alteración o manipulación de datos e información y, a informar a los afectados por dicho suceso. Por otro lado, el marco legal impulsa el intercambio de información entre el sector privado y el gobierno, ofreciendo una serie de beneficios exclusivos para aquellas organizaciones que voluntariamente contribuyan en ello. Del mismo modo, la educación en seguridad informática en Estados Unidos cuenta con el respaldo y financiamiento federal, con el objetivo de formar profesionales en seguridad cibernética, capaces de poner en práctica

[24] *Benchmarking*: mecanismo utilizado para presentar las mejores prácticas y mejores desempeños para actividades similares, dentro o fuera de la industria de la organización objetivo.

sus conocimientos frente a las amenazas de incidentes informáticos. Prestigiosas universidades, tales como UC Berkeley School of Information y George Washington University, ofrecen la posibilidad de formación en el campo de la ciberseguridad.

Las *Small and Medium-Sized Business/Enterprises* —SME o SMB— (hasta 499 empleados) representan más del 99% de las empresas norteamericanas y, tal como sucede en Argentina, son el eslabón central de la economía nacional, generando el 48% del empleo privado en el país (*Office of the United States Trade Representative, Small Business*, s.f.). Además, las pequeñas y medianas empresas poseen un rol único en el ecosistema empresarial, pues muchas veces pueden ser utilizadas como puerta de acceso a las grandes empresas que se encuentran interconectadas. En el ámbito de la ciberseguridad, estas compañías se encuentran expuestas a los riesgos derivados de la implementación de tecnologías informáticas y la gestión de información crítica para el negocio. No obstante, en línea con lo mencionado en el párrafo anterior acerca del nivel de importancia asignado a la seguridad cibernética en los Estados Unidos, cada vez más organismos y entidades reguladoras de la actividad comercial exigen la alineación de las empresas a los estándares y normativas de mayor aceptación en materia de ciberseguridad. En este sentido, distintos marcos de referencia como el *Cybersecurity Framework* y la norma ISO 27001, son adoptados por todo tipo de organizaciones para desarrollar o mejorar sus ambientes corporativos de ciberseguridad. De esta manera, se observan dos tendencias en el ámbito de las pequeñas y medianas empresas. En primer lugar, se encuentran aquellas organizaciones que perciben el cumplimiento de estos requerimientos como medida necesaria para ser competitivas en un mercado con grandes jugadores como lo es el de Estados Unidos. En segunda instancia, observamos a las empresas que, desde una perspectiva estratégica, buscan adoptar un marco de referencia como guía para gestionar los riesgos y reducir las vulnerabilidades en materia de ciberseguridad y, en consecuencia, impulsar el crecimiento corporativo.

En este contexto, un reporte de Better Business Bureau[25] indica que el 90% de las SME´s estadounidenses emplean algún tipo de medida de ciberseguridad de manera proactiva (S*tate of Cybersecurity among Small Business in North America*, 2017). La implementación de antivirus, *firewall* y la capacitación de los empleados son señaladas como las medidas más utilizadas con el objetivo de proteger los activos informáticos en los que se apoya el negocio. Asimismo, en el mercado existe una tendencia creciente a contratar seguros para transferir los costos derivados de incidentes cibernéticos a las compañías aseguradoras. Ello demuestra el aumento de la consciencia respecto de las amenazas cibernéticas y el compromiso por proveer seguridad a sus recursos informáticos. Por último, el informe destaca que los principales desafíos que se presentan en las pequeñas y medianas empresas son la falta de recursos y de conocimiento sobre el tema.

En conclusión, las pequeñas y medianas empresas (SME´s) de lo Estados Unidos, al igual que el resto de las organizaciones del mundo, se enfrentan diariamente con nuevos y más desafiantes amenazas en el plano cibernético que amenazan sus negocios. No obstante, el tratamiento institucional de la ciberseguridad provee un escenario mejor preparado, con más herramientas pero, también con mayores obligaciones, para el desarrollo de las pequeñas y medianas empresas en dicho país.

2. Chile

En Chile, el sector privado no está obligado por ley a denunciar e informar los incidentes informáticos, pero el Estado trabaja en conjunto con las empresas para crear una cultura de concientización en torno a la ciberseguridad. A pesar de que Chile se encuentra adherido al Convenio sobre la Ciberdelincuencia del Consejo de Europa, en materia de legislación en ciberseguridad está decididamente retrasado, ya que la ley que tipifica y sanciona las acciones en el ámbito cibernético fue creada en 1993 y, no ha sido actualizada desde entonces. En este sentido, el país trasandino cuenta, desde 2017, con una

[25] *Better Business Bureau*: es una organización sin fines de lucro enfocada en el avance de la confianza del mercado a partir del tratamiento de distintos aspectos, como bien lo es la ciberseguridad.

Política Nacional de Ciberseguridad. Entre los principales objetivos con impacto en el ámbito empresarial, se destaca la creación de un modelo de divulgación obligatorio de incidentes y, el abordaje de las certificaciones en seguridad informática como un mecanismo para establecer niveles de confianza en el mercado. En cuanto a la educación y formación de profesionales en el área de ciberseguridad, la Universidad de Chile ofrece títulos avanzados en seguridad cibernética y también están disponibles diversos cursos en línea y capacitación para empleados. Asimismo, la Universidad Tecnológica de Chile es pionera en la región latinoamericana en dictar la carrera de Ingeniería en Ciberseguridad (Rivas, 2018).

De acuerdo a un estudio realizado por *The Boston Consulting Group* (BCG) Chile, en 2017 las compañías chilenas invirtieron un 4% más en seguridad informática respecto del año anterior (Núñez, 2018). Además, la consultora señala que la industria bancaria y el *retail* fueron quienes más invirtieron en ese período. No obstante, la cantidad no asegura la calidad y efectividad de las medidas implementadas. Las pequeñas y medianas empresas se encuentran en una etapa de madurez en el campo de la ciberseguridad. Están comenzando a tomar medidas con el objetivo de lograr condiciones de protección de los datos e información que resulta críticos para sus negocios. En este sentido, consideran fundamental el papel que desempeñan los empleados en el desarrollo de ambientes de trabajo seguros. El Club CISO Chile es una iniciativa del sector privado, creada como un canal de comunicación e intercambio de experiencias, mejores prácticas.

Con el objetivo de dar a conocer la magnitud de las consecuencias que un ciberincidente puede causar en los negocios, se describe el ataque informático que padeció el Banco de Chile en mayo de 2018 (Duna, 2018). A través de una carta firmada por el CEO, enviada por correo electrónico, la entidad bancaria explicó a sus clientes el ciberataque por el que perdió 10 millones de dólares. En este comunicado, el banco asegura que el dinero robado pertenecía al patrimonio de la firma y no afectó a los fondos de los clientes, ni tampoco se vieron perjudicados los datos, registros y transacciones de estos últimos. La notificación de la brecha de seguridad informática sufrida por el Banco de Chile fue realizada 19 días después del ataque. A partir de lo sucedido, las

autoridades manifestaron que comenzarán a exigir que los bancos informen los incidentes de manera inmediata. Asimismo, se definieron dos ejes de acción (Harán, 2018): 1) solicitar asesoramiento a un organismo internacional para identificar aspectos a mejorar y, 2) revisar el marco regulatorio en materia de ciberseguridad. De esta manera, se puede observar el carácter reactivo de las medias alineadas al desarrollo de un ámbito de ciberseguridad corporativo.

CAPÍTULO 4: ANÁLISIS DE CIBERSEGURIDAD EN ZONA VITAL Y FARMABELÉN

En este capítulo se realiza, en primera instancia, la descripción de la relevancia otorgada al tratamiento de la ciberseguridad en los casos de estudio seleccionados (Zona Vital y FarmaBelén), a la luz de los objetivos y las variables planteadas en la presente investigación. Luego, se lleva a cabo un análisis que compara los aspectos surgidos en el punto anterior. Finalmente, se efectúan algunas conclusiones para finalizar el apartado.

1. Zona Vital

Zona Vital (fundada en 1964) cuenta con más de 50 años de experiencia en el mercado farmacéutico. Es una organización de profesionales farmacéuticos con capital 100% nacional que se define como un centro de salud y belleza, con una clara visión de brindar un servicio de excelencia a la comunidad. Se trata de una de las cadenas de farmacias líderes en Zona Norte del conurbano bonaerense y, sus principales competidores son Selma y Simplicity. Según lo señala el sitio web de la compañía, más de cinco millones de clientes visitan anualmente los catorce locales —dos de ellos con atención 24hs— de la firma con presencia en Capital Federal, Gran Buenos Aires, Luján y Bariloche. Cuenta con una amplia oferta de medicamentos, productos para la salud, fragancias y cosmética. Los amplios, confortables y modernos locales, situados estratégicamente, con estacionamientos privados y dotados de profesionales de excelencia, son algunos de los rasgos distintivos de Zona Vital reflejados en su página web.

Desde el punto de vista estructural, la empresa se encuentra dividida en dos segmentos: farmacia y, perfumería y cosmética. Según la gerente comercial y de operaciones de Zona Vital[26], las ventas de la división farmacia representan el 80% del total de las ventas de la firma, mientras que el restante 20% corresponde a las ventas del canal de perfumería y cosmética. En tal sentido, el segmento de perfumería y cosmética genera un mayor margen de

[26] Entrevista personal. *Ver Anexo 1: Entrevistas* para mayor detalle.

rentabilidad que la farmacia. No obstante, la inmovilización del stock y los cortos plazos de pago generan grandes costos financieros. En cuanto al sector de farmacia, si bien el margen resulta inferior, la rotación de los medicamentos se produce dentro del plazo de pago a los proveedores, disminuyendo las erogaciones de carácter financiero. Además, la entrevistada señaló que el margen generado por la división de farmacias puede ser optimizado al negociar y comprar los medicamentos directamente a los laboratorios, sin tener que asumir los costos de intermediación (de las droguerías, por ejemplo). En definitiva, como en todo negocio de *retail*, el volumen es lo que define el desempeño de la empresa. Por tal motivo, la reducción de las unidades vendidas en el 2017 ha generado una gran preocupación en el sector. De acuerdo con lo manifestado por la entrevistada, los principales desafíos de la empresa se encuentran alineados a las problemáticas financieras del mercado farmacéutico, planteadas anteriormente (4.5 Justificación del *retail* farmacéutico): cómo hacer para que el negocio continúe siendo rentable en un contexto de creciente inflación, en un mercado donde la venta de medicamentos está regulada por ley con un porcentaje máximo de aumento anual. Asimismo, se incorpora el desafío impuesto por el Convenio PAMI con la reducción del 5% del precio de los medicamentos cubiertos por dicho organismo.

La innovación ha sido un rasgo distintivo de Zona Vital desde sus orígenes, brindando tecnología de vanguardia a los clientes e incorporando de manera constante una amplia variedad de servicios de calidad (Centro de Dermocosmética Personalizado, jornadas gratuitas de concientización sobre la salud y eventos de interés social, Consejo Farmacéutico, entre otros señalados en el sitio web de la compañía), permitiendo posicionar a la marca en la mente del consumidor. Además, en términos de la gerente comercial y de operaciones, la organización es pionera —dentro del rubro farmacéutico— en el desarrollo e implementación de un programa de fidelización del cliente: la "Tarjeta Zona Vital" otorga beneficios, descuentos y premios a los clientes, a través de la acumulación de puntos obtenidos por las compras que realizan. El diseño de este programa se basa en las experiencias previas en sistemas de fidelización del cliente desarrollados por la firma ("Club de Puntos Zona Vital",

“Pesos Zona Vital”). Dicho programa fue creado en base a dos objetivos principales: 1) ampliar la base de clientes y retener a los actuales, fortaleciendo la lealtad a la marca; y 2) obtener información valiosa para estudiar el comportamiento de los clientes (cada cuanto, qué, cuándo compra). Actualmente, la entrevistada sostiene que el proyecto “Tarjeta Zona Vital” se encuentra consolidado, con un buen nivel de recepción por parte de los consumidores, pero se están destinando esfuerzos en el análisis de los datos obtenidos para mejorar la experiencia del cliente.

El papel de la ciberseguridad, en este contexto, podría ser considerado como un elemento clave para el resguardo de los datos e información —no solo de los clientes, sino también la información corporativa contenida en los sistemas—, cada vez con mayor relevancia para el crecimiento de la compañía. Asimismo, el cumplimiento de la Ley de Protección de Datos Personales debería ser motivo suficiente para la implementación de medidas de seguridad informática, tendientes a proteger los datos administrados de los clientes. Sin embargo, tal como afirma la entrevistada, la ciberseguridad no es un tema del que se habla en el entorno organizacional. A continuación, se lleva a cabo un análisis del ámbito de la seguridad informática, en función de los ejes de análisis establecidos en la presente investigación.

1.1 Dimensiones de la ciberseguridad

En este apartado se describen las dimensiones generales en cuanto al tratamiento de la seguridad informática en Zona Vital. Para ello, se proponen los siguientes ejes temáticos: 1) el conocimiento del significado de la ciberseguridad y de los ciberincidentes, y su incidencia en el ámbito corporativo; 2) el diseño de la ciberseguridad dentro de la estructura organizacional y designación de un presupuesto destinado a dicho sector y; 3) la importancia de los activos de información.

En primer lugar, la gerente comercial y de operaciones, reconoció su desconocimiento respecto de las nociones de ciberseguridad y ciberincidentes dentro del ámbito corporativo, como así también en relación a los riesgos a los que la empresa se encuentra expuesta por la ausencia de medidas orientadas al resguardo de sus activos de información. Asimismo, señaló que Zona Vital

no posee experiencia en el desarrollo de funciones ligadas a la seguridad informática, más allá de las actividades llevadas a cabo por el único empleado encargado de la gestión de los sistemas de la firma. En tal sentido, manifestó que, dentro de la organización, la ciberseguridad no es analizada como un aspecto a tener en cuenta al momento de realizar nuevos desarrollos de negocio o emprender nuevos desafíos. La descripción de esta situación en Zona Vital, la coloca en una posición de alta vulnerabilidad frente a la ocurrencia de incidentes informáticos.

En segunda instancia, la compañía no cuenta con un área de seguridad informática, ni tampoco un empleado responsable en dicho ámbito. Una sola persona es la encargada de llevar adelante las tareas operativas relacionadas al funcionamiento y mantenimiento de los sistemas de gestión empleados, la actualización de los programas y el soporte de los equipos. En este sentido, la entrevistada reconoció la deficiencia del área de sistemas e hizo énfasis en que la dependencia en dicho empleado queda demasiado expuesta y no puede ser permitida en una empresa de la envergadura de Zona Vital. Por lo tanto, declaró la necesidad de replantear el área de sistemas y contratar un empleado de nivel gerencial en dicho sector para encarar futuros proyectos, como el lanzamiento de un canal de venta *online*, por ejemplo. Sin embargo, hizo referencia a que la conformación de un área específica de ciberseguridad es inviable en el contexto actual del negocio. En todo caso, señaló que la gestión de la seguridad informática podría ser desarrollada por el empleado de sistemas. Finalmente, al no haber un área o responsable en materia de ciberseguridad dentro de la compañía, tampoco existe un presupuesto destinado en dicho ámbito.

Por último, la gerente consultada manifestó que los activos de información (datos e información digital) siempre fueron considerados de relativa importancia dentro de la organización, utilizada de manera operativa para el desarrollo del negocio. Sin embargo, destacó que, a partir de la implementación del programa de fidelización, comenzó a ser abordada desde una perspectiva más estratégica, aunque aún no lo suficiente para justificar una inversión en medidas de protección de la información contenida en medios digitales. Además, cree que es poco probable que un incidente informático tenga lugar

en Zona Vital, debido a dos razones: por un lado, el pensamiento acerca de que la información solamente posee valor al interior de la firma y, por el otro, que nunca sufrieron un robo o pérdida de información. Ello pone de manifiesto la falta de concientización respecto de los riesgos asociados a la utilización de tecnologías informáticas y gestión de activos de información que existe en la compañía.

En resumidas palabras, a partir de la entrevista y las observaciones realizadas, es posible señalar que la ciberseguridad no se encuentra abordada en Zona Vital debido a que no es considerada como una actividad clave para el negocio. De esta manera, se están desaprovechando las oportunidades de crecimiento y expansión de la compañía mediante la gestión eficiente de sus activos de información críticos, respaldados por mecanismos de seguridad informática que le provean confidencialidad, integridad y disponibilidad.

1.2 Funciones de la ciberseguridad

En la actualidad, Zona Vital no se encuentra implementando ningún tipo de marco de referencia orientado a la seguridad informática. A pesar de la ausencia de un área o responsable de ciberseguridad y, de actividades formales definidas en dicho ámbito, a continuación se realiza un análisis de la situación de la compañía, a la luz de las funciones orientadas a la seguridad informática (identificar, proteger, detectar, responder y restaurar), planteadas en el marco referencial del presente trabajo.

En primer lugar, en cuanto a la función de **identificación**, Zona Vital cuenta con un inventario de los equipos y dispositivos físicos (tales como, computadoras, impresoras, *routers*, etc.) pero, carece de un registro de los activos digitales que administra. En otras palabras, no conoce la cantidad y diversidad de archivos en distintos formatos, datos e información que utiliza y almacena. Asimismo, no posee normas, políticas, ni ningún tipo de procedimiento formal delineado en cuanto a la gestión de los activos de información. En cuanto al análisis de los riesgos relacionados con la utilización de tecnologías informáticas, lo cual, según el *Risk IT Framework*, constituye una de las primeras medidas a desarrollar para el diseño de una estrategia responsable de ciberseguridad, no se encuentra dentro de las tareas realizadas

por la firma. En tal sentido, las actividades relacionadas al campo de la seguridad informática se encuentran implícita e inconscientemente presentes en el trabajo diario del personal de la farmacia, lo cual genera que, muchas veces, no se lleven a cabo. Por ejemplo, la utilización de contraseñas seguras de acceso a los usuarios es un lineamiento, implementado en Zona Vital, que vela por el resguardo de los recursos digitales. Sin embargo, las contraseñas se encuentran escritas en papeles pegados a las pantallas de las computadoras o en los escritorios para evitar su olvido y, porque permite que un empleado pueda acceder al usuario de otro en caso que se requiera (por ausencia, enfermedad, etc.). La gerente comercial y de operaciones señaló que los accesos cruzados entre usuarios se consideran un buen procedimiento para evitar retrasos en la actividad, dejando de lado los innumerables riesgos a los que se encuentran expuestas a partir de esta conducta. Al mismo tiempo, ello deteriora la buena práctica llevada a cabo en Zona Vital, en cuanto a la limitación del acceso a los recursos informáticos (datos, información, sistemas) disponibles según el nivel jerárquico de la compañía.

En segundo término, la **protección** consiste en que la empresa sea capaz de minimizar el impacto de un potencial ciberincidente. Como se ha mencionado a lo largo del trabajo, los empleados constituyen la primera defensa para lograr ese objetivo y, Zona Vital no cuenta con personal debidamente capacitado en el ámbito de la ciberseguridad. En este sentido, las acciones y el comportamiento de los empleados en torno a la utilización y el cuidado de la información, se encuentran determinados por sus experiencias profesionales. En consecuencia, aquellos mecanismos de seguridad informática implementados en la empresa no cuentan con una base sólida de apoyo, es decir, personal lo suficientemente preparado para optimizar sus prestaciones. No obstante, cabe mencionar que la compañía posee algunos mecanismos (tal como la mencionada restricción al acceso de los recursos informáticos) y herramientas básicas para reducir las consecuencias de un incidente informático, las cuales serán abordadas en el siguiente apartado.

En tercera instancia, en cuanto a la función de **detección** propuesta en el *Cybersecurity Framework*, la cual tiene el principal objetivo de descubrir oportunamente actividades sospechosas y evitar la ocurrencia de incidentes

cibernéticos, Zona Vital se limita a la instalación de un antivirus y su actualización a cargo del empleado de sistemas. Este programa es utilizado de manera pasiva, es decir, simplemente se encuentra instalado en las computadoras de los empleados como si fuese a proveer una defensa absoluta contra las amenazas cibernéticas. De esta manera, se están desaprovechando las distintas prestaciones que ofrece el antivirus, como por ejemplo, en cuanto al monitoreo continuo y reportes de actividades sospechosas.

En cuarto lugar, Zona Vital no posee un plan de **respuestas** para reducir los daños frente a la materialización de ciberincidentes. En tal sentido, la gerente consultada manifestó que si no cuentan con un responsable en el ámbito de la seguridad informática, mucho menos invertirán en diseñar mecanismos para atenuar los efectos negativos de un incidente que no creen probable que ocurra en su entorno. Del mismo modo, el personal entrevistado declaró su desconocimiento respecto de la manera de proceder en caso de ser afectada por un ciberincidente (qué, a quién y cómo denunciar). Asimismo, señaló que la falta de información y participación de las autoridades y organismos en este ámbito, contribuye a profundizar esa problemática.

Por último, los procesos implementados de recuperación y **restauración** de los sistemas y activos informáticos afectados por un incidente informático, para retornar a las condiciones normales de trabajo, se reducen a la realización de copias de seguridad de la información que se considera más crítica para la organización (información de ventas, reportes de gestión y datos de clientes). Los *back-ups* son resguardados en discos externos y dispositivos de almacenamiento USB. El problema observado en esta instancia es que la periodicidad con la que se realizan los *back-ups*, se encuentra a discreción del empleado de sistemas, quien las hace cuando dispone de tiempo suficiente, una vez que ha concluido con sus tareas diarias. Asimismo, otra debilidad del proceso informal de copias de seguridad es que los dispositivos que las contienen se encuentran dentro de Zona Vital; por lo cual, todo lo realizado sería en vano frente a una inundación o un incendio, por ejemplo. Finalmente, es importante señalar el desconocimiento respecto de los seguros contra ciberincidentes que pueden ayudar a la organización a recuperarse frente a estos hechos, sin tener que asumir la totalidad de los costos asociados

(pérdida de datos, destrucción de equipos, etc.). Por lo tanto, su contratación ni siquiera entra en la consideración de las autoridades de la farmacia.

1.3 Instrumentación de la protección de los activos de información

En relación a esta tercera variable planteada para el análisis comparado de los casos de estudio, a continuación se desarrollan, por un lado, los mecanismos generales en torno a la ciberseguridad y, por el otro, la implementación de soluciones específicas de *hardware* y *software* en Zona Vital.

Por un lado, se encuentran aquellas medidas empleadas para la protección de sus datos e información digital de carácter general. En tal sentido, la compañía posee asignados niveles de autorización, según la jerarquía del personal y el tipo de actividad, para limitar el acceso a los recursos disponibles. No obstante, como hemos mencionado anteriormente, esta buena práctica se encuentra cercenada debido a la gestión deficiente en el uso de contraseñas privadas para cada usuario. En cuanto a la actualización del sistema operativo y los programas, fundamental para evitar amenazas que se aprovechen de versiones antiguas, esta es realizada por el empleado de sistemas si ningún tipo de proceso definido. En otras palabras, cuando un usuario detecta (recibe un mensaje de alerta) que algún programa debe ser actualizado, lo notifica al empleado de sistemas para que haga lo que se necesita. Asimismo, desde el punto de vista de la recuperación de los sistemas e información que pudiera ser afectada tras un ciberincidente, la empresa (más bien, el empleado de sistemas) realiza y guarda copias de seguridad en dispositivos de almacenamiento USB. Finalmente, cabe resaltar que Zona Vital no lleva a cabo una de las principales actividades para la conformación de una cultura consciente en el ámbito de la seguridad informática: capacitación de sus empleados. Por este motivo, a pesar de la implementación de las medidas mencionadas y, las soluciones que serán desarrolladas a continuación, no logran ser eficientemente aprovechadas, disminuyendo su valor y funcionamiento en pos del resguardo de los activos de información de la compañía.

Por otro lado, desde el punto de vista de la implementación de herramientas y soluciones de hardware y *software*, Zona Vital cuenta con UPS´s (*Uninterruptible Power Supply* o Sistema de alimentación ininterrumpida) en sus oficinas administrativas para proporcionar energía eléctrica en caso de que se produzca una interrupción de la corriente y, evitar el daño ocasionado en los equipos y en la información. Luego, las computadoras poseen instalado un *firewall* para controlar la entrada y salida de datos e información de la red interna de la firma, y un antivirus para la detección de amenazas. En este aspecto, cabe mencionar que la empresa, años atrás, tenía un antivirus que no contaba con la licencia de uso correspondiente. La gerente entrevistada recordó un problema surgido en torno a ello, cuando un empleado que se fue de Zona Vital en malos términos realizó una denuncia por este motivo (además, tenían otros programas sin licencia), lo cual derivó en una inspección y en la consecuente regularización de este aspecto. Además, cuenta con dos proveedores que se encargan de la reparación del *hardware.*

1.4 Conclusiones del caso de estudio

Zona Vital se encuentra en un nivel inicial o parcial —en los términos referidos en el *Cybersecurity Framework*— en materia de ciberseguridad. En este nivel de madurez, la empresa se caracteriza por la ausencia de prácticas formalizadas, implementadas y difundidas en todos los sectores y niveles de la organización en materia de ciberseguridad. Ello se debe, principalmente, a que no existe una cultura de trabajo consciente de los riesgos derivados del desarrollo de actividades basadas en tecnologías informáticas y, en donde, los activos digitales ocupan un papel cada vez de mayor trascendencia para el crecimiento del negocio. En consecuencia, la importancia brindada a la ciberseguridad es mínima si se contrasta la realidad de este sector, carente de un responsable a cargo y un presupuesto alineado a las necesidades (entre otras deficiencias), con la situación de otras áreas. Por ejemplo, con el diseño organizacional del área administrativa, la cual cuenta con un equipo definido y conformado por personal de rango jerárquico y empleados que reportan a aquel.

Finalmente, se evidencia que Zona Vital se encuentra altamente vulnerable en el contexto actual de negocios, donde las herramientas tecnológicas cumplen

un papel fundamental para su desarrollo. Sin embargo, a pesar del bajo nivel de concientización en materia de ciberseguridad reflejado, el programa de fidelización de clientes propicia una gran oportunidad para cambiar de manera radical la percepción de la compañía respecto de la importancia en el tratamiento de la seguridad informática. Las oportunidades de crecimiento a partir de la información aportada por este programa deben encontrarse sustentadas en eficiente medidas para su protección.

2. FarmaBelén

FarmaBelén es un emprendimiento familiar con más de seis décadas de presencia en el mercado farmacéutico. Actualmente, cuenta con ocho sucursales —una con atención 24hs— ubicadas en Capital y Provincia de Buenos Aires. La compañía se define como un centro de salud y belleza que se encuentra enfocado en proveer servicios de excelencia a los clientes, basados en relaciones de confianza. En tal sentido, tanto en su página web como en sus redes sociales, destaca "Nuestra prioridad es cuidar a nuestros AMIGOS". Asimismo, el sitio web resalta como principales aspectos de la compañía, la permanente capacitación de sus empleados y la innovación para construir una organización de vanguardia en el mercado farmacéutico, en donde constituyen un eslabón fundamental en la cadena de salud. La competencia de FarmaBelén se encuentra delimitada por la zona geográfica en la que se circunscribe su actividad, es decir, que los principales competidores son las denominadas farmacias de barrio, cuya arma de competitividad se basa en el contacto personal con el cliente. No obstante, el empleado del área de sistemas entrevistado[27], agregó que en este sentido, a partir del lanzamiento de la tienda *online* expandió las fronteras de alcance en los potenciales clientes.

Las actividades de la firma se encuentran segmentadas en dos líneas de negocio: farmacia y perfumería. Estas divisiones comparten personal administrativo y contable, por ejemplo, pero cuentan con una dotación de empleados diferente en las áreas de compra, ventas y marketing, por ejemplo. Ello se debe, según explicó uno de los empleados entrevistados, a que ambos

[27] Entrevista personal. Ver *Anexo 1: Entrevistas* para mayor detalle.

mercados apuntan a distintos objetivos. Por un lado, la división de farmacia se dedica a la dispensa de medicamentos y acompañamiento de la comunidad de clientes. Este segmento posee una mayor participación en el total de las ventas de FarmaBelén que la línea de perfumería y cosmética. Esta última se caracteriza por apuntar a un público más selectivo, a través de los productos ofrecidos (perfumes y artículos para el cuidado y la belleza corporal de alta calidad). Por lo tanto, las estrategias de marketing, por ejemplo, tienen una mayor presencia en la división de perfumería y cosmética, mediante el lanzamiento de promociones y beneficios a través de las redes sociales. En cambio, en referencia a lo señalado por uno de los empleados consultados, la farmacia es en mercado en donde la rigurosidad y profesionalismo en la atención de los clientes, representan los principales pilares.

En relación a los principales desafíos planteados por FarmaBelén en los próximos años, a partir de lo mencionado por el personal entrevistado, se destacan: por un lado, el crecimiento de las ventas mediante en canal *online*. En este sentido, el desarrollo de esta modalidad es considerada de especial trascendencia para competir a la vanguardia del sector farmacéutico y aumentar la base de cliente actual. Asimismo, cabe destacar que son pocas las cadenas de farmacias (Farmacity, por ejemplo) que en la actualidad cuentan con este recurso, el cual agrega una nueva experiencia de compra y un servicio de excelencia que ofrece una gran diversidad de productos (todos los disponibles en los locales físicos de la compañía, con excepción de medicamentos de venta bajo receta). Por el otro, la incorporación de nuevas sucursales representa el segundo de los desafíos manifestados.

2.1 Dimensiones de la ciberseguridad

A continuación, del mismo modo que se ha realizado en el caso de estudio anterior, se procede a analizar la importancia otorgada al tratamiento de la ciberseguridad en FarmaBelén, a partir de los siguientes ejes temáticos establecidos: 1) el conocimiento del significado de la ciberseguridad y de los ciberincidentes, y su incidencia en el ámbito corporativo; 2) el diseño de la ciberseguridad dentro de la estructura organizacional y designación de un presupuesto destinado a dicho sector y; 3) la importancia de los activos de información.

En primera instancia, el empleado del área de sistemas, señaló que dentro de su equipo de trabajo y en la empresa en general, la ciberseguridad es un tema abordado en algunos aspectos del negocio. En tal sentido, mencionó que, si bien los conceptos abordados en la presente investigación (ciberseguridad o seguridad informática, ciberincidentes, ciberataques, etc.) son apenas nombrados en reuniones de trabajo y en juntas que se llevan a cabo en colegios de farmacéuticos, fueron dos los episodios concretos que resaltaron la importancia de la seguridad informática en cuanto a la protección de los activos de información claves de la firma. Por un lado, a partir del inicio del proyecto de la tienda *online*, el equipo de sistemas comenzó a investigar acerca de distintos aspectos en el ámbito de la ciberseguridad, con el objetivo de proteger a los futuros usuarios de dicha herramienta. De esta manera, se contrató el protocolo SSL (*Secure Sockets Layer*) para el cifrado de los datos suministrados por los clientes al ingresar datos en la página web de la empresa y realizar transacciones en el canal de *e-commerce*. Por otro lado, hace unos años, FarmaBelén padeció la pérdida de información confidencial de ventas, lo cual generó un retraso en la actividad, ya que se decidió suspender momentáneamente el sistema de facturación hasta tanto se solucionara lo que había sucedido, con el fin de evitar más pérdidas de información. Este incidente que se cree, fue causado internamente por negligencia de algún empleado, afectó las dimensiones que le brindan calidad a este activo, es decir, su confiabilidad, integridad y disponibilidad. Actualmente, este hecho es recordado como una anécdota que sirvió para mejorar los aspectos relacionados al cuidado de los activos informáticos.

En segundo lugar, si bien, tal como sucede en la mayoría de las pequeñas y medianas empresas, no existe un responsable designado en ciberseguridad, FarmaBelén cuenta con un área de sistemas formalmente diseñada dentro de la estructura organizacional. El equipo de “sistemas de facturación y herramientas de información” está conformado por tres asistentes y un jefe o supervisor. Este sector se encarga de asegurar el correcto funcionamiento de los sistemas de gestión utilizados por la empresa y de proveer soporte a las distintas áreas en relación al uso de dispositivos y tecnologías informáticas (solucionar problemas en los programas y computadores, principalmente).

Asimismo, realizan tareas de configuración, mantenimiento y actualización del sistema operativo y *software*. En referencia al presupuesto asignado al desarrollo de funciones y actividades relacionadas a la protección de los activos de información críticos de FarmaBelén, este se encuentra incluido (aunque no discriminado) en los recursos destinados al área de sistemas. En otras palabras, frente a la ausencia de un sector de ciberseguridad conformado en la organización, el equipo de sistemas se encarga del desarrollo de mecanismos e implementación de soluciones ligadas a la ciberseguridad. De esta manera, se destacan las capacitaciones periódicas en distintos aspectos, tales como la confidencialidad de la información laboral, la utilización de dispositivos de almacenamiento, el cuidado en la navegación de internet y, fundamentalmente, en el uso del correo electrónico.

Por último, el personal entrevistado indicó que el capital humano y la información digital son los principales activos que posee FarmaBelén. Asimismo, considera probable que la organización pueda se afectada por un ciberincidente dentro de los próximos doce meses, aunque desconociendo la gravedad del impacto que podría generar dentro de la organización, tanto a nivel económico como el perjuicio a la imagen de la empresa. Por tales motivos, se considera muy importante el desarrollo de una cultura de concientización y construcción de capacidades en el ámbito de la seguridad informática en el escenario corporativo, en donde los activos de información desempeñan un papel fundamental.

En resumidas palabras, en FarmaBelén se ha observado un nivel de importancia aceptable, en función de las características del ámbito PyME en el que se desenvuelve, en materia de ciberseguridad. No obstante, el asistente del área de sistemas, señaló que es importante continuar destinando esfuerzos para establecer una estrategia de seguridad informática concreta, alineada a los objetivos del negocio, principalmente por los nuevos desafíos que plantea la venta *online*.

2.2 Funciones de la ciberseguridad

Actualmente, FarmaBelén no adopta ningún tipo de *framework* de ciberseguridad, sino que las acciones llevadas a cabo en dicho ámbito, se rigen

por el criterio profesional del personal de sistemas, en función del capital disponible y las necesidades del negocio. Sin embargo, a partir del lanzamiento de la tienda *online*, el equipo de sistemas ha comenzado a investigar sobre las mejores prácticas en el mercado y no han descartado una futura implementación de un marco de referencia para impulsar el crecimiento de esta nueva plataforma. En este apartado se lleva a cabo un análisis del desarrollo de las funciones de ciberseguridad (identificar, proteger, detectar, responder y restaurar) abordadas en el marco referencial del presente trabajo.

En primer lugar, FarmaBelén posee **identificados** los sistemas utilizados para el desarrollo de su negocio y tiene un inventario de los dispositivos físicos utilizados. No obstante, a pesar de la relevancia otorgada a los activos de información digitales como recurso crítico de la organización, carece de un registro formal y detallado de ellos. En otras palabras, FarmaBelén no cuenta con un inventario de los datos e información de los que se vale para la toma de decisiones, lo cual representa un gran riesgo y expone a la empresa a diversas vulnerabilidades en el ámbito de la seguridad informática (robo, pérdida, alteración, destrucción, manipulación de datos e información). Uno de los aspectos que merece ser destacado es la existencia de un análisis, por más rudimentario que esa, de los riesgos derivados de la utilización de tecnologías informáticas. En este sentido, los mencionados riesgos fueron tenidos en cuenta —a la par de los riesgos financieros, por ejemplo— en los últimos grandes proyectos relacionados al ámbito de sistemas: desarrollo (tercerizado) de página web y lanzamiento de la tienda *online*. Ello se relaciona a uno de los principales aportes del apartado *Risk IT* del COBIT, el cual hace referencia a la buena práctica de integrar la evaluación del riesgo de ciberseguridad con el análisis del riesgo corporativo. Esta característica demuestra, en principio, el compromiso de FarmaBelén por comprender la gestión del riesgo de una manera integral en el negocio. Además, el equipo de sistemas ha delineado algunas políticas, aún no formalizadas en un manual o documento: contraseñas seguras y privadas que deben ser actualizadas dentro de un período dado, copias de seguridad automáticas, entre otras.

En segundo lugar, entre las de medidas de ciberseguridad implementadas para la **protección** de los activos de información de FarmaBelén se destaca la

capacitación de los empleados. Es una característica que sobresale positivamente debido, a que como se ha reiterado en la presente investigación, en el ámbito PyME no es una práctica muy abordada y demuestra el compromiso de la organización por comenzar a tratar la seguridad informática desde una perspectiva más estratégica. El empleado de sistemas señaló que la formación y el desarrollo de las capacidades de los empleados en ciberseguridad, permite que tomen consciencia de las implicancias de sus trabajos diarios y colabore a generar responsabilidad en torno a la gestión de los sistemas e información. Asimismo, este comportamiento se enfatiza mediante la utilización de herramientas y mecanismos orientados al resguardo de los recursos informáticos críticos de la compañía, los cuales serán abordados en el siguiente apartado.

En cuanto a la función de **detección**, FarmaBelén trabaja con un antivirus instalado en cada uno de los equipos utilizados, el cual es gestionado por los miembros del equipo de sistemas. Ellos se encargan de configurarlo, mantenerlo actualizado y canalizan las consultas del personal en torno a su funcionamiento. Cabe mencionar que este programa es utilizado con una mirada proactiva, ya que los empleados del área de sistemas utilizan los reportes ofrecidos por el antivirus para evaluar su correcta actividad y observar las amenazas que fueron oportunamente detenidas.

En tercera instancia, en relación a la capacidad de **respuesta**, FarmaBelén no cuenta con un plan de contingencias para minimizar las consecuencias ante la ocurrencia de un incidente informático. No obstante, cabe mencionar que la existencia de un área de sistemas formalmente diseñada (con roles y responsabilidades establecidas) y, fundamentalmente, con conocimiento de los riesgos en el ambiente cibernético, proporciona mejores oportunidades para reducir los daños que un hecho así puede causar en la organización. Por su parte, uno de los aspectos a tener en cuenta en el desarrollo de un plan de respuestas incluye la notificación del hecho ocurrido a la autoridad competente. En este sentido, cuando la empresa sufrió la pérdida temporal de información, ello no ha sido denunciado por dos razones principalmente: 1) nunca se terminó de comprender si se trató de un ataque dirigido a la empresa por un tercero ajeno a la organización o algún empleado malintencionado o, si en

verdad, fue causado por negligencia del mismo personal de FarmaBelén y; 2) de haber conocido con certeza el origen del incidente cibernético, no hubieran sabido cómo proceder en ese contexto.

Por último, la empresa basa su proceso de **recuperación** de los activos digitales afectados en la gestión de copias de seguridad resguardadas en dispositivos físicos, como también en el servicio de la nube. Este mecanismo es considerado fundamental en la farmacia debido a que, cuando tuvo lugar el incidente de pérdida de información, se corrió el riesgo de no recuperarla ya que no contaban con el *back-up* de dicho activo digital. Finalmente, en cuanto a la consideración de seguros contra los ciberincidentes, si bien en la actualidad no se encuentran dentro de las prioridades (ni mucho menos), el equipo de sistemas reconoce que el crecimiento del negocio apoyado en herramientas tecnológicas debe estar respaldado por un seguro.

2.3 Instrumentación de la protección de los activos de información

En lo referido a los mecanismos, herramientas y controles implementados para instrumentar la protección de los activos de información en FarmaBelén, a continuación se lleva a cabo una descripción detallada de las medidas tomadas por la empresa en tal sentido. Con el objetivo de facilitar su comprensión, el análisis se divide en: 1) mecanismos generales de ciberseguridad y; 2) soluciones específicas de *hardware* y *software.*

Por un lado, la empresa cuenta con un esquema de privilegios diseñado para restringir el acceso a los recursos de información disponibles, según la posición ocupada en la compañía. El equipo de sistemas, como se ha mencionado anteriormente, se encarga de la actualización del *software* y del sistema operativo cuando se encuentren disponibles. Asimismo, los empleados que requieran instalar otros programas deben solicitarlo al equipo de sistemas. Por último, el procedimiento de *back-up* desarrollado por la compañía refleja su compromiso para responder frente a la materialización de un incidente, reduciendo su impacto mediante el resguardo de copias d seguridad de la información más valiosa de la organización. Cada uno de estas medidas, y las que serán desarrolladas a continuación, se apoyan en el compromiso de

FarmaBelén por mantener a sus empleados actualizados sobre los distintos riesgos que pueden afectar su trabajo diario. Las capacitaciones, impulsadas desde cualquier sector o empleado que considere el tratamiento de algún aspecto, constan de charlas sobre un tema en particular o reuniones de debate general, en donde participan activamente los empleados. Generalmente, se abarcan temas simples y concisos, como el cuidado al abrir archivos adjuntos a los correos electrónicos, la importancia de generar contraseñas seguras y privadas, entre otros.

Por el otro lado, FarmaBelén implementa un *firewall* del tipo *software* para proveer monitoreo y bloqueo de actividades sospechosas entre la red interna de la firma e internet. Esta herramienta ofrece la configuración de bloqueo de sitios web que podrían contener amenazas para el entorno de la seguridad informática. Por su parte, con el objetivo de detectar potenciales incidentes cibernéticos, la cadena de farmacias posee un antivirus licenciado. Asimismo, cuenta con el método SSL para transformar datos en texto cifrado que no puede ser leído por destinatarios no deseados y, posee UPS´s para proveer suministro eléctrico a los equipos y evitar daños en ellos y en la información contenida. Finalmente, cabe mencionar que FarmaBelén no trabaja con proveedores de servicios de ciberseguridad, ni tampoco recurre a consultores especialistas en dicho tema.

2.4 Conclusiones del caso de estudio

Luego de haber analizado el contexto de la ciberseguridad en FarmaBelén, en función de las variables planteadas, podemos concluir que se encuentra en un nivel parcial, aunque más avanzado que Zona Vital, en referencia a la clasificación adoptada por el marco de referencia *Cybersecurity Framework*. En tal sentido, la compañía es consciente de los riesgos a los que se encuentra expuesto sus activos digitales, como consecuencia de la utilización de tecnologías informáticas. De esta manera, se observan lineamientos (no documentados) de seguridad informática y la importancia brindada a las capacitaciones de los empleados, como puntos de partida para el abordaje estratégico de la ciberseguridad. No obstante, las prácticas de gestión de riesgos se limitan a proyectos que surgen de manera *ad hoc*, es decir, que no existe un proceso formal de evaluación de los riesgos derivados del uso de

tecnologías informáticas. Además, la posibilidad de expandir el negocio a través del canal de ventas *online* constituye otro motivo, por el cual el tratamiento de la ciberseguridad debería tratarse de una de las principales tareas en la agenda de FarmaBelén.

3. Conclusiones y reflexiones del capítulo

En este apartado se efectúa un análisis que contrasta la situación de la ciberseguridad de los dos casos de estudio involucrados en el trabajo. En este sentido, las distintas variables de comparación se corresponden con los ejes de análisis que fueron definidos en la sección de estrategia metodológica de la investigación.

Con respecto a las dimensiones generales de la ciberseguridad, en FarmaBelén se evidencia un mayor entendimiento de la importancia de las nociones de ciberseguridad y ciberincidentes en el ámbito corporativo. Al mismo tiempo, si bien en el caso de Zona Vital, el programa de fidelización impulsó la importancia del papel desarrollado por la información digital, en FarmaBelén se pudo observar una adopción más estratégica de este activo. No obstante, cabe agregar que, en ambas cadenas farmacéuticas el rol de la información aumentó como consecuencia de una iniciativa comercial: la tienda *online* en FarmaBelén y la "Tarjeta de Puntos Zona Vital" en la empresa homónima. En tanto, el diseño de la ciberseguridad y la conformación de un presupuesto destinado a dicho ámbito son características que reflejan el mismo patrón de comportamiento en ambas firmas. En otras palabras, las dos empresas carecen de un área o un responsable de seguridad informática formalmente delineado en la estructura organizacional y, en consecuencia, tampoco asignan un presupuesto a dicho ámbito. No obstante, es este punto, se evidenció que, al menos, FarmaBelén destina recursos en el presupuesto de sistemas para el desarrollo de funciones y actividades ligadas a la ciberseguridad.

El siguiente punto hace referencia al desarrollo de las funciones en el campo de la ciberseguridad, según fueron definidas en los *frameworks* abordados en el marco referencial. En este sentido, las principales semejanzas entre ambos

casos de estudio se observan en la funciones de detección, respuesta y recuperación ante incidentes cibernéticos. En primer lugar, tanto Zona Vital como FarmaBelén limitan su capacidad de detección de amenazas que pueden poner en riesgo sus activos de información, a través de la implementación de un antivirus en los equipos utilizados. No obstante, cabe mencionar que existe una diferencia en la administración de estos programas, ya que FarmaBelén hace un uso más proactivo de dicha herramienta en el trabajo diario. En segundo término, ambas compañías farmacéuticas se caracterizan por no contar con un plan de contingencias para responder de manera eficiente a los ciberincidentes que pudieran ocurrir. Finalmente, la función de recuperación con objeto de minimizar los costos y pérdidas organizacionales derivados de un incidente informático, se encuentra abordada de manera similar por las dos firmas: realización de copias de seguridad. Aunque, se evidencia un proceso de *back-up* mejor implementado en el caso de FarmaBelén. En cuanto a las desigualdades observadas en el análisis de las restantes funciones de ciberseguridad (identificación y protección), Zona Vital no cuenta procesos delineados en dicho ámbito, mientras que FarmaBelén posee procesos definidos (no formalizados en manuales o documentos) en seguridad informática, tales como la conformación de contraseñas robustas en los usuarios. Por último, pero no menos importante, la principal desigualdad detectada en la función de protección, se refiere a las capacitaciones que será indicada en el siguiente párrafo.

Para concluir, en lo referido a la implementación de mecanismos y soluciones de *hardware* y *software*, se evidencia una gran diferencia en cuanto al desarrollo de capacitaciones y formación de las competencias de los empleados en cuestiones de seguridad informática en el caso de FarmaBelén. Por el contrario, Zona Vital no lleva a cabo dichas actividades que constituyen la base de una cultura sólida en el tratamiento de la ciberseguridad. En relación a las soluciones empleadas, en ambos casos se observan similitudes en la adopción de programas antivirus y *firewall.*

A modo de cierre, con el objetivo de esquematizar y facilitar la comprensión de las cuestiones más relevantes surgidas a partir del análisis comparado de los casos de estudio, se incluye la siguiente tabla en donde se sintetizan las

similitudes y diferencias en materia de ciberseguridad entre Zona Vital y FarmaBelén.

Ejes de análisis	Sub-variables	Zona Vital	FarmaBelén
Dimensiones generales de ciberseguridad	i) Conocimiento de los conceptos	No posee	Básico
	ii) Diseño de la ciberseguridad y presupuesto	No posee	Básico
	iii) Importancia de la información digital	Perspectiva estratégica moderada	Perspectiva estratégica alta
Funciones de ciberseguridad	i) Identificación	*Carece de identifiación de los activos digitales; *No posee políticas de seguridad informática.	*Carece de identifiación de los activos digitales; *Posee políticas no formales de seguridad informática.
	ii) Protección	*No realiza capacitaciones. *Implementa mecanismos y soluciones de ciberseguridad.	*Realiza capacitaciones. *Implementa mecanismos y soluciones de ciberseguridad.
	iii) Detección	* Utilización de antivirus.	* Utilización de antivirus.
	iv) Respuesta	*No posee un plan de contingencias.	*No posee un plan de contingencias.
	v) Recuperación	**Backup* básico; *Desconocimiento de seguros contra ciberincidentes.	**Backup* avanzado; *Conocimiento de seguros contra cibeincidentes.
Instrumentación de ciberseguridad	i) Mecanismos generales	* Contraseñas , actualziación de *software* y *backup.*	* Capacitación, contraseñas seguras, actualziación de *software* y *backup.*
	ii) Soluciones de *hardware* y *software*	* Antivirus, *firewall* y UPS.	* Antivirus, *firewall,* encriptación de datos y UPS.

Fuente: elaboración personal

CAPÍTULO 5: CONCLUSIONES, APORTE PROFESIONAL Y LÍNEAS FUTURAS DE INVESTIGACIÓN

En este capítulo, se presentan algunas conclusiones y recomendaciones finales que se desprenden del estudio llevado a cabo. Luego, se resalta el valor práctico de la presente investigación y, finalmente, se exponen algunas líneas que resultan interesantes de ser investigadas en futuros trabajos.

1. Conclusiones y recomendaciones

En primer lugar, cabe mencionar que, dado el foco y el método de estudio empleado para el desarrollo de la presente investigación, las conclusiones que serán presentadas a continuación se encuentran limitadas a los casos de estudio abordados. En tal sentido, aquellas cuestiones de carácter general que se remarcan en torno a la ciberseguridad son señaladas para contextualizar el entorno en el que se enmarcan las empresas comprendidas en nuestro estudio.

La migración de la información del papel a medios digitales es un proceso que se ha iniciado hace varios años y, que, actualmente, se encuentra consolidado como una de las maneras más eficientes de almacenar y gestionar datos e información. No obstante, la validez estratégica de este recurso dentro del ámbito corporativo depende de las medidas de protección llevadas a cabo, con el objetivo de resguardar las características de confidencialidad, integridad y disponibilidad de la información digital. En este sentido, en el presente trabajo, se ha hecho énfasis en la importancia de desarrollar una estrategia integral y efectiva de ciberseguridad, destinada al resguardo de los activos de información, fundamentalmente, de aquellos que resultan críticos para el desarrollo y crecimiento de la empresa. Al mismo tiempo, cabe destacar que las medidas adoptadas en tal sentido deben ser lo suficientemente rigurosas para proteger a los recursos de información de las amenazas cibernéticas, pero no deben obstaculizar el crecimiento e innovación del negocio. En otras palabras, es necesario analizar el *trade-off* entre las medidas de seguridad informática aplicadas y el nivel de protección de la información deseado, que

sea más eficiente para que la ciberseguridad actúe como facilitadora del desarrollo organizacional.

La innovación se recuesta sobre buenos datos, capaces de generar información de utilidad para la toma de decisiones. En dicho proceso, la tecnología funciona como un habilitador del negocio que permite gestionar, procesar, almacenar y transmitir la información, pero la seguridad es el elemento diferenciador que garantiza la integridad, confiabilidad y disponibilidad de dicha información. En tal sentido, la inversión para la conformación de ambientes de trabajo que proporcionen seguridad en el espacio informático representa un gran desafío para las empresas. Pues, no se trata de asignar indiscriminadamente una cantidad determinada de recursos (dinero, capital humano, etc.) para la adquisición de programas y equipos físicos (antivirus, *firewall,* UPS, controles biométricos, etc.) para mitigar la probabilidad de ocurrencia de incidentes informáticos. A pesar de las capas de seguridad que se hayan implementado en la compañía para la protección de los activos de información, si el usuario no es consciente de sus acciones (descarga un *malware* al acceder a un sitio web o conecta un *pendrive* infectado a su computadora), ninguna de las soluciones y herramientas utilizadas cumplirán con sus objetivos. En otras palabras, las inversiones que se focalizan solamente en el aspecto tecnológico de la ciberseguridad no añaden ningún valor en el desarrollo de una cultura donde la seguridad informática sea tratada como una prioridad, a menos que se destinen los recursos adecuados para capacitar a los empleados. La construcción de un espacio de trabajo donde cada empleado sea consciente de los riesgos asociados a la utilización de tecnologías informáticas, es el primer paso en el proyecto de desarrollo de capacidades en el ámbito de la seguridad informática.

En referencia al análisis comparado de casos, se evidenció que las PyMEs de la industria de *retail* farmacéutico estudiadas, se encuentran en una etapa de aprendizaje en materia de ciberseguridad, en donde su la relevancia discutida. De esta manera, más allá de las semejanzas y desigualdades presentadas anteriormente entre ambas compañías, resulta pertinente agregar un concepto central en el análisis. En este sentido, tanto Zona Vital como FarmaBelén han

demostrado una actitud o accionar predominantemente reactivo al abordar la seguridad informática en el interior de la organización. Dicho de otra manera, en ambas compañías farmacéuticas se evidencia un comportamiento pasivo en el desarrollo de prácticas y medidas relacionadas al ámbito de la ciberseguridad. En el caso de Zona Vital, a partir del programa de fidelización se comenzó a priorizar el valor otorgado por la información como base para el crecimiento del negocio. Por su parte, en FarmaBelén, el desarrollo de funciones y mecanismos orientados a la protección de sus activos digitales, empezaron a ser tenidos en cuenta e implementarse, a partir del diseño del gran proyecto de lanzamiento de su tienda *online* y de la ocurrencia de un incidente (como lo fue la pérdida de información mencionada). En resumidas palabras, resulta interesante señalar cómo estas empresas, con una larga trayectoria en el sector de *retail* farmacéutico, comienzan a reconocer la relevancia de sus activos digitales y del abordaje de la ciberseguridad para su resguardo de forma reactiva, a partir de un hecho en particular (como lo es un incidente o una iniciativa de negocio) y, no parece surgir desde un interés o preocupación estratégica de la compañía. En este contexto, el riesgo es que las empresas actúen solamente desde un punto de vista operativo (por ejemplo, incorporando una solución tecnológica), sin tener en consideración la perspectiva integral, sistémica, con foco en el mediano y largo plazo. En este sentido, el apoyo de estas firmas en las herramientas y recomendaciones brindadas por los *frameworks* o marcos de mejores prácticas en el ámbito de la seguridad informática, podría generar un cambio de la mentalidad en dicho aspecto, con el objetivo de abordar la ciberseguridad desde una posición estratégica.

En esta era digital, donde lo único constante y seguro es el cambio, una de las calves para afrontar los distintos riesgos que se presentan es entender la ciberseguridad como una aliada estratégica del negocio. Las compañías deberían considerarla como un factor clave, una solución integral para impulsar el crecimiento y crear ventajas competitivas para diferenciarse del resto de los jugadores del mercado. Por ello, para conformar una estrategia sólida y eficiente de seguridad informática, la pregunta principal no debería ser si la empresa va a sufrir un ciberincidente porque, tal como señala el *Executive*

Director en Ciberseguridad de EY, si se encuentra conectada a la red es un blanco más[28]. Las preguntas que giran en torno a los ciberincidentes no son una cuestión de si ocurrirán, sino de cuándo y cómo responder, de manera de minimizar los costos. En tal sentido, la ciberseguridad debería ser abordada como un proceso de mejora continua, capaz de readaptarse continuamente a los cambios que presenta el entorno. Las nuevas tecnologías, el *Internet of Things*, y los nuevos medios de información digital, implican nuevos riesgos y vulnerabilidades. Por lo tanto, el desafío de la ciberseguridad solamente aumentará y dependerá de las empresas ubicarse un paso por delante de las amenazas.

Para concluir, cabe señalar que la responsabilidad de la conformación de un entorno de negocios donde prime la seguridad informática, se podría plantear desde el compromiso en dos dimensiones. Por un lado, desde el Estado y, a través de los organismos e instituciones públicas, se debería abordar a la ciberseguridad desde diversos aspectos, tales como el establecimiento de canales eficientes de comunicación en donde fluya conocimiento, información, experiencias y las mejores prácticas en relación a la adopción de medidas orientadas a la seguridad informática. Asimismo, se debería trabajar en la mejora de la legislación vigente y creación de nuevas normas en dicho ámbito, ya que se podría pensar que, tal vez, la legislación local sea un tanto laxa para con las firmas nacionales y, por ello, no tengan incentivos para desplegar iniciativas de manera proactiva en el campo de la ciberseguridad. En tal sentido, se podría analizar el caso de las regulaciones estrictas impuestas a las empresas europeas, como lo es el *General Data Protection Regulation*, que las obliga a actuar activamente en cuestiones de seguridad informática para prevenir multas y sanciones, que las dejarían expuestas frente al entorno corporativo (clientes, proveedores y demás socios del negocio).

Por otro lado, desde el sector privado se debería comenzar (en aquellas empresas donde el nivel de concientización en ciberseguridad se encuentra en una etapa inicial) e impulsar (en las compañías con mayor experiencia en dicha área) el desarrollo de funciones y actividades orientadas a la conformación de ámbitos corporativos seguros desde el punto de vista del resguardo de un

[28] Entrevista personal. *Ver Anexo 1: Entrevistas* para mayor detalle.

activo fundamental, como lo es la información. De esta manera, los marcos de referencia que recomiendan una gran cantidad de controles, herramientas y procedimientos orientados a la ciberseguridad, como así también la certificación en estándares internacionales, tales como las normas ISO, podrían ser abordados como guías para el desarrollo de capacidades corporativas en el ámbito de la seguridad informática.

2. Aporte profesional

En primer lugar, resulta importante mencionar que uno de los principales objetivos del estudio es aportar un visión con impronta profesional para que aquellos empresarios de PyMEs argentinas del sector de *retail* farmacéutico (dueños de farmacia, profesionales del área, y para quienes lo consideren pertinente) puedan comprender: la relevancia del tema abordado, la magnitud de los riesgos a los que se encuentran expuestas sus compañías frente a la ausencia de medidas de ciberseguridad y los beneficios que pueden obtener, a partir del empleo de mecanismos de protección frente a eventuales incidentes informáticos. Debido a que la disponibilidad de recursos económicos con la que cuentan estas compañías, en relación a las grandes corporaciones, suele ser más acotada, uno de los propósitos es brindar lineamientos que ayuden a que esos empresarios puedan eficientizar las inversiones en ciberseguridad para sus negocios. De esta manera, los lineamientos que brindan los frameworks abordados y las distintas medidas y soluciones desarrolladas en el capítulo 2, se encuentran orientadas a establecer una guía de adopción de las mejores prácticas de seguridad informática para las pequeñas y medianas empresas. En síntesis, a través del relacionamiento entre el marco referencial planteado y el análisis de los casos abordados, se busca crear conciencia sobre la ciberseguridad en el contexto de las PyMEs en general y de la industria de *retail* farmacéutico en particular, mediante la descripción del escenario actual de riesgos e incidentes relacionados a la gestión de la seguridad informática, como así también de las mejores prácticas para velar por el resguardo de la confiabilidad, disponibilidad e integridad de la información.

En segunda instancia, se espera que, a través de sucesivas muestras de adopción de medidas efectivas de ciberseguridad en la esfera de las pequeñas y medianas empresas, cada vez más compañías logren acercarse y familiarizarse con el concepto de la ciberseguridad como un aspecto esencial para la sostenibilidad del negocio en el tiempo. En este sentido, la inclusión de un marco de referencia internacional respecto de la situación en materia de seguridad informática en otros países pretende generar un aporte adicional para el ámbito empresarial. En definitiva, la intención es darle una aplicación práctica al trabajo, un valor agregado más allá de la descripción realizada de los distintos aspectos y problemas que existen respecto de la seguridad informática en las PyMEs de *retail* (farmacéutico en particular).

Finalmente, se espera informar a los hacedores de políticas públicas acerca de las mejores formas de apoyar a las pequeñas y medianas empresas para enfrentar los desafíos de la ciberseguridad de manera eficiente. En función de la relevancia que tienen estas organizaciones en el desarrollo económico y social del país, sería importante enfocarse en el abordaje de soluciones integrales, holísticas de ciberseguridad que se encuentren alineadas a las necesidades de estas firmas. El apoyo de los organismos públicos en términos de financiamiento, formación y asesoramiento resulta fundamental para fomentar el crecimiento del tejido empresarial.

3. Futuras líneas de investigación

En el siguiente capítulo se enunciarán aquellos temas, susceptibles de ser analizados, surgidos a partir del marco teórico y del desarrollo de la presente investigación pero que, en función de nuestros objetivos y enfoque, no fueron abordados en el trabajo. A continuación se señalarán diversas líneas de investigación que merecen ser estudiadas en profundidad en futuros trabajos, y pueden complementar el análisis del presente estudio.

En primer lugar, haciendo énfasis en la relevancia de la formación de profesionales en el campo de la ciberseguridad, se propone un estudio de la situación de la educación universitaria y terciaria en dicho ámbito, y su relación

con el estado de la ciberseguridad y la carencia de personal capacitado en el mundo corporativo argentino. En este sentido, se considera oportuno resaltar la gran oportunidad que representa esta realidad para los jóvenes, ya que los profesionales de ciberseguridad capaces de evolucionar al ritmo del cambio tecnológico serán cada vez más requeridos en todo tipo de industria, alrededor de todo el mundo. Según Forbes, se crean un millón de nuevos puestos de trabajo en ciberseguridad en el mundo por año y, se proyecta que para el 2019, el número de profesionales requeridos globalmente aumente de cinco a seis millones (Maggi, 2017). Sin embargo, la oferta laboral de talento en este campo es incapaz de cubrir el exponencial crecimiento de la demanda. Por tal motivo, resulta interesante evaluar las condiciones existentes de enseñanza en seguridad informática en el país, para lo cual se podría llevar a cabo un análisis comparativo con otras naciones para de poder identificar las medidas a desarrollar para impulsar dicho aspecto.

En segunda instancia, otra posible línea de investigación es el estudio de un tipo de ciberincidente en particular, como bien podría tratarse del análisis del impacto del *ransomware* en las grandes empresas. Esta clase de ataque informático se encuentra en constante ascenso y representa una de las mayores preocupaciones de las organizaciones y compañías a nivel global. En 2016, según un informe de KasperskyLab, las empresas alrededor del mundo recibían un ataque de este tipo cada 40 segundos y, una de cada cinco pequeñas y medianas empresas pagaban el rescate exigido y nunca recuperaron la información robada (*Kaspersky Security Bulletin*, 2016). El crecimiento de estos ciberataques es una realidad que debe ser afrontada con la responsabilidad que corresponde porque, de lo contrario, cada vez serán más dañinos para las empresas y la sociedad en general. De hecho, en 2017, tuvieron lugar los renombrados "WannaCry", "Petya" y "Bad Rabbit", los cuales afectaron a usuarios de todo tipo, desde grandes y pequeñas empresas hasta particulares y organismos gubernamentales de diferentes países, a lo largo y ancho del planeta. En este sentido, cabe mencionar que la tendencia marca —fundamentalmente, dado al crecimiento proyectado del *bitcoin* (criptomoneda exigida como recompensa)— que este ciberataque continuará en expansión durante los próximos años. Por estas razones, el análisis en profundidad de

este fenómeno y de las mejores prácticas y medidas para minimizar su impacto resulta una interesante propuesta de investigación a futuro.

Luego, el estudio de las nuevas vulnerabilidades a las que se encuentran expuestas las personas y/o empresas a partir del inminente desarrollo de la IoT (*Internet of Things*), resulta un tema novedoso y de suficiente relevancia para plantear un estudio. En este sentido, se estima que “la Internet de las Cosas será parte de prácticamente la mitad de los dispositivos conectados para 2020, como autos, heladeras, dispositivos médicos e incluso objetos que aún no han sido inventados, lo que llevará a un tremendo aumento en amenazas y vulnerabilidades de 2018 en adelante” (Ramachandran, 2018). De hecho, el informe de predicciones de ciberseguridad realizado por Gartner, revela que para el 2020, más del 25% de los ataques cibernéticos padecidos por las empresas estarán vinculados a la utilización de IoT, aunque el presupuesto asignado a esta disciplina será solo del 10% del total brindado para la ciberseguridad (Panetta, 2016). Esto podría generar una increíble explosión de amenazas en cada uno de los sistemas de seguridad que conocemos actualmente, exhibiendo grandes debilidades y desafiándolos al desarrollo de nuevos y más sofisticados mecanismos de ciberseguridad para la protección de dispositivos IoT.

Finalmente, planteamos el análisis de las cuestiones éticas que rodean a la gestión de la ciberseguridad en el escenario corporativo como una futura línea de investigación que presenta grandes desafíos. En este sentido, los mecanismos, procedimientos y herramientas orientadas a la administración de la seguridad informática en las empresas opera en una delgada línea entre comportamientos éticos y otros que pueden ser razonablemente cuestionados desde esta óptica. En otras palabras, el personal responsable de desarrollar dichas actividades y monitorear su cumplimiento posee acceso al contenido del correo electrónico corporativo del resto de los empleados, en muchos casos, sin que estos últimos lo sepan. Asimismo, qué tan ético puede ser considerado el control y los límites impuestos sobre los sitios web a los que acceden los trabajadores o, el ingresar a los archivos guardados en sus equipos sin consentimiento alguno. En esta misma línea podríamos continuar enumerando situaciones de estas características que no son nada fáciles de resolver, por lo

cual se propone una investigación relacionada a este aspecto de la ciberseguridad.

Fuentes de referencia

Bibliografía

Canedo Estrada, A. (Junio de 2010). La informática forense y los delitos informáticos. *Revista Pensamiento Americano*(4), 81-88. Recuperado de: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/98/93

Clase Sistemas de Información UdeSA. (Mayo de 2017). *Módulo VI: Auditoría, seguridad y delito informático*. Prof. Gabriel Aramouni. Universidad de San Andrés, Victoria, Argentina.

Clase Sistemas de Información. (Mayo de 2017). *Módulo V – Continuación: E-commerce, E-business, Balanced Score Card*. Prof. Gabriel Aramouni. Universidad de San Andrés, Victoria, Argentina.

Dewdney, A. (1989). Computer Recreations: Of Worms, Viruses and Core War. *Scientific American*. Recuperado de: http://www.koth.org/info/akdewdney/Last.htm

Drucker, P. (1999). *Management Challenges for the 21st Century* (First Edition). Estados Unidos: Harper Business.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2010). *Merodología de la investigación* (Quinta ed.). México DF: Mc Graw Hill.

Laudon, K. y Laudon, J. (2012). *Management Information Systems* (Twelfth Edition). Estados Unidos: Prentice Hall.

Ojeda-Pérez, J., Rincón-Rodríguez, F., Arias-Flórez, M., & Daza-Martínez, L. (Enero-Junio de 2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad, 11*(28), 41-66. Recuperado de: http://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176/2416

Tonon, G. (Mayo de 2011). La utilización del método comparativo en estudios cualitativos en ciencia política y ciencias sociales: diseño y desarrollo de una tesis doctoral. *Revista Kairos*(27), 1-12.

Informes y artículos

Acosta, D. (23 de diciembre de 2016). Guía rápida para entender el marco de trabajo de ciberseguridad del NIST. *Internet Security Auditors*. Recuperado de: http://blog.isecauditors.com/2016/12/guia-rapida-para-entender-marco-trabajo-de-ciberseguridad-del-NIST.html

Better Business Bureau. (2017). *State of Cybersecurity among Small Business in North America.* Virginia, Estados Unidos. Recuperado de: https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf

Cámara Industrial de Laboratorios Farmacéuticos. (2017). *Plan Estratégico para el Desarrollo del Sector Farmacéutico Nacional 2017-2021.* Buenos Aires, Argentina. Recuperado de: http://www.cilfa.org.ar/archivos/File/La%20industria%20farmaceutica/Plan%20estrat%C3%A9gico%20CILFA%20%202017-2021%20VF.pdf

Centro Criptológico Nacional. (2017). *Ciberamenazas y Tendencias*. Recuperado de: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2224-ccn-cert-ia-16-17-ciberamenzas-y-tendencias-edicion-2017/file.html

Duna. (13 de junio de 2018). *Miguel Pérez por ciberataque: "Países como Chile e instituciones y empresas chilenas están más en riesgo que las compañías internacionales"*. Recuperado de: http://www.duna.cl/programa/hablemos-en-off/2018/06/13/miguel-perez-por-ciberataque-paises-como-chile-e-instituciones-y-empresas-chilenas-estan-mas-en-riesgo-que-las-companias-internacionales/

Ebizlatam. (22 de septiembre de 2017). *El 60% de las empresas argentinas invertirá en ciberseguridad en los próximos dos años*. Recuperado de: http://www.ebizlatam.com/60-las-empresas-argentinas-invertira-ciberseguridad-los-proximos-dos-anos/

Fernández, V. (Mayo de 2018). La identidad de los usuarios, un elemento crítico en la seguridad de las empresas. *CSO España*. (26). Recuperado de: http://cso.computerworld.es/pubs/cso26/

Fortino, M. (7 de Diciembre de 2017). Realizando auditorías de seguridad utilizando COBIT 5, ISO 27001 y el framework NIST Cybersecurity. *Information Systems Audit and Control Association*. Recuperado de: https://isaca.org.ar/2017/12/07/realizando-auditorias-de-seguridad-utilizando-cobit-5-iso-27001-y-el-framework-nist-cybersecurity/

Gobierno del Reino Unido. (2018). *UK Government's Cyber Essentials Scheme.* Recuperado de https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

González Pérez, L. (7 de noviembre de 2017). Argentina, entre los países que más phishing reciben en el mundo. *Clarín*. Recuperado de: https://www.clarin.com/sociedad/argentina-paises-phishing-reciben-mundo_0_SkrEtz1kM.html

Harán, J. (13 de Junio de 2018). Chile busca asesoramiento en ciberseguridad tras ciberataque al Banco de Chile. *Welivesecurity*. Recuperado de: https://www.welivesecurity.com/la-es/2018/06/13/chile-busca-asesoramiento-en-ciberseguridad-tras-ciberataque-al-banco-de-chile/

Instituto Nacional de Ciberseguridad de España. (30 de Noviembre de 2016). *CEO, CISO, CIO… ¿Roles en ciberseguridad?* Recuperado de Instituto Nacional de Ciberseguridad: https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad

Information Systems Audit and Control Association. (2017). *Getting started with data governance using COBIT 5*. Estados Unidos.

Information Systems Audit and Control Association. (2017). *State of Cyber Security 2017.* Estados Unidos: ISACA. Recuperado de: https://www.cybersecobservatory.com/wp-content/uploads/2017/06/state-of-cybersecurity-2017-part-2_res_eng_0517-1.pdf

Information Systems Audit and Control Association. (s.f.). *ISACA Certification fact sheet*. Recuperado de: https://www.isaca.org/About-ISACA/Press-room/Documents/Certification-Fact-Sheet_0318.pdf

International Telecommunication Union. (2017). *Global Cybersecurity Index 2017.* Recuperado de: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

Kaminski, P., Rezek, C., Richter, W., & Sorel, M. (Enero de 2017). *Protecting your critical digital assets: Not all systems and data are created equal*. Recuperado de: https://www.mckinsey.com/business-functions/risk/our-insights/protecting-your-critical-digital-assets-not-all-systems-and-data-are-created-equal?cid=eml-app

Kantor, D. (15 de Mayo de 2016). Delitos informáticos: la mayoría de las empresas no los denuncia. *Clarín*. Recuperado de: https://www.clarin.com/economia/Delitos-informaticos-mayoria-empresas-denuncia_0_S1XgKqjOv7l.html

Kaspersky Lab. (2016). *Kaspersky Security Bulletin 2016.* Estados Unidos. Recuperado de: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07182317/KASPERSKY_SECURITY_BULLETIN_2016.pdf

Maggi, G. (28 de Agosto de 2017). Ciberseguridad, un desafío para las empresas y una oportunidad en el mercado laboral. *Télam*. Recuperado de: http://www.telam.com.ar/notas/201708/199392-ciberseguridad-empresas-mercado-laboral-opinion.html

Mendoza, M. (16 de Junio de 2015). ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia. *Welivesecurity.* Recuperado de: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Núñez, L. (26 de Mayo de 2018). Ciberataques en Chile no sólo afectan a bancos: Por qué los hackers también apuntan a servicios industriales y de la salud. *Emol*. Recuperado de: http://www.emol.com/noticias/Tecnologia/2018/05/26/907521/Ciberataques-en-Chile-no-solo-afectan-a-bancos-Por-que-los-hackers-tambien-apuntan-a-servicios-industriales-y-de-Salud.html

Obama, B. (2015). *Remarks by the President at the National Cybersecurity Communications Integration Center*. Virginia, Estados Unidos.

Recuperado de: https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent

Office of the United States Trade Representative, Small Business. Recuperado de: https://ustr.gov/issue-areas/small-business

Panetta, K. (15 de Junio de 2016). Gartner's Top 10 Security Predictions 2016. *Gartner*. Recuperado de: https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/

Perazo, C. (31 de Diciembre de 2017). Un repaso por los hechos tecnológicos más notables de 2017. *La Nación*. Recuperado de: https://www.lanacion.com.ar/2096518-un-repaso-por-los-hechos-tecnologicos-mas-notables-de-2017

Price Waterhouse Coopers. (2018). *Encuesta Global de Seguridad de la Información.* Buenos Aires, Argentina.

Price Waterhouse Coopers. (2017). *Encuesta Global de Seguridad de la Información. Capítulo Argentina.* Buenos Aires, Argentina. Recuperado de: https://www.pwc.com.ar/es/publicaciones/assets/encuesta-global-seg-inf2017.pdf

Price Waterhouse Coopers. (2017). *Encuesta Mundial sobre el Estado de la Seguridad de la Información 2017.* Madrid, España: PwC.

Price Waterhouse Coopers. (2017). *Consumer Intelligence Series: Protect.me.* Estados Unidos. Recuperado de: https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf

Ramachandran, R. (Enero de 2018). *Predicciones para 2018 sobre ciberseguridad*. Recuperado de: https://isaca.org.ar/2018/01/02/predicciones-para-2018-sobre-ciberseguridad/

Rivas, F. (4 de Enero de 2018). Seguridad informática: escasez de profesionales es uno de los principales obstáculos. *Biobiochile*. Recuperado de: https://www.biobiochile.cl/noticias/ciencia-y-

tecnologia/moviles-y-computacion/2018/01/04/seguridad-informatica-escasez-de-profesionales-es-uno-de-los-principales-obstaculos.shtml

Roy, M. (Mayo de 2018). CISO careers: Several factors propel high turnover. *TechTarget*. Recuperado de: https://searchcio.techtarget.com/feature/CISO-careers-Several-factors-propel-high-turnover

Tchouhadjian & Asociados. (2018). *Mercado de la farmacia. Análisis 2017 y evolución y perspectivas para el año 2018.* Buenos Aires, Argentina.

Varela, G. (2017). Las 15 principales estadísticas de 2017 para IT. *Revista IT Now*. Recuperado de: https://revistaitnow.com/las-15-principales-estadisticas-2017/

Normativas, regulaciones y *frameworks*

Consejo de Europa. (Noviembre de 2001). *Convenio sobre la Ciberdelincuencia.* Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Information Systems Audit and Control Association. (2009). *The Risk IT Framework.* Recuperado de: http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf

International Organization for Standardization . (2013). *ISO/IEC 27001:2013.*

International Organization for Standardization. (2012). *ISO/IEC 27032:2012 .*

Information Systems Audit and Control Association. (2012). *COBIT 5.*

Ministerio de Justicia y derechos Humanos. Presidencia de la Nación. *Ley 11.723*: *Propiedad Intelectual.* Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

Ministerio de Justicia y derechos Humanos. Presidencia de la Nación. (Octubre, 2000). *Ley 25.326: Protección de los Datos Personales*. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

Ministerio de Justicia y derechos Humanos. Presidencia de la Nación. (Junio, 2008). *Ley 26.388: Modificación del Código Penal*. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

Ministerio de Modernización, Presidencia de la Nación. El panorama de ciberseguridad en números. Recuperado de: https://www.argentina.gob.ar/sites/default/files/cofemod_comisionciberseguridad_el_panorama_de_la_ciberseguridad_en_numeros_12-08-16.pdf

Ministerio de Modernización. (Marzo de 2017). Comisión de Ciberseguridad. *Plan de Trabajo 2017.* Recuperado de: https://www.argentina.gob.ar/sites/default/files/cofemod_comisionciberseguridad_plan_de_trabajo_2017.pdf

Ministerio de Producción de la Nación. (2018). *Resolución 154/2018*. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/309999/norma.htm

Ministerio de Producción de la Nación. (2017). *Resolución 103-E/2017*. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/270000-274999/273192/norma.htm

National Institute of Security and Technology. Cybersecurity Framework 2017. Recuperado de: https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf

National Institute of Security and Technology. (s.f.*).* Cybersecurity Framework. Recuperado de: https://www.nist.gov/industry-impacts/cybersecurity

Reglamento General de Protección de Datos. *Reglamennto (UE) 2016/679 del Parlamento Europeo y del Consejo*. Recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from

Sitios web consultados

Cámara Argentina de Comercio Electrónico: http://www.cace.org.ar/estadisticas

Deslock: https://www.deslock.com/

Farmacias Belén: https://farmaciasbelen.com.ar/

Greycortex: https://www.greycortex.com/mendel-analyst

Kaspersky Lab: https://usa.kaspersky.com/small-business-security/small-office-security

Ministerio de Moderinzación de la Nación: https://www.argentina.gob.ar/modernizacion

Ministerio de Producción de la Nación: https://www.produccion.gob.ar/pymes

Observatorio de la Ciberseguridad en América Latina y el Caribe: http://observatoriociberseguridad.org/graph/countries//selected//0/dimensions/1-2-3-4-5

Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Recuperado de: http://www.icic.gob.ar/capacitacion.html

ZMA IT Solutions: https://www.zma.la/producto/password-manager-pro/

https://www.zma.la/producto/wfilter/

Zona Vital: http://zonavital.com

Entrevistas realizadas

Gerente Comercial y de Operaciones de Zona Vital. (25 de Abril de 2018).

Asistente de Sistemas de facturación y herramientas de información de FarmaBelén. (30 de Abril de 2018).

Executive Director en Ciberseguridad en Ernst&Young Argentina y Profesor de Sistemas de Información en UdeSA, Nicolás Ramos. (16 de Julio de 2018).

Anexos

Anexo 1: Entrevistas

A continuación se enuncian las preguntas que se emplearon como guía en las entrevistas llevadas a cabo con los distintos actores involucrados en el desarrollo de la presente investigación.

1.1 Preguntas guía: Zona Vital y FarmaBelén

Aspectos generales de las compañías

- ¿Cuál es su posición en la empresa?
- ¿Cuántos empleados y sucursales tiene la compañía?
- ¿Existe una división por segmentos en la firma?, ¿Cuál es el más relevante en términos de facturación?
- ¿Cómo se define la empresa en el mercado farmacéutico?, ¿Cómo buscan diferenciarse de la competencia?
- ¿Quiénes son los principales competidores de la compañía?
- ¿Cómo se comportó el mercado del *retail* farmacéutico en los últimos 5 años?
- ¿Cuáles son los principales desafíos de la empresa actualmente?

Aspectos particulares de ciberseguridad

- ¿Cuál considera que es el principal activo de la empresa?
- ¿Qué importancia posee la información digital en su trabajo diario?
- ¿Posee algún conocimiento de las nociones de ciberseguridad/seguridad informática, ciberincidentes y ciberataques?
- ¿La compañía ha sufrido algún tipo de pérdida, robo de información digital o acceso indebido de terceros a recursos corporativos?
- En caso de que la respuesta a la pregunta anterior fuera positiva, ¿ha denunciado o informado a las autoridades el hecho? Si no, ¿por qué?
- ¿Cree que la empresa puede ser afectada por este tipo de incidentes?
- ¿Qué impacto piensa que un ciberincidente podría generar en la firma?
- ¿Toman algún tipo de recaudos frente a los ciberincidentes? ¿Qué medidas de seguridad informática implementan?

- ¿Cómo definiría el presupuesto asignado a cuestiones de ciberseguridad, en relación a otros aspectos de la organización (p. ej.: marketing, atención al cliente, etc.)?
- ¿La compañía realiza capacitaciones (charlas, reuniones, etc.) sobre temas ligados a la seguridad informática?
- ¿Cuenta la empresa con un área de seguridad informática? ¿y, de sistemas? En ambos casos, ¿cuáles son sus principales tareas?
- ¿Implementan medidas de seguridad informática para proteger su información digital? En caso de que la respuesta sea negativa, ¿cuál es el motivo?
- ¿Existen procesos de seguridad informática definidos? ¿Realizan análisis de los riesgos informáticos a los que se encuentra expuesta la compañía?
- ¿Trabajan con algún proveedor de servicios de ciberseguridad?
- ¿Se asesoran con consultores en materia de seguridad informática?

1.2 Preguntas guía: Especialista en ciberseguridad (*Executive Director* de Ciberseguridad en EY Argentina, Nicolás Ramos)

- ¿Qué hacen las PyMEs en materia de ciberseguridad?
- ¿Existe algún tipo de regulación en seguridad informática para las empresas de *retail* en Argentina?
- ¿Por qué crees que es importante el tratamiento de la seguridad informática en el ámbito de *retail*?
- ¿Cuáles son las medidas que recomienda a las PyMEs de la industria de *retail* comenzar a implementar en seguridad informática?
- ¿En qué consiste una auditoría en ciberseguridad?

Anexo 2: Actividades no incluidas dentro de la categoría PyME

T	SERVICIOS DE HOGARES PRIVADOS QUE CONTRATAN SERVICIO DOMÉSTICO
U	SERVICIOS DE ORGANIZACIONES Y ÓRGANOS EXTRATERRITORIALES
O	ADMINISTRACIÓN PÚBLICA, DEFENSA Y SEGURIDAD SOCIAL OBLIGATORIA
R 920	SERVICIOS RELACIONADOS CON JUEGOS DE AZAR Y APUESTAS

Fuente: Resolución 103E-2017 – elaboración personal

Anexo 3: Ejemplo de *Phishing*

Fuente: corresponde a un caso real de *phishing* a través de correo electrónico enviado al autor de la presente investigación. En él se pueden observar los elementos que se repiten en esta técnica de engaño.