UNIVERSIDAD TORCUATO DI TELLA

Master of Business Administration

Año 2014

ESTUDIO DE MEDIDAS DE SEGURIDAD DE LA INFORMACION PARA SER APLICADAS EN MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS

Autor: Freyre, Carlos Alfredo

Tutor: Dickman, Ricardo

Lugar: Ciudad Autónoma de Buenos Aires

Fecha: Mayo 2016

UNIVERSIDAD TORCUATO DI TELLA

AGRADECIMIENTOS

A mis hijos Ezequiel, Letizia, Cecilia y Sabrina, mis padres y hermanas,
por ser la inspiración constante en mi vida.

A Belén, Christian, Leandro, Marcos y Miguel,
compañeros del Grupo 4% del MBA 2014-15 y desde ese entonces amigos de la vida,
por las vivencias compartidas estos años.

A los Profesores Ramiro Montealegre y Vanessa Welsh,
y en su nombre al resto de los docentes, personal administrativo de la UTDT y tutor,
por la dedicación durante este tiempo.

A los compañeros de trabajo y en especial a la Dra. Graciela Núñez,
por el aliento y apoyo continuo que he recibido de parte de ellos.

UNIVERSIDAD TORCUATO DI TELLA

RESUMEN

La utilización de las Tecnologías de la Información y las Comunicaciones (TICs) ha llevado a las empresas a tener que actualizarse dando un giro radical en la forma de llevar a cabo los negocios, y para ello han incorporado a sus operaciones diarias herramientas informáticas y sistemas de información que les permitan operar más eficientemente, como factor de ventaja competitiva. De allí que en la actualidad, la mayor parte de la información de una empresa reside en equipos informáticos, redes de comunicación de datos, dispositivos móviles y soportes de almacenamiento.

Existen riesgos físicos y naturales que pueden afectar el adecuado funcionamiento de la tecnología utilizada y, por ende, la continuidad de las operaciones de negocio. También existen riesgos lógicos, intrínsecos a la propia tecnología empleada, que pueden afectar a la información y sus características. Espionaje cibernético, virus informáticos, robos de identidad y accesos no autorizados, son algunas de las amenazas que pueden acabar con la confianza de clientes y la imagen de las empresas.

En este trabajo intentamos aportar información sobre el estado de situación en el conocimiento y aplicación de medidas de Seguridad de la Información que permitan proteger adecuadamente la información administrada por Micro, Pequeñas y Medianas Empresas, seleccionando para ello una muestra y entrevistando a representantes de 16 empresas ubicadas en la Ciudad Autónoma de Buenos Aires y el primer cordón del Conurbano Bonaerense, de sectores de industria y servicios, con una antigüedad de al menos 15 años.

Todas las empresas entrevistadas señalan una amplia utilización de la tecnología, sistemas y herramientas informáticas en sus operatorias diarias, gestionando la información, considerada principal instrumento en las decisiones de negocio y, en general, declaran un notable grado de implementación de medidas básicas de seguridad que protegen los recursos informáticos utilizados,

No obstante, se arribó a la conclusión que si bien estas empresas le dan suma importancia a la atención de sus procesos críticos de negocio, de proteger la información que administran, como así también la consideración de los compromisos asumidos con sus clientes, existen aspectos fundamentales y vitales para el funcionamiento del negocio

UNIVERSIDAD TORCUATO DI TELLA

relacionados con Seguridad de la Información que no son atendidos debidamente.

Palabras claves

Tecnología de la Información y las Comunicaciones, Seguridad de la Información, Micro, Pequeñas y Medianas Empresas, Riesgos.

UNIVERSIDAD TORCUATO DI TELLA

ÍNDICE

UNIVERSIDAD TORCUATO DI TELLA

UNIVERSIDAD TORCUATO DI TELLA

UNIVERSIDAD TORCUATO DI TELLA

1. GENERAL

1.1. INTRODUCCION

La utilización de nuevas tecnologías, siendo sus estrellas principales Internet y las telecomunicaciones, ha favorecido las comunicaciones personales, el intercambio y diversidad cultural, tanto desde aspectos de relaciones sociales, como profesionales y comerciales, como también entre países, Fridman (2005).

Estas nuevas herramientas tienen un alcance e impacto profundo en el trabajo, el ocio y el conocimiento compartido a nivel mundial. La visión del mundo mutó a una nueva dimensión, global y digital, por encima de países, comunidades y localidades, donde ya no existen fronteras. Expresiones tales como autopista de información, globalización, economía del conocimiento, y otras, forman parte de nuestro vocabulario actual.

También la producción económica se está organizando en torno a las nuevas redes informáticas; empresas, clientes y proveedores aumentan su colaboración y control de los procesos de generación de valor, en beneficio de su competitividad. Los recursos denominados de Tecnología de la Información y la Comunicación (TICs)[1] constituyen ya el principal activo para lograr y mantener la eficiencia de la gestión general y de cada una de las funciones específicas en las organizaciones.

Las empresas, en sus intercambios de productos y servicios, organización y alineamiento empresarial, tienen la facilidad de contar con mayor detalle de información de gestión, trazabilidad y registración simplificada en la línea misma de montaje, utilización de dispositivos inteligentes como interfaces móviles, personalización en línea[2] de la relación con clientes y proveedores de todo el mundo, y demás beneficios e impronta que han aportado las nuevas tecnologías en el mundo actual de los negocios.

No obstante este apego a las TICs que brindan tantas herramientas para generar ventajas competitivas tan importantes, trae aparejado consigo riesgos intrínsecos derivados del mismo entorno. A medida que las organizaciones fueron consolidando sus procesos en

[1] Concepto que involucra el conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de la información, involucrando tanto la infraestructura tecnológica de una organización como también la de las personas que lo utilizan.

UNIVERSIDAD TORCUATO DI TELLA

los sistemas informáticos, su supervivencia termina basándose netamente sobre la misma tecnología aplicada la cual dista enormemente de ser perfecta e inviolable. Desde desastres naturales como incendios, inundaciones o terremotos, pasando por situaciones no intencionales como fallas eléctricas, tecnológicas o errores humanos, hasta acciones deliberadas como espionaje, falsificación, fraudes, sabotaje o venta de información, pueden bastar para generar una grave crisis. Pero no sólo las causas externas son los únicos factores a los cuáles habrá que temer, por el contrario, la mayor cantidad de amenazas suele provenir del propio personal de la compañía, usuarios internos que cometen errores involuntarios o directamente delitos malintencionados, Collazo & Saroka (2010).

En esta nueva dimensión para el intercambio de información, debemos ser conscientes que existen personas que utilizan estas tecnologías y la información que allí se recolecta con el objeto de causar daño, aprovecharse u obtener algún rédito. Casi ninguna de estas amenazas son nuevas, por el contrario, ya existían tiempo atrás; el hecho es que los malhechores también fueron perfeccionándose y tecnificándose con la utilización de estas nuevas herramientas y sólo fueron adaptadas a la nueva dimensión tecnológica. Y por supuesto las empresas no están exentas de tales amenazas, todo lo contrario, son uno de los objetivos principales debido a la posibilidad de producir fraudes y recaudar dinero fácil. La simple introducción de un *malware*[3] en alguno de los equipos informáticos a través de un correo electrónico podría ocasionar pérdidas parciales o totales de los datos gestionados, modificaciones no autorizadas de la información almacenada, y hasta cambios significativos en el comportamiento de los sistemas y/o recursos/dispositivos interconectados, pudiendo llegar a alterar drásticamente la vida diaria de la organización, de una comunidad o región, o mismo de un país.

Existe un área de la informática que se especializa en la protección de las plataformas tecnológicas y de la información que en ellas se gestiona. La Seguridad de Tecnologías de la Información, o simplemente Seguridad de la Información, dispone de estándares, protocolos, métodos, reglas, mejores prácticas y herramientas que permiten minimizar posibles riesgos informáticos y esas amenazas a las que nos vemos expuestos con el uso

[2] En el ámbito de la informática, es utilizado para nombrar a algo que está conectado o a alguien que está haciendo uso de algún recurso en red.

UNIVERSIDAD TORCUATO DI TELLA

de las nuevas tecnologías.

La implementación de medidas apropiadas de seguridad de la información en organizaciones de envergadura habitualmente requiere de recursos profesionales idóneos y la adquisición de herramientas tecnológicas y/o de software, incurriendo en gastos que estarán directamente relacionados a las características de la empresa, las plataformas tecnológicas utilizadas y en función de la industria o negocio que se trate. Vale la pena mencionar, que existen mercados en los cuáles están regulados/controlados -como ser el financiero- y requieren aplicar tales medidas de seguridad, u otros que por normas propias, internas/corporativas, decanta también en la obligatoriedad de su implementación.

Si nos referimos a empresas de menor porte, aquellas que se encuentran entre las definidas como Micro, Pequeñas y Medianas Empresas (de aquí en adelante las denominaremos MiPyMEs), que habitualmente disponen de menores o acotados presupuestos económicos destinados a la adquisición e instalación de tecnología de la información, resultará interesante conocer ¿en qué medida las diferentes prácticas de Seguridad de la Información son conocidas?, y ¿hasta qué nivel son llevadas a cabo para la protección de sus activos y recursos de información?.

En términos generales, de acuerdo a la estadística y la metodología seguida por la Fundación Observatorio PyME (FOP) y en línea con los estándares internacionales, una PyME es una empresa que tiene entre 10 y 200 empleados. El 75% de las pequeñas empresas (10 a 50 empleados) y el 92% de las medianas (51 a 200 empleados) están conformadas jurídicamente como sociedades del tipo SRL o SA (Fundación Observatorio Pyme, 2015).

Para ello se seleccionaron 16 empresas consideradas MiPyMEs, correspondientes a la Ciudad Autónoma de Buenos Aires y el primer cordón del Conurbano Bonaerense, pertenecientes a los sectores de industrias y servicios, con una antigüedad de al menos 15 años en el mercado.

El pre-requisito de la antigüedad intenta considerar la necesidad de incorporación de recursos TICs que tales empresas seguramente hayan requerido, a medida fueron

[3] Software malicioso cuyo objetivo es infiltrarse, tomar control de un recurso tecnológico, efectuar algún

UNIVERSIDAD TORCUATO DI TELLA

evolucionando sus procesos por cambios producidos en el desarrollo de nuevas formas de hacer negocios a través de las herramientas y redes informáticas.

Se desarrollaron entonces entrevistas que permitieron extraer datos descriptivos y conocer la situación de las MiPyMEs seleccionadas en materia de Seguridad de la Información, contrastando la comparación de los resultados obtenidos con el rendimiento potencial o deseado según las mejores prácticas y estándares internacionales.

La investigación desarrollada describe dicha situación y permite arribar a conclusiones, a través del análisis de resultados, la observación participante y la utilización de fuentes externas, como ser bibliografía, informes y reportes de consultoras y empresas internacionales relacionados con el tema objetivo.

En tal sentido, el objetivo del presente trabajo propone es llevar a cabo un estudio análisis de la situación actual referido a los niveles de exposición a riesgos relacionados con Seguridad de la Información con que permitan determinar estrategias de mejora en cuanto a la protección de la información en que administran las MiPyMEs.

Adicionalmente, como objetivo secundario, se incluye una guía con los principales conceptos de uso y recomendaciones de buenas prácticas relacionadas para ser consideradas en una adecuada implementación de Seguridad de la Información.

daño y/u obtener información y reenviarla.

2. MARCO TEÓRICO

CAPITULO 1: CARACTERISTICAS GENERALES DE MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS

En este capítulo se describe en forma sintética los aspectos relacionados con las características esenciales de las micro, pequeñas y medianas empresas, las diferentes definiciones existentes según el contexto donde se encuentren, considerando la Unión Europea, Mercosur y la República Argentina, sus ventajas y desventajas, y las capacidades necesarias para la creación de valor como empresas exitosas.

1.1. Definición de MiPyME

La Unión Europea considera empresas a aquellas entidades que ejerzan una actividad artesanal u otras actividades a título individual o familiar, las sociedades de personas y las asociaciones que ejerzan una actividad económica de forma regular.

El tamaño de una empresa representa un rasgo característico del desarrollo de la misma, interpretándolo como el resultado de un conjunto de variables que interactúan y conforman su propia organización. Sin embargo, debe tenerse en cuenta que las empresas no siempre crecen, su tamaño suele ser el resultado de un proceso de ajuste a las condiciones ambientales, estructurales e institucionales de cada economía (Fundación Observatorio Pyme, 2013).

En líneas generales, el tamaño de una empresa puede medirse por el volumen de facturación anual o la cantidad de trabajadores que desempeñan su función en ellas. Una adecuada clasificación de las empresas permitirá comprender determinadas características y necesidades del sector, factores relacionados tanto con el diseño y ejecución de las políticas públicas por parte de los gobiernos, como también los acuerdos comerciales que se establecen en el sector privado.

UNIVERSIDAD TORCUATO DI TELLA

Una MiPyME "es una unidad económica, dirigida por su propietario de forma personalizada y autónoma, de pequeña dimensión en cuanto a número de trabajadores y cobertura de mercado"[4].

El desempeño de las MiPyMEs cumple un rol fundamental, ya que con su aporte produciendo y/u ofertando bienes y servicios, constituyen un eslabón importante de la actividad económica en un país. La literatura sobre las MiPyMEs las señala como referencias a unidades de análisis con propiedades particulares, como generadoras de empleo, contribución al desarrollo regional, aporte al crecimiento exportador de los países, promotoras de la innovación tecnológica, de rápidas reacciones ante los cambios, con mayores flexibilidades de adaptación, entre otras.

La MiPyME, que usualmente era considerada una empresa de segunda, resulta ser en la actualidad reconocida como el motor de la economía de los países, especialmente aquellos en vías de desarrollo, por su aporte al empleo y al bienestar económico (Maristany, 2006).

Existen diferentes definiciones para establecer los límites entre micro, pequeñas y medianas empresas, aún persisten las diferencias entre países de nivel semejante de desarrollo industrial. A menudo se observan existencias de MiPyMEs organizadas en distritos industriales, interrelacionados de forma horizontal o verticalmente entre las empresas, y conformando verdaderos parques o polos productivos.

En el año 2003, la Comisión Europea establece sus diferencias fijando un método transparente para ubicar a cada tipo de empresa, distinguiendo en cantidad de empleados y facturación anual (FIGURA Nº 1).

FIGURA Nº 1: Definición de MiPyME en la Unión Europea

Categoría de empresa	Cantidad de empleados efectivos	Volumen de negocio	Balance general
Mediana	<250	<= 50 m €	<= 43 m €
Pequeña	<50	<= 10 m €	<= 10 m €

[4] Fuente. Crear, Agencia de Desarrollo del Ministerio de Economía del Gobierno de Rio Negro: http://www.crear.rionegro.gov.ar/noticias/item/26.

UNIVERSIDAD TORCUATO DI TELLA

Micro	<10	<= 2 m €	<= 2 m €

Fuente: Comisión de las Comunidades Europeas, Artículo 1° de la Recomendación del 6-5-2003 sobre la definición de micro, pequeñas y medianas empresas.

Otra definición es la otorgada por los países del Mercosur. En el año 1992, un grupo de trabajo integrado por representantes de Argentina, Brasil, Paraguay, Uruguay y Venezuela, desarrollaron para el Mercosur un criterio general el cual define la siguiente categorización de empresas (FIGURA N°2).

FIGURA Nº 2: Definición de MiPyME para el Mercosur

Categoría de empresa	**Cantidad de empleados**	**Volumen de ventas**
Mediana	<200	<= 10.000.000 (U$S)
Pequeña	<50	<= 2.000.000 (U$S)
Micro	<10	<= 400.000 (U$S)

Fuente: Mercosur/GMC/Resolución a 59/98.

En este caso, el tamaño de la empresa queda definido bajo los dos criterios conjuntos: cantidad de empleados y volumen de ventas anual. Sin embargo, el criterio general definido explicita que prevalece el criterio de ventas anuales, mientras que el de empleados es utilizado como referencia.

1.2. Definición de MiPyMEs en Argentina

Según Boletín Oficial de la República Argentina, Resolución 11/2016 de la Secretaría de Emprendedores y de la Pequeña y Mediana Empresa, perteneciente al Ministerio de Producción, en el cual se afirma que las MiPyMEs son un verdadero motor de creación de empleo y valor en la economía y son los actores más dinámicos en los procesos de desarrollo económico, y que a los fines de dimensionar el universo de las mismas al interior de cada sector de actividad de la economía argentina, se han considerado límites de facturación por sub-segmento cuyas ventas totales anuales expresadas en millones de

UNIVERSIDAD TORCUATO DI TELLA

pesos ($) no superen determinados valores, los cuales son diferentes en función de los sectores industriales, servicios y comercio (FIGURA Nº 3).

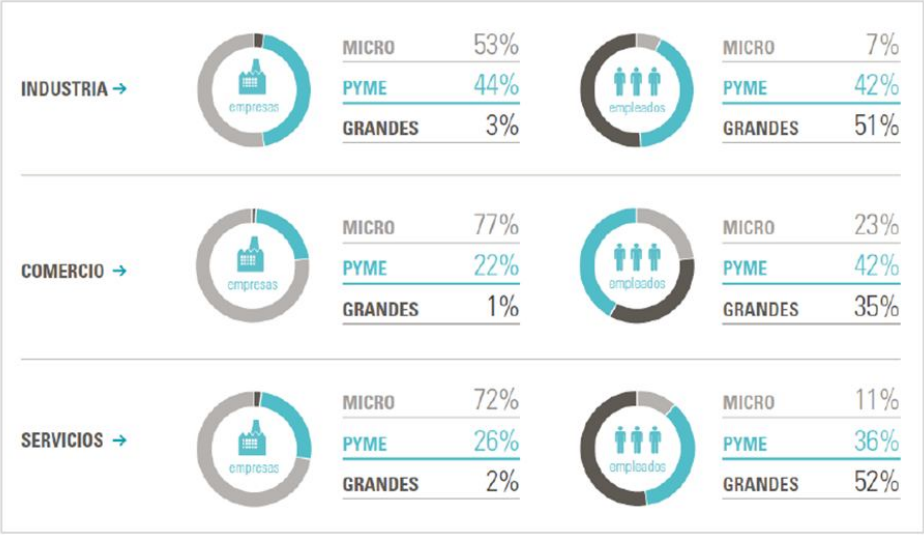
FIGURA Nº 3: Definición de MiPyME en la Argentina

Categoría de empresa	Agrope-cuario	Industria y Minería	Comercio	Servicios	Construc-ción
Mediana	<= 160 m $	<= 540 m $	<= 650 m $	<= 180 m $	<= 270 m $
Pequeña	<= 13 m $	<= 45,5 m $	<= 55 m $	<= 15 m $	<= 22,5 m$
Micro	<= 2 m $	<= 7,5 m $	<= 9 m $	<= 2,5 m $	<= 3,5 m $

Fuente: Boletín Oficial de la República Argentina, Resolución 11/2016 de la Secretaría de Emprendedores y de la Pequeña y Mediana Empresa.

En Argentina, las MiPyMEs representan una parte importante del entramado productivo nacional (FIGURA N° 4).

FIGURA Nº 4: Relevancia de las empresas según su tamaño



Fuente: Observatorio de Empleo y Dinámica Empresarial, Ministerio de Trabajo, Empleo y Seguridad Social (Fundación Observatorio Pyme, 2013).

UNIVERSIDAD TORCUATO DI TELLA

El grupo de las pequeñas y medianas empresas aporta una importante participación en relación a la cantidad de empresas existentes como personal empleado en las mismas, siendo el sector industrial donde mayor participación alcanzan con un 44% del total de las empresas industriales empleando al 42% del total de asalariados. Si bien en el sector de comercio y servicios la incidencia en la cantidad de empresas no es tan participativa, con el 22% y 26% sobre el total de empresas, su relevancia es significativa relacionada con la cantidad de empleados, con el 42% y 36% respectivamente. Por otra parte, se observa que si bien el nivel de micro empresas en términos de cantidad de empresas es de mayor participación en los tres sectores de industria, comercio y servicios, su relevancia es inversamente proporcional en cuanto a la cantidad de personas que emplea.

No obstante, considerando los tres grupos que conforman las MiPyMEs en Argentina, se aprecia la importante participación que tienen en el desarrollo productivo a nivel nacional.

1.3. Creación de valor en las MiPyMEs

Las MiPyMEs presentan ventajas y desventajas por su tamaño, en su formación y desarrollo (Maristany, 2006). Dentro de las ventajas se pueden enumerar:

- Poseen una reducida estructura organizativa que permite el contacto directo entre los dueños y el personal de la empresa.
- Los dueños suelen tener conocimiento del área en la que operan.
- Poseen una infraestructura sencilla que la hace más ágil y menos pesada que a las grandes empresas.
- Los procesos de gestión suelen ser más sencillos.
- Son flexibles al mercado de oferta y demanda, adaptándose rápidamente.
- Producen y venden artículos a precios competitivos.
- Existe contacto cercano, directo y personal con los clientes.
- Desarrollan pedidos especializados y/o personalizados a requerimiento.
- Asimilan y adaptan con facilidad y creatividad las tecnologías disponibles.

Referido a las desventajas que tienen se pueden mencionar:

- No tiene gran respaldo económico-financiero.

UNIVERSIDAD TORCUATO DI TELLA

- Poseen dificultades para la obtención de créditos, pagando tasas más caras.
- Poseen falta de información respecto del mercado al no poder pagar estudios específicos.
- No pueden aprovechar las economías de escalas.
- Capacidades limitadas a nivel tecnológico y publicitario.
- Suele haber falta de especialización a nivel superior, debido a no poder pagar sueldos caros a supervisores en puestos claves.
- Tienen dificultades de encontrar mano de obra especializada.
- Habitualmente sus procesos no siguen lineamientos ni patrones, recreándolos a cada momento.

Existen factores que conllevan a las MiPyMEs a su crecimiento y expansión, como otros que pueden llevar a su estancamiento y hasta extinción. No es posible establecer claros criterios que permitan condicionar estos factores de manera favorable para lograr una mejora deseada, ya que las condiciones son muy distintas según los países, el momento y contexto en el que se encuentren, y de la habilidad que posean para obtener provecho de las ventajas y/o revertir las desventajas que posean.

Si las empresas se focalizan en la creación de valor, es posible encontrar elementos que lo favorecen, como ser: 1) la rentabilidad referido a la capacidad actual de la empresa de generar retornos superiores al costo del capital, 2) las oportunidades de crecimiento que pueden tener, y 3) la capacidad de explotar una ventaja competitiva para mantener en el tiempo un retorno económico por encima del costo del capital.

Maristany (2006) hablando de la MiPyME menciona:

> Lo que suelen hacer estos *entrepreneurs* clásicos es seguir su intuición. Esto ha producido grandes éxitos en la historia de las empresas. Pero cada vez es más difícil en la compleja sociedad actual manejarse solamente por la intuición. Tiene que haber un método, una racionalidad que permita reasegurarse sobre la continuidad de la organización (p. 55).

Entre los varios obstáculos que habitualmente se deben superar en el surgimiento y crecimiento de una MiPyME, mencionado ya como desventaja, corresponde con la información asimétrica como principal factor asociado con las dificultades que se les

UNIVERSIDAD TORCUATO DI TELLA

presentan para acceder al crédito bancario (Consejo de Financiamiento de Pymes y Emprendimiento, 2015[5];Lapelle, 2007).

Este racionamiento en el que se verían perjudicadas las MiPyMEs significa que el mercado no es capaz de financiar sus proyectos por más que su capacidad de repago fuese mayor, debiendo entonces tener que recurrir a otros tipos de financiamiento, seguramente a mayores tasas, o descartando la idea original del proyecto. Si bien éste podría ser visto con un problema de índole general, la consideración del tamaño de la MiPyME tiene implicancias de correlación directa con la búsqueda de información que las entidades crediticias pueden obtener de ella. "Hay indicios de que la magnitud del fenómeno de la asimetría informativa aumenta en la medida en que crece la heterogeneidad de los proyectos de inversión y, por supuesto, cuando más difícil es obtener información acerca de los mismos" (FIEL, 1996, p. 170).

Otro de los obstáculos a superar para lograr el crecimiento de una empresa, se condice con la asignación de importantes recursos destinados a la investigación y el desarrollo, a fin de permitir mantener alguna posición dominante en los mercados, como también la adquisición y el aprovechamiento de los avances tecnológicos ya existentes en otros países y/o empresas, son barreras que se imponen a las MiPyMEs, principalmente en los países en desarrollo.

Por último, las empresas que fracasan se caracterizan porque se encuentran en una desventaja competitiva. Suele suceder que se les dificulta cambiar sus estrategias y estructuras para adaptarse a las cambiantes condiciones de mercado. Las capacidades son difíciles de cambiar debido a que cierta rigidez dentro de los procesos establecidos de toma de decisiones estratégicas y administración de la empresa. Superar las barreras para el cambio dentro de una organización es uno de los requerimientos claves para mantener una ventaja competitiva (Hill & Gareth, 1996).

[5] CONSEJO DE FINANCIAMIENTO DE PYMES Y EMPRENDIMIENTO (2015). Estrategia para Financiamiento de las PYMES y el Emprendimiento, Recuperado el 25 de mayo de 2016 de http://www.economia.gob.cl/wp-content/uploads/2015/09/Informe-Final-Estrategia-para-Financiamiento-de-las-Pymes-y-el-Emprendimiento.pdf

UNIVERSIDAD TORCUATO DI TELLA

CAPITULO 2: IMPORTANCIA EN LA UTILIZACION DE TECNOLOGIA DE LA INFORMACION Y LAS COMUNICACIONES

En este capítulo se describe la importancia que ha ganado una buena gestión de la información que administran las organizaciones, y la dependencia existente con las tecnologías y sistemas de información, como herramientas necesarias para un eficaz tratamiento y arribo de decisiones gerenciales.

2.1. La información, principal recurso de una organización

La Era de la Información[6] es el nombre que recibe el período de la historia de la humanidad que está relacionado con la evolución y utilización de las Tecnologías de la Información y las Comunicaciones (TICs). Las últimas décadas transcurridas se han caracterizado por el acelerado proceso de desarrollo tecnológico que se produjo a nivel mundial, siendo su principal elemento diferenciador la interconectividad lograda a través del uso de Internet. Hoy ya es una forma de hacer negocios y fuerza a estar presente allí de una u otra manera.

Por otra parte, en la actualidad, la información es un recurso clave y vital para toda organización, y especialmente importante en el ambiente de los negocios, cuya interconexión va creciendo día a día, justamente de la mano de la tecnología y las comunicaciones (Collazo & Saroka, 2010).

La información genera la creación de conocimiento, que a su vez genera rápidas acciones estratégicas creando ventajas competitivas. En este sentido, los recursos informáticos se han constituido en un activo importante para la organización.

Las estructuras de las organizaciones cada vez se están basando más en redes horizontales y planas, donde la información fluye basada en la necesidad de saber, siendo las redes de comunicaciones digitales el medio más utilizado para ello. Una buena administración de estos recursos resulta fundamental para cualquier empresa, con ello puede lograr un alto nivel competitivo, significando la diferencia entre el éxito o el fracaso de su gestión.

[6] También conocida como Era Digital o Era Informática.

UNIVERSIDAD TORCUATO DI TELLA

Resulta entonces que el objetivo principal de la información gestionada en una empresa es la de apoyar a la toma de decisiones gerenciales, siendo la información la materia prima de la actividad ejecutiva.

En este sentido, las empresas se han ajustado y actualizado, dejando de la lado su visión vertical y tradicional del uso de la informática, alineándose a las nuevas tecnológicas emergentes, integrando sistemas de información con las reglas del negocio, incorporando los niveles organizacionales en la cadena de decisión; transformando así las tecnologías de la información en las principales herramientas gerenciales utilizadas para incrementar la eficacia de su organización y añadir valor a su actividad (Monforte, 1994).

Es así como las habilidades gerenciales en cuanto a la resolución de problemas y decisiones de negocio han migrado a la destreza relacionada con el usufructo de las nuevas herramientas tecnológicas e informáticas, colaborando en la recolección, procesamiento, análisis y generación de resultados en la toma de decisiones. Es así como la información de la que dispone el nivel gerencial de una empresa pasa a entonces determinar la calidad de sus decisiones tomadas.

”La información es un recurso de la organización, tal como el dinero, el personal y el equipo. Más aún, la información es el recurso crítico, pues los restantes recursos no pueden ser administrados sin ella” (Collazo & Saroka, 2010, p. 49).

Es necesario hacer la salvedad que la información existe de muchas formas, puede estar impresa, escrita en papel, almacenada electrónicamente, puede ser transmitida por correo postal o utilizando los medios electrónicos actuales, estar presentada en fotos o videos, y hasta es transmitida verbalmente.

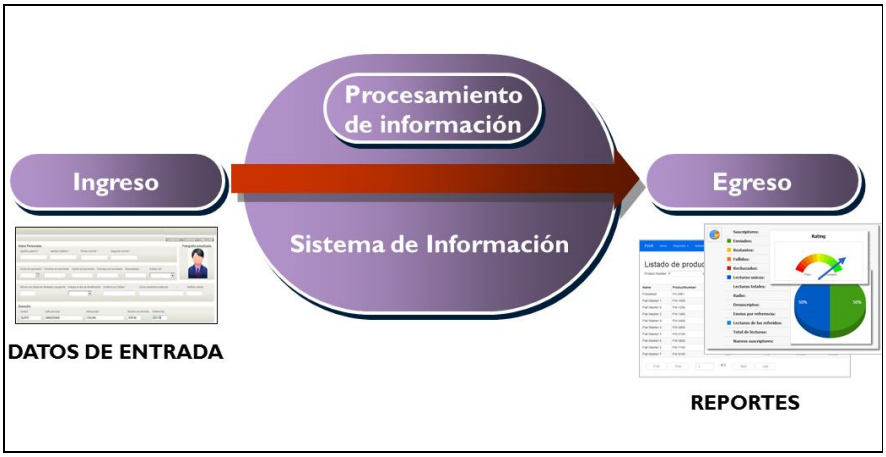
2.2. Los sistemas de información como herramientas gerenciales

Se denomina sistema de información a un conjunto de aplicaciones de negocios, procesos, tecnologías y software, interrelacionados, orientados a la administración y tratamiento de datos e información, que dan lugar a información más elaborada que permite su distribución y accesibilidad de manera más adecuada en una organización, generados para cubrir una necesidad u objetivo definido.

UNIVERSIDAD TORCUATO DI TELLA

Podemos entender entonces un sistema de información como un proceso transformador de datos[7] o conjunto de datos de entrada, en uno o varios productos o datos de salida, para brindar información a quienes operan y toman decisiones, la información que necesiten para el desarrollo de sus funciones (FIGURA N° 5).

FIGURA Nº 5: Esquema del modelo de un sistema de información



Fuente: Elaboración propia.

Bajo este contexto, la información en su carácter funcional, representa el significado de un dato o conjunto de datos seleccionados, evaluado por una persona, en un momento dado, con un fin específico.

La información hace referencia a un conjunto de datos estructurados, seleccionados y evaluados, para un usuario, en una situación, momento y lugar dado. Mientras los datos no sean evaluados, serán sólo datos, una representación simbólica, de allí el objetivo de los sistemas de información, que convierten datos en información.

Es posible afirmar entonces, que tanto los datos como la información procesada son únicos para cada organización. Cada una tiene una forma particular para gestionar su tratamiento, que incluirá la recolección, almacenamiento, modificación, procesamiento y hasta la misma destrucción. Una adecuada gestión de datos/información por parte de las organizaciones constituye un factor clave competitivo, así como la destrucción o

[7] Representación simbólica de un atributo o variable cuantitativa o cualitativa, que describen hechos empíricos, sucesos y/o entidades

UNIVERSIDAD TORCUATO DI TELLA

alteración malintencionada podría afectar la rentabilidad, imagen y reputación de la empresa, hasta provocar su desaparición.

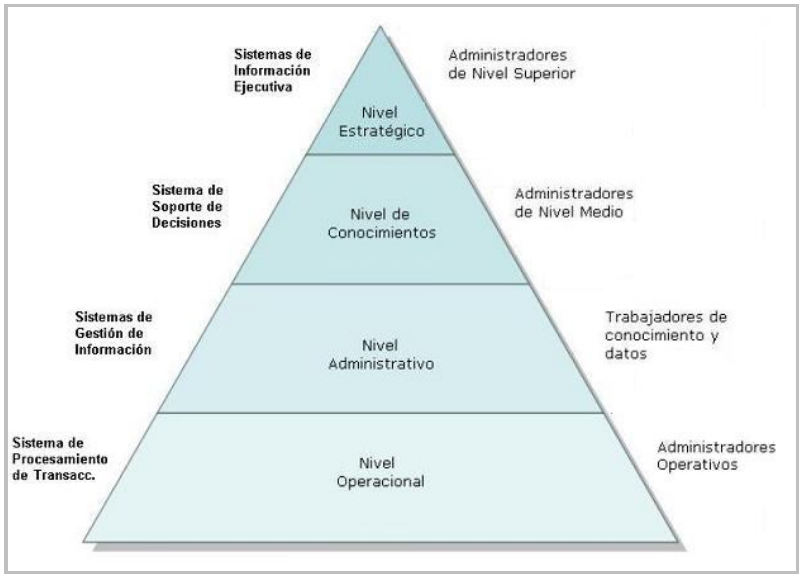
En términos generales, desde el punto de vista empresarial, los sistemas de información se pueden clasificar según el modelo de la pirámide de cuatro niveles (Euromed Marseille School of Management)[8], considerando las siguientes clasificaciones (FIGURA N° 6):

- Sistemas de información ejecutiva: se encuentran en el tope de la pirámide, a nivel estratégico, utilizados por el nivel directivo, permite analizar el entorno en el que opera la compañía, identificando tendencias a largo plazo y definiendo planes de acción en consecuencia. La información procesada en este nivel provee de los sistemas de información de niveles inferiores y también de fuentes externas.
- Sistemas de soporte de decisiones: puede ser visto como un sistema base de conocimiento, utilizado por gerentes y jefes de nivel senior, para analizar la información de la compañía, realizar proyecciones y simular situaciones ante diferentes alternativas de decisiones a tomar.
- Sistemas de gestión de información: comúnmente relacionados con los sistemas administrativos contables, son aquellos administrados por niveles medios de jefaturas y supervisión, basados en información interna y utilizados para la gestión diaria, brindan información para evaluar la performance de la compañía.
- Sistemas de procesamiento de transacciones: son los que se encuentran en la base de la pirámide, a nivel operacional, utilizados por usuarios finales[9], ya sea operarios o empleados de mostrador, que proveen el ingreso de datos principales necesarios para la gestión de las operaciones. Siendo estos datos usualmente obtenidos a través de interfaces automáticas o semiautomáticas en tareas operativas básicas.

[8] Euromed Marseille School of Management: http://www.chris-kimble.com/Courses/World_Med_MBA/Types-of-Information-System.html
[9] Persona o grupo de personas que manipulan de manera directa un producto de software.

UNIVERSIDAD TORCUATO DI TELLA

FIGURA Nº 6: Clasificación de los sistemas de información[10]



Fuente: Euromed Marseille School of Management.

De esta forma, se aprecia la manera en que los diferentes sistemas de información, a diferentes niveles organizacionales, cumplen un rol decisivo en la vida de una empresa.

Finalmente, tanto la información como los sistemas de información que la administran, revisten un carácter de recursos estratégicos para el apoyo a la toma de decisiones gerenciales y de negocios.

[10] Euromed Marseille School of Management: http://www.chris-kimble.com/Courses/World_Med_MBA/Types-of-Information-System.html

CAPITULO 3: PROTEGIENDO LA INFORMACION ADMINISTRADA

En este capítulo se describen los conceptos más relevantes relacionados con la necesidad de proteger la información administrada por las organizaciones, los estándares internacionales, las leyes y reglamentaciones, relacionadas con las mejores prácticas de implementación de adecuados entornos de seguridad y control de la información.

3.1. Amenazas y vulnerabilidades asociadas a las TICs

Considerando entonces a la información y su tratamiento como recursos que revisten un carácter de importancia relevante en las organizaciones, y la exposición a la gran variedad de amenazas y vulnerabilidades que se generan incansablemente asociadas con la misma evolución de la tecnología que se emplea para su tratamiento, será necesario gestionar adecuados ambientes de control y resguardo a fin de evitar situaciones que pudieran poner en peligro la vida de la propia empresa.

Se entiende por amenaza el evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales (FIGURA N° 7).

FIGURA Nº 7: Tipos de amenazas

Fuente: Elaboración Propia.

UNIVERSIDAD TORCUATO DI TELLA

Se consideran tipos de incidentes los siguientes (Ardita, 2008):

- Aquellos que causen un daño físico en las instalaciones o equipos, como fuego, humo o daños por agua.
- Aquellos que afecten de forma indirecta la posibilidad de acceso a las instalaciones, como evacuación de emergencia por amenazas de bomba, o amenazas externas tales como incendios en instalaciones cercanas, fuga de gases tóxicos, manifestaciones, etc.
- Los desastres regionales no previstos o inesperados, tales como inundaciones, huracanes o fuertes tormentas eléctricas, que pueden causar daños en las instalaciones y equipos, o impedir el acceso normal al personal encargado aunque las instalaciones se encuentren intactas.
- Cualquier incidente externo que pudiera potencialmente causar una interrupción de las operaciones del negocio, tales como la pérdida de los servicios de suministro eléctrico o telecomunicaciones.
- Cualquier incidente que afecte al funcionamiento de alguna de las plataformas tecnológicas utilizadas, ya sea tanto problemas en el hardware como en el software, incluyendo también fallas en las fuentes de alimentación, equipos de refrigeración, etc.
- Cualquier incidente que suponga la paralización de las actividades de la organización por motivos ajenos a la tecnología, tales como problemas laborales propios, de algún sector o que afecten al área geográfica donde se encuentra ubicada.

La misma tecnología, que se utiliza para desarrollar y alcanzar los principales objetivos de negocios planteados por las empresas, termina siendo una puerta de ingreso para los riesgos que atentan contra este logro. La gran dependencia de los procesos en la tecnología hace que la capacidad de cometer delitos y fraudes, adquieran nuevos matices en Internet, dando lugar a una nueva clasificación de delitos denominados cibernéticos.

La vulnerabilidad de los sistemas informáticos y la gravedad de los efectos relacionados con fraudes y desastres crecen día a día. Delitos cibernéticos asociados con la privacidad y confidencialidad de la información, tanto la que corresponde a los negocios de las

UNIVERSIDAD TORCUATO DI TELLA

empresas como la administrada relacionada con la de las personas, pasan a ser el desafío principal de aquellos que tienen la responsabilidad por su seguridad.

Según lo enunciado por Price Waterhouse Coopers (2014), en la Encuesta global sobre delitos económicos, el 51% de los 5.000 encuestados ha sido víctima de un delito económico y 1 de cada 3 informó que el riesgo de delito informático ha aumentado casi el 50% con respecto al año 2011.

Considerado uno de los mayores problemas a los que se encuentran las organizaciones, frente a los tipos de delitos informáticos, es que éstos afectan no sólo a los activos tangibles de las empresas, sino también a aquellos activos intangibles, el cual el nivel de madurez en la gestión de este tipo de riesgos se encuentra aún en un nivel muy básico. Temas como legislación sobre delitos informáticos, definición de propietarios y utilización de activos intangibles o pólizas de seguro que cubran este tipo de riegos, son algunos ejemplos que indican que el nivel de madurez recién está identificándose en los gobiernos y organizaciones (Sharma, 2007).

Para citar un ejemplo de delitos sobre activos intangibles, dentro de las amenazas y ciberataques generados se encuentran los denominados robo o pérdida de datos, caracterizados por afectar la información administrada por las organizaciones. Los *ransomware*, que en la actualidad son un tipo de campaña de ciberespionaje capaz de afectar a todo tipo de organización e individuos, son un tipo de software malicioso que se filtra e infecta la computadora, otorgándole permisos al ciberdelincuente para bloquear el equipo y encriptar[11] los archivos allí residentes, quitando el control de toda la información y datos almacenados, solicitando el pago de un rescate virtual para desbloquear el virus informático.

Según el informe de seguridad de la empresa Kaspersky Lab, en su *Security bulletin* menciona que en el año 2015 hubo cerca de 2 millones de notificaciones sobre infecciones relacionadas a este tipo de malware (ver Anexo I).

Por otra parte, las organizaciones destinan enormes sumas de dinero para almacenar y gestionar grandes cantidades de información que administran. El resguardo de la

[11] Proceso para transformar ilegible determinada información a través de la ejecución de algoritmos matemáticos.

información es el objetivo principal, independientemente del lugar en donde se encuentre registrada, ya sea en algún medio electrónico o físico (FIGURA N° 8).

FIGURA Nº 8: Lugares donde reside la información

Fuente: elaboración propia.

De acuerdo con el estudio realizado por Symantec (2012), en el reporte sobre el costo y manejo de la información empresarial, resultados América Latina, anualmente a nivel global, las MiPyMEs gastan en información un promedio de US$332,000 dólares, mientras que las grandes empresas invierten, en promedio, U$S38 millones de dólares por año en cuestiones relacionadas con el manejo de la información.

En el mismo reporte realizado por Symantec (2012), de acuerdo con las respuestas dadas por 500 profesionales de Tecnología de la Información en América Latina, señalan que aproximadamente el 50% del valor de sus organizaciones deriva de la información que poseen, y que las consecuencias por pérdida de dicha información empresarial sería catastrófico, debido a multas, menores ganancias, daño de la marca y/o pérdida de clientes (ver Anexo II).

Las consecuencias por pérdida de la información pueden afectar tanto a la organización, como a las terceras partes con las que puedan interactuar. Según el tipo de datos perdidos, los daños causados pueden oscilar entre el deterioro de la imagen institucional, pérdida de clientes, disminución de las ventas, y hasta sanciones financieras, que puedan

UNIVERSIDAD TORCUATO DI TELLA

surgir de regulaciones, multas por falta de cumplimiento de acuerdos contractuales y/o demandas judiciales.

Si la seguridad que se aplique, sólo se basa en medios técnicos será limitada, por lo tanto deberá ser respaldada por gestión y procedimientos de control que lo soporten. Es así entonces como una adecuada gestión de seguridad de la información buscará establecer y mantener políticas, planes y controles que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información.

3.2. Políticas relacionadas con Seguridad de la Información

Toda organización que intente valorizar el manejo de sus activos de información deberá definir una política de seguridad de la información, estableciendo una declaración formal organizacional sobre la que se desarrolle y gestione un programa eficaz de protección de activos de información.

El objetivo de esta declaración será el de crear un marco normativo que asegure la protección de la información en todas sus formas y medios, contra su modificación accidental o deliberada, utilización no autorizada, divulgación o interrupción.

Se entiende como políticas a los lineamientos o principios básicos relacionados con seguridad de la información, que sirven de medio para alcanzar los objetivos de la organización y sobre los cuales deben asentarse las normas y procedimientos, con la intención de:

- Apoyar la misión de la organización y brindar soporte a las estrategias de negocio de la misma.
- Definir un proceso que permita identificar y clasificar los activos de información de la organización.
- Definir y gestionar una adecuada configuración de los recursos y protección de los activos de información, garantizando que las medidas implementadas sean acordes con las características de la información a proteger.
- Clarificar al personal y terceras partes relacionadas, sus responsabilidades y tareas con respecto a la protección de los recursos de información.

UNIVERSIDAD TORCUATO DI TELLA

- Permitir a los niveles directivos y gerenciales tomar decisiones acerca de la seguridad de la información en concordancia con el resto de las políticas y normas establecidas en la organización.
- Coordinar los esfuerzos de diferentes grupos dentro de la organización para que los recursos se encuentren debida y consistentemente protegidos más allá de su localización, forma o tecnología que los soporta.
- Definir responsabilidades por el acceso y uso de los recursos y activos de información.
- Definir pautas para asegurar el cumplimiento de requerimientos legales, regulatorios, obligaciones contractuales y/o cualquier otro requerimiento relacionado con seguridad de la información.
- Proponer y colaborar en la toma de conciencia por parte de personas que interactúan con la organización sobre temas relacionados con seguridad de la información.

En síntesis, una Política de Seguridad de la Información debe definir claramente los participantes, con sus roles y responsabilidad, los ámbitos de aplicación, y una vez implementada, deberá ser comunicada a los empleados de la organización y terceras partes involucradas, con el efecto de cumplimentar lo allí dispuesto.

3.3. Características de seguridad

Se explican a continuación los principales conceptos a ser considerados para lograr una adecuada seguridad de la información:

- Autorización: la información, al ser accedida, debe cumplir con los niveles de permisibilidad correspondientes para su utilización y divulgación.
- Confidencialidad: asegurar que todos los recursos tecnológicos y la información administrada se encuentren adecuadamente protegidos contra divulgación indebida, ya sea por utilización no autorizada o revelaciones accidentales.
- Disponibilidad: garantizar la existencia de previsiones para minimizar las amenazas de interrupción del servicio y preservar la continuidad de la operatoria normal.

UNIVERSIDAD TORCUATO DI TELLA

- Integridad: mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados, considerándola completa, correcta y libre de errores.

También existen otros conceptos relacionados con las características que toda información debería cumplir, a saber: confiabilidad, oportunidad, cumplimiento, economía, utilidad, confiabilidad, claridad, entre otras.

3.4. Estándares internacionales

Las normas o estándares internacionales es el trabajo de diferentes organizaciones, orientadas para un grupo de personas, empresas y/o algún sector de la industria, siendo reglas concretas que definen cursos de acción precisos para las distintas tareas que se tuvieran que desarrollar.

Los estándares internacionales pueden ser aplicados directamente o a través de su modificación, adaptándolos a las condiciones locales, creándose así normativas nacionales equivalente que contemple, entre otros, situaciones propias de la región, clima, geografía, recursos, infraestructura, leyes gubernamentales o requisitos específicos.

En lo referente con la utilización de estándares internacionales relacionados con la implementación de TICs, se han desarrollado, publicado y adaptado localmente una serie de normas relativas a la gestión de la Seguridad de la Información.

La norma IRAM-ISO/IEC[12] 27002:2008, dentro del marco de Tecnología de la Información y Técnicas de Seguridad, establece un código de práctica para la gestión de la seguridad de la información.

En su inicio, dicha norma menciona que “la seguridad de la información es la protección de la información de una amplia variedad de amenazas, con el objeto de asegurar la continuidad del negocio, minimizar los riesgos y maximizar el retorno de la inversión y las oportunidades de negocio”, e indica que “cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe estar protegida en forma adecuada”.

UNIVERSIDAD TORCUATO DI TELLA

Esta norma constituye un código de práctica que establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización, proporcionando una guía general sobre los objetivos comúnmente aceptados para dicho tratamiento.

Utilizada como marco de referencia teórico y punto de partida para el desarrollo del presente trabajo, establece los siguientes controles necesarios para cualquier organización, dependiendo de la legislación aplicable:

- La protección de los datos y la privacidad de la información personal.
- La protección de los registros de la organización.
- Los derechos de propiedad intelectual.

Y considera como práctica común en la gestión de la seguridad de la información la inclusión de:

a. Documentos de la política de seguridad de la información.
b. Asignación de las responsabilidades de seguridad de la información.
c. Concientización respecto de la seguridad de la información.
d. Procesamiento correcto de las aplicaciones.
e. Gestión de las vulnerabilidades técnicas.
f. Gestión de la continuidad del negocio.
g. Gestión de los incidentes y mejoras de la seguridad de la información.

La norma contiene 11 capítulos relacionados con controles de seguridad, que se describen a continuación con su respectivo objetivo de cumplimiento, los cuales han sido considerados en la preparación de las preguntas a realizar durante las entrevistas.

1. Política de seguridad: proporcionar dirección y apoyo de la alta dirección para la seguridad de la información de acuerdo con los objetivos del negocio y los requerimientos relacionados con leyes y regulaciones aplicables.
2. Organización de la seguridad: gestionar la seguridad de la información tanto dentro de la organización como en lo relacionado con aquellas gestionadas por terceras partes.

[12] Instituto Argentino de Normalización y Certificación, Organización Internacional de Normalización y Comisión Electrotécnica Internacional.

UNIVERSIDAD TORCUATO DI TELLA

3. Gestión de activos: alcanzar y mantener una adecuada protección de los activos de la organización, inventariando los activos más importantes, identificando sus propietarios y asignando responsables de para su control.
4. Seguridad de los recursos humanos: asegurar que los empleados, contratistas y usuarios sean adecuados para los roles a cumplir y comprendan sus responsabilidades relacionadas con la protección de la información que gestionan, como así también aquellas acciones asociadas con sus desvinculaciones o cambios funcionales.
5. Protección física y ambiental: impedir accesos físicos no autorizados, daños o posibles interferencias a las instalaciones e información de la organización, gestionando adecuados perímetros de seguridad y protegiéndolo de amenazas físicas y del ambiente.
6. Gestión de comunicaciones y operaciones: garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y los servicios de red, estableciendo procedimientos operativos para una adecuada gestión y funcionamiento, controlando cambios en los sistemas e instalaciones, asegurando una adecuada segregación de funciones y controles por oposición, protegiendo la integridad de la información de software malicioso, y su disponibilidad a través de la ejecución de adecuados procedimientos de resguardo y recupero.
7. Control de accesos: controlar el acceso a la información, a las instalaciones de procesamiento y a los procesos de negocios de la organización, asignando y revisando periódicamente las autorizaciones de accesos y privilegios otorgados, gestionando la configuración de contraseñas de usuarios, su identificación y autenticación.
8. Adquisición, desarrollo y mantenimiento de sistemas de información: garantizar que la seguridad sea una parte integral de los sistemas de información, contemplando los sistemas operativos, motores de bases de datos, herramientas, servicios, productos enlatados y/o software desarrollado por el usuario.

UNIVERSIDAD TORCUATO DI TELLA

9. Gestión de los incidentes de la seguridad de la información: garantizar que los eventos de seguridad de la información y las debilidades asociadas a los sistemas de información se comuniquen a través de procedimientos formales y la confección de reportes de eventos sucedidos.
10. Gestión de la continuidad del negocio: contrarrestar las interrupciones de las actividades de la organización y proteger los procesos críticos del negocio de los efectos de las fallas significativas de los sistemas de información o desastres, asegurando una pronta y oportuna reanudación, minimizando así el impacto que se pudiera producir con la inoperatividad.
11. Cumplimiento: impedir infracciones y violaciones de cualquier obligación legal, reglamentaria, reguladora o contractual, y de cualquier requerimiento de seguridad.

3.5. Leyes y reglamentaciones relacionadas con protección de la información

También existen leyes y reglamentaciones gubernamentales, dependiendo del sector o tipo de industria en la que se encuentre la organización, que están vinculadas con factores de seguridad y protección de los datos y la información gestionada.

En Argentina, rige la Ley 25.326 de Protección de los Datos Personales (2000, y Disposiciones complementarias posteriores), de orden público y alcance nacional, cuyo objetivo es "la protección integral de los datos personales asentados en archivos, registros, bases o bancos de datos, a fin de garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre"[13].

Entre otras definiciones, esta norma identifica al responsable como aquella "persona física o de existencia ideal, pública o privada, que es titular de un archivo, registro, base o banco de datos".

[13] Fuente: Información Legislativa: http://www.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm.

UNIVERSIDAD TORCUATO DI TELLA

Por tratarse de una ley de alcance nacional, y que establece características generales de seguridad y responsabilidad referidas al tratamiento de los datos personales recolectados, la misma deberá ser contemplada en su aplicación para todo tipo de organizaciones (ver Anexo III).

UNIVERSIDAD TORCUATO DI TELLA

3. TRABAJO DE CAMPO

3.1. METODOLOGIA DE LA INVESTIGACION

Este trabajo de investigación ha sido abordado con una metodología cualitativa, para extraer datos descriptivos mediante entrevistas realizadas a los principales referentes de las empresas seleccionadas, con observación no participante, y la utilización de fuentes externas, como ser bibliografía, reportes y encuestas relacionadas de consultoras y empresas internacionales.

El diseño de la implementación es descriptiva no experimental, ya que interpreta los conceptos relacionados con Seguridad de la Información, contrastando la comparación de los resultados obtenidos con el rendimiento potencial o deseado según las mejores prácticas y estándares internacionales. La observación es no participativa, dado que las entrevistas han sido desarrolladas con el sólo objetivo de obtener información relevante para el presente trabajo.

El universo de esta investigación lo constituyen las MiPyMEs que utilicen tecnologías de la información como herramientas en sus procesos de negocio. La muestra se tomó durante los meses de febrero y marzo de 2016, de manera no probabilística, para lo cual se seleccionaron 16 empresas, coordinaron días y horarios de encuentro y se realizaron las entrevistas a personas con responsabilidades importantes en cada una de ellas.

Las empresas seleccionadas se encuentran ubicadas en la Ciudad Autónoma de Buenos Aires y el primer cordón del Conurbano Bonaerense, pertenecen a sectores de industrias y servicios, y tienen una antigüedad de al menos 15 años en el mercado. Este último requisito intentó considerar la necesidad que pudieron haber tenido estas empresas de incorporar recursos tecnológicos según hubieran ido evolucionando sus procesos de negocio junto con la evolución natural dada por las TICs en el último tiempo,

Basado en la norma IRAM-ISO/IEC 27002:2008 y lo emanado por la Ley 25.326 de Protección de los Datos Personales, se procedió a confeccionar una guía de pautas predefinidas, incluyendo 60 preguntas de tipo semi-estructuradas, permitiendo armar un grillado y tabular algunos resultados, facilitando así su análisis y evaluación.

UNIVERSIDAD TORCUATO DI TELLA

Las preguntas desarrolladas han incluido los capítulos generales correspondientes a gestión de la seguridad de la información, gestión de los activos, seguridad de los recursos humanos, física y ambiental, evaluación de los riesgos y gestión de la continuidad del negocio.

A tal efecto, se procedió a agrupar y sub-agrupar las preguntas en función de temas relacionados, ordenándolas por dominios mencionados en la norma (ver guía completa de preguntas en Anexo IV).

Si bien el cuestionario comprendía preguntas abiertas, en algunas de ellas además se establecieron criterios de respuestas tipo: “si”, “no”, “a veces / a medias”, “no sabe / no contesta”, de manera de tipificarlas y obtener conclusiones generales.

A continuación se describen las tareas realizadas para la ejecución del presente trabajo:

- Confección de la guía de preguntas a ser utilizadas durante las entrevistas.
- Búsqueda y selección de empresas comprendidas dentro de los criterios de inclusión definidos.
- Establecimiento de contacto con los responsables de las empresas seleccionadas y coordinación del día, hora y lugar para su realización, pudiendo ser éstas presenciales o de forma remota a través de conversaciones telefónicas o vía Skype[14]. Ejecución de las entrevistas.
- Transcripción de las conversaciones mantenidas.
- Tabulación de las respuestas dentro de criterios prefijados.
- Evaluación de los resultados obtenidos.
- Arribo de las conclusiones.

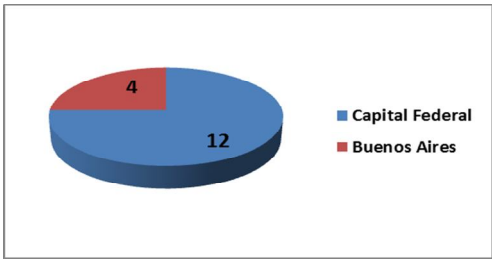
[14] Software que permite comunicarse entre dos o más personas, en cualquier parte del mundo, a través de videollamadas, mensajes de texto y/o compartir archivos.

UNIVERSIDAD TORCUATO DI TELLA

3.2. INSTRUMENTOS DE RECOLECCION DE LA INFORMACION

De las 16 empresas seleccionadas, 12 pertenecen a la Ciudad Autónoma de Buenos Aires y 4 se encuentran ubicadas en el primer cordón del Conurbano Bonaerense (FIGURA N° 9).

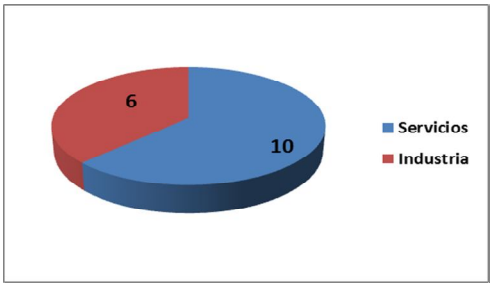
FIGURA Nº 9: Distribución de las empresas seleccionadas según su ubicación



Fuente: elaboración propia.

Asimismo de esta población estudiada 6 pertenecen al sector de industria y 10 al de servicios (FIGURA N° 10), intentando así obtener un análisis equilibrado.

FIGURA Nº 10: Distribución de las empresas seleccionadas según tipo de sector al que pertenecen



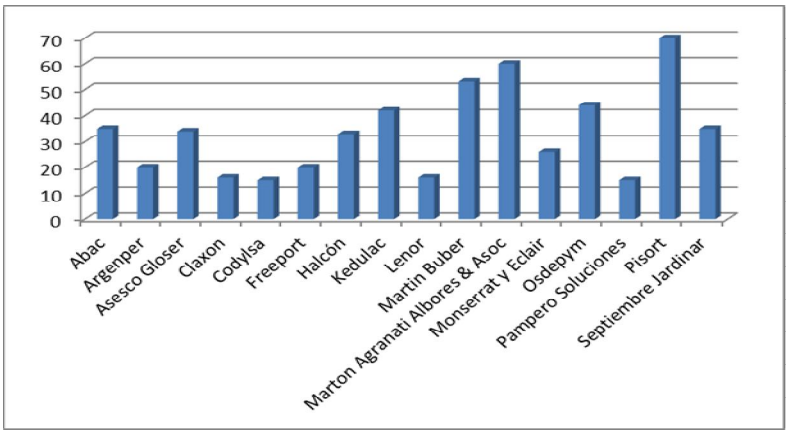
Fuente: elaboración propia.

Y por último, relacionado con la muestra seleccionada está el análisis de la antigüedad, punto que interesa particularmente , dado que se intenta considerar la necesidad de incorporación de recursos TICs que seguramente las empresas han requerido durante

UNIVERSIDAD TORCUATO DI TELLA

dicho período, oscilando la antigüedad de la muestra entre los 15 y 70 años en el mercado (FIGURA N° 11):

FIGURA Nº 11: Distribución de las empresas seleccionadas según años de antigüedad que poseen



Fuente: elaboración propia-.

Habiendo utilizado la entrevista como técnica para obtener información relacionada con la protección que las empresas seleccionadas realizan con la información que gestionan, se procedió a efectuar una síntesis de las respuestas obtenidas y efectuar un análisis como conclusiones generales de la información recolectada.

UNIVERSIDAD TORCUATO DI TELLA

3.3. ANALISIS DE RESULTADOS

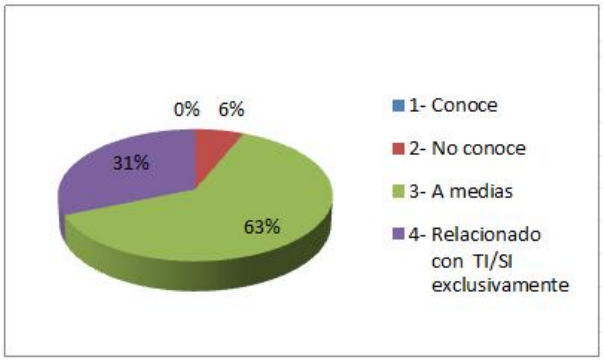
A continuación se exponen una síntesis de las respuestas obtenidas durante las entrevistas, considerando para ello los grupos de temas definidos.

3.3.1. Conocimientos previos en seguridad de la información

Sobre el conocimiento previo en seguridad de la información, correspondientes a las respuestas obtenidas a las preguntas de la Nº 1 a la 3 del Anexo IV, se obtuvo que independientemente de los conocimientos técnicos que pudieran tener o no los entrevistados, y del nivel de responsabilidad dentro de la empresa, la totalidad de los encuestados desconoce la completitud de los objetivos y alcances del concepto Seguridad de la Información, circundándolo casi exclusivamente a lo relativo con la tecnología y/o seguridad informática, en cuanto al acceso a información digital (FIGURA Nº 12).

Frases como “el acceso a la información y su custodia, relacionado con seguridad informática”, “relacionado con tecnología y seguridad informática”, han sido respuestas comunes.

FIGURA Nº 12: Conocimiento del significado seguridad de la información



Fuente: determinación del conocimiento en cuanto al significado de seguridad de la información (elaboración propia).

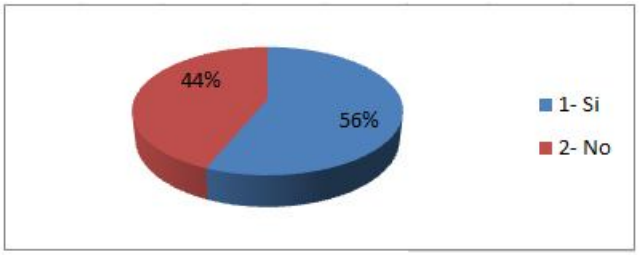
Asimismo, más de la mitad entiende que proteger la información de su empresa podría ayudar a maximizar el retorno de su inversión, básicamente colaborando en la

UNIVERSIDAD TORCUATO DI TELLA

organización de la información, asegurando la no divulgación a personas ajenas y reteniendo clientes a través de brindarles tranquilidad sobre sus datos (FIGURA Nº 13).

Respuestas positivas han mencionado, por ejemplo, que "para las empresas relacionadas con investigación de mercado es fundamental la protección de la información que administran", "el cliente por el tipo de acuerdo que busca lo toma como un estándar" y "se entiende que puede maximizar la rentabilidad y mejorar las oportunidades".

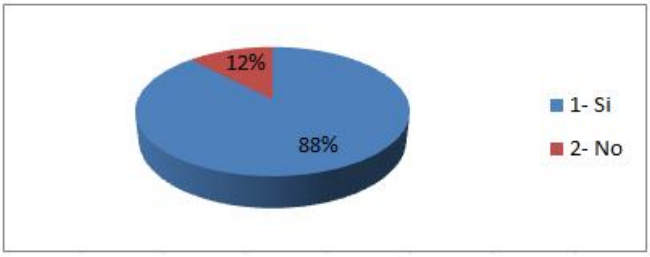
FIGURA Nº 13: Ayudaría a maximizar retornos de inversión



Fuente: determinación del conocimiento en cuanto a la maximización del retorno de la inversión (elaboración propia).

Además, la mayoría asegura que la falta de protección de la información podría ocasionarle problemas, ya sean legales y/o económicos (FIGURA Nº 14). Las respuestas en general están relacionadas con "legal básicamente, juicios", "podrían ocurrir problemas legales y deterioro de la imagen" y "si hubiera algún incidente repercutiría en la imagen del estudio".

FIGURA Nº 14: Ocasionaría problemas la falta de protección de la información



Fuente: determinación del conocimiento de problemas en cuanto a la falta de protección de la información (elaboración propia).

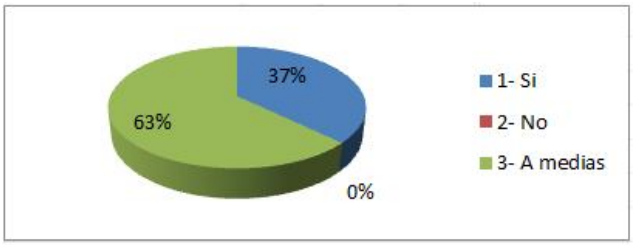
3.3.2. Temas relacionados con seguridad de la información

Sobre los temas generales abordados relacionados con seguridad de la información, correspondientes a las preguntas de la Nº 4 a la 23 del Anexo IV, se han obtenido las siguientes respuestas.

3.3.2.1. Gestión de activos de la información

De una u otra forma, todas las empresas entrevistadas dicen administrar inventarios de los distintos tipos de información que utilizan (FIGURA Nº 15), aunque la mayoría no lo tiene concentrado en un único listado, sino que se encuentra diseminado en cada área/sector de su organización, no existiendo un único responsable por su actualización y gestión. Una respuesta típica recibida ha sido "no hay un único listado, no es formal, está diseminado en distintos sistemas y lugares".

FIGURA Nº 15: Posee inventario de tipos de información administrada

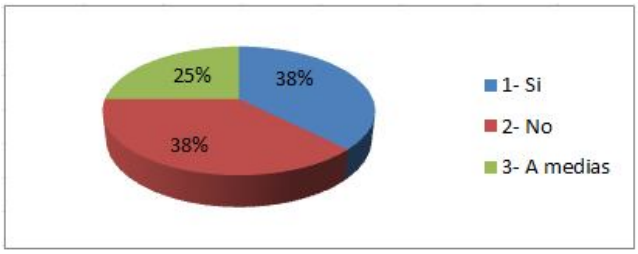


Fuente: distribución de las respuestas según posean inventarios de tipos de información (elaboración propia).

Las empresas que dicen manejar inventarios de los tipos de información que poseen, más de la mitad de ellas lo utilizada como punto de partida para su clasificación basado en su importancia, valor para el negocio y seguridad de acceso (FIGURA Nº 16).

UNIVERSIDAD TORCUATO DI TELLA

FIGURA Nº 16: Clasifican los tipos de información



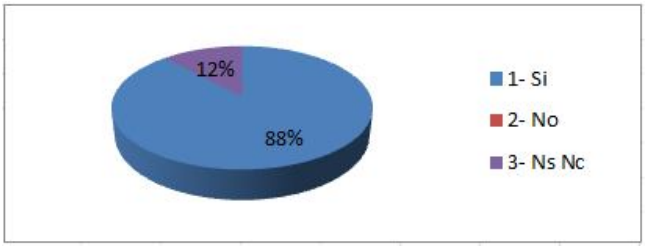
Fuente: distribución de las respuestas según clasificación de los tipos de información (elaboración propia).

El proceso de confección y clasificación de este tipo de inventario es importante para asegurar una adecuada protección de los activos de la empresa, colaborar también en otros aspectos de negocio (seguridad, aseguramiento y/o financiación, entre otros) y como prerrequisito para la gestión de los riesgos relacionados.

La mayoría de los que tienen clasificada la información, la misma es memorizada y manejada sólo por cada responsable, no habiendo seguimiento ni revisiones periódicas. No desarrollar estas tareas de forma metodológica, asignando responsables para su ejecución y supervisión, podría implicar que no se cuente con toda la información necesaria para poder recuperar las operaciones de negocio ante una eventual contingencia.

Todos dicen cumplir de una u otra forma los requerimientos legales, regulatorios, estándares y/o de la industria en la que se encuentran (FIGURA Nº 17). Si bien no se solicitaron verificar acciones de cumplimiento, los entrevistados demostraron conocer los requerimientos que deberían cumplimentar.

FIGURA Nº 17: Cumplimiento de leyes y reglamentaciones



Fuente: distribución de las respuestas según cumplimiento de leyes y reglamentaciones relacionadas (elaboración propia).

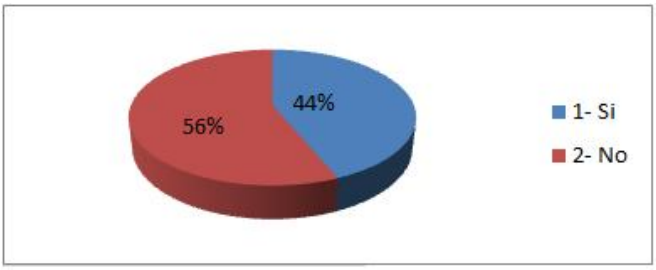
Algunas de las reglamentaciones mencionadas en las respuestas se corresponden con "Ley 25.326 de Habeas Data y normativa internacional ESOMAR", "Ley 25.326 de Protección de Datos Personales y normas ISO certificadas" y "nuevas disposiciones que hubieron para importar productos al país", entre otras.

3.3.2.2. Gestión de riesgos

En cuanto al análisis de los riesgos involucrados en la administración de la información, casi la mitad de las empresas reconocen su tratamiento, pero no de manera metodológica, más bien informal y esporádica, principalmente luego de la ocurrencia de algún incidente (FIGURA Nº 18).

Las respuestas en general están relacionadas con "sí se analiza, no como metodología periódica, pero se analizan" y "salen los temas en la medida que suceden y/o en las reuniones de trabajo que se realizan".

FIGURA Nº 18: Gestión de los riesgos de cada tipo de información



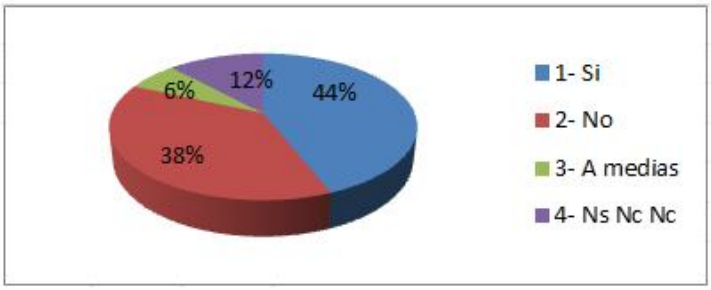
Fuente: distribución de las respuestas según gestión de riesgos realizada para cada tipo de información (elaboración propia).

UNIVERSIDAD TORCUATO DI TELLA

3.3.2.3. Seguridad en los recursos humanos

La mitad de las empresas disponen formalmente de una asignación de roles y responsabilidades para con sus empleados, siendo trasmitidas las tareas a realizar de manera verbal en algunos casos (FIGURA Nº 19). Algunas respuestas obtenidas han sido "existen descripciones de puestos formales" y "están en el manual de funciones de la empresa".

FIGURA Nº 19: Disponen de instructivos los empleados para realizar sus funciones



Fuente: distribución de las respuestas según disposición de instructivos para empleados acorde a sus funciones (elaboración propia).

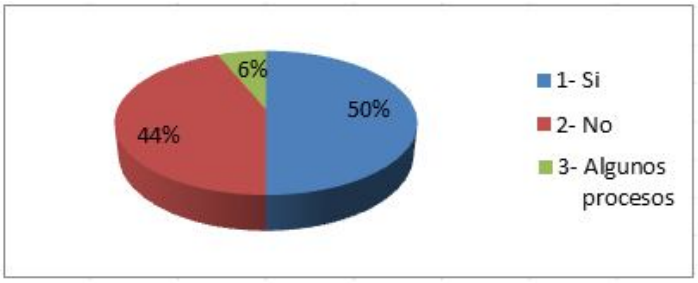
También la mitad de las empresas realiza actividades de capacitación a través de la entrega de algún instructivo, manuales funcionales, de sistemas, lectura de normativas internas y/o plataformas tecnológicas con acceso a documentos digitales. Se recibieron respuestas como "sólo capacitación inicial de 2 o 3 días", "verbalmente en la inducción a nuevos empleados" y "a través de e-learning" sobre el tema capacitación.

3.3.2.4. Gestión de la continuidad del negocio

Para los procesos más importantes relacionados con el negocio de cada empresa entrevistada, solamente la mitad dicen tener analizados los posibles problemas que pudieran surgir y planes para mantener una continuidad de sus operaciones de manera casi normal (FIGURA Nº 20).

UNIVERSIDAD TORCUATO DI TELLA

FIGURA Nº 20: Gestión de la continuidad del negocio



Fuente: distribución de las respuestas según gestión realizada para la continuidad del negocio (elaboración propia).

La mayoría de estos planes no están escritos, tampoco su análisis es considerado de forma metodológica, sólo en algunos casos son conocidos por sus empleados, ni se realizan pruebas que permitan asegurar un adecuado funcionamiento en caso de contingencia. Algunas de las respuestas han sido “se analizan los problemas y las soluciones según ocurren”, “depende de los casos particulares” y “sólo algunos problemas se analizan, no como metodología de trabajo”.

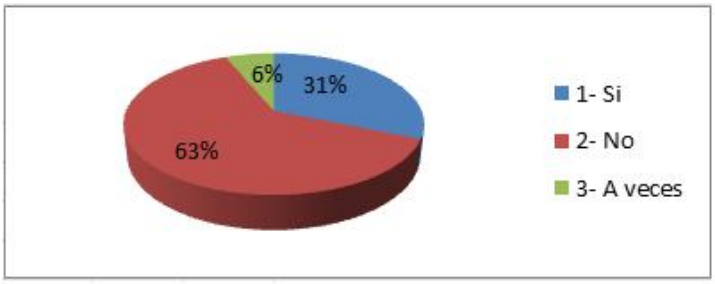
Sólo el simulacro de evacuación ante posibles incendios es llevado a cabo regularmente por estas empresas.

3.3.2.5. Actividades de concientización

La mayoría de las empresas entrevistadas no realiza actividades de concientización, o si las realiza son informales, sobre los temas relacionados con seguridad de la información tratados en este apartado (FIGURA Nº 21).

UNIVERSIDAD TORCUATO DI TELLA

FIGURA Nº 21: Se realizan charlas de concientización



Fuente: distribución de las respuestas según la realización de charlas de concientización en tema de seguridad de la información (elaboración propia).

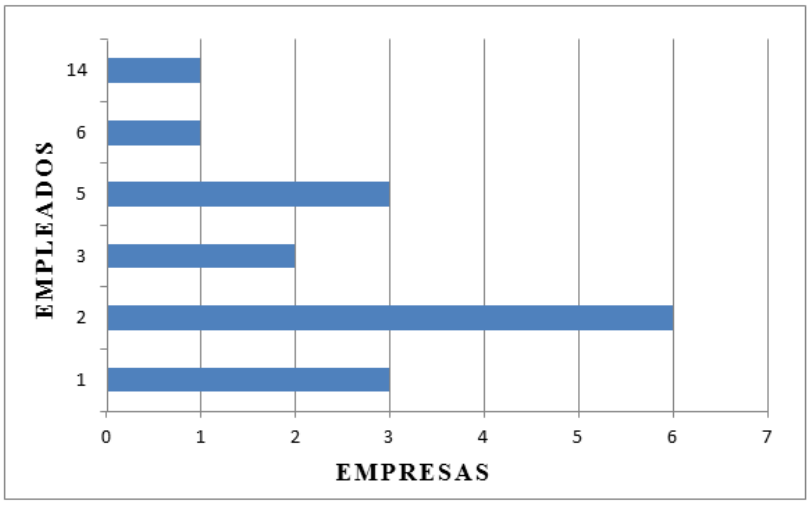
3.3.3. Temas relacionados con la tecnología y seguridad de la información implementada

A continuación se detallan aquellos temas relacionados con la tecnología y medidas de seguridad implementadas, correspondientes a las preguntas de la Nº 24 a la 55 del Anexo IV:

3.3.3.1. Gestión de la tecnología y sistemas de información

Más de la mitad de las empresas entrevistadas tienen, entre uno y seis empleados que se encargan de estas tareas; sólo una de ellas tiene un plantel de 14 empleados (FIGURA Nº 22).

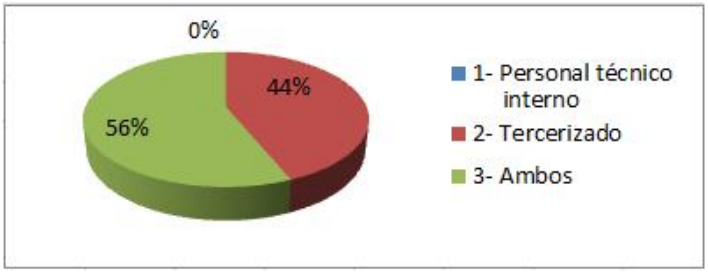
FIGURA Nº 22: Cantidad de empleados de tecnología de la información



Fuente: distribución de las respuestas según cantidad de empleados que atienden temas de tecnología de la información (elaboración propia).

Pero todas ellas tienen tercerizado al menos un servicio de tecnología informática, en especial aquel relacionado con servicios de Internet, comunicaciones y/o *hosting*[15] (FIGURA Nº 23).

FIGURA Nº 23: Modalidad de servicio de tecnología de la información



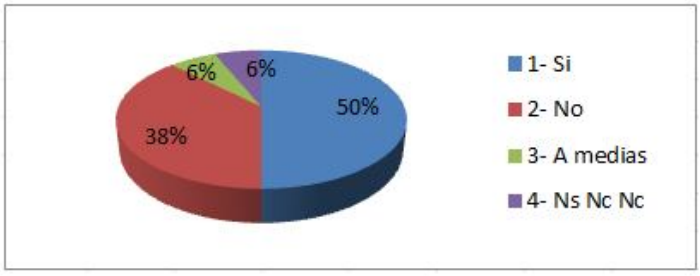
Fuente: distribución de las respuestas según la modalidad de servicios utilizada asociada con tecnología de la información (elaboración propia).

[15] También conocido como *web hosting*, es un servicio ofrecido por un proveedor para utilizar recursos de alojamiento digital ubicado en algún lugar de Internet.

UNIVERSIDAD TORCUATO DI TELLA

La mitad cree tener contratos y/o acuerdos de nivel de servicios con sus proveedores, pero no así los correspondientes al tratamiento de confidencialidad de la información a la que pudieran acceder (FIGURA Nº 24).

FIGURA Nº 24: Contratos de servicios de terceros de tecnología de la información



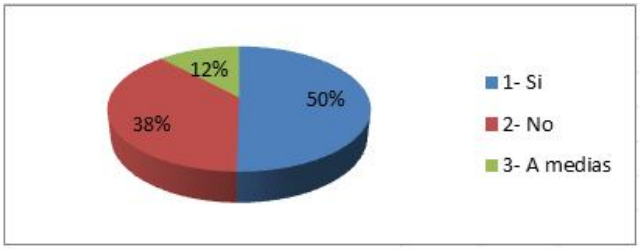
Fuente: distribución de las respuestas según posean contratos de servicios de terceros relacionados con tecnología de la información (elaboración propia).

En la mayoría de los casos el proveedor entrega un reporte sobre las tareas realizadas, al cual sólo se le hace seguimiento para el pago del servicio.

3.3.3.2. Protección física de los recursos tecnológicos

Más de la mitad reconocen tener el equipamiento en condiciones relativas de seguridad, en cuanto al acceso directo al equipamiento, y de amenazas externas y del ambiente, contra daños potenciales causados por fuego, temperatura, corte de suministro eléctrico, entre otros (FIGURA Nº 25).

FIGURA Nº 25: Equipamiento con adecuada protección física



Fuente: distribución de las respuestas según dispongan de adecuada protección física la tecnología informática utilizada (elaboración propia).

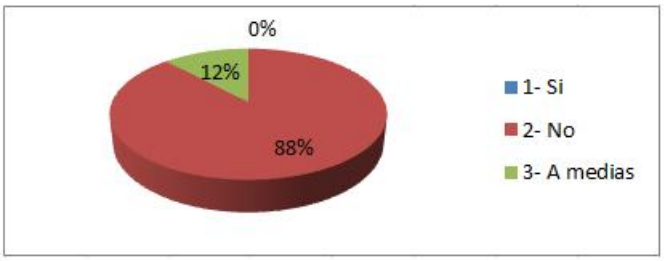
UNIVERSIDAD TORCUATO DI TELLA

Algunos mencionan contar con "recintos protegidos con UPS[16], equipos de aire acondicionado y detectores de humo", mientras que otros señalan que "son las características contratadas al proveedor del *hosting*".

3.3.3.3. Protección lógica de los recursos tecnológicos

Todas las empresas entrevistas reconocen que los responsables técnicos, ya sean empleados o personal tercerizado, utilizan usuarios administradores con permisos especiales para acceder a las diferentes plataformas, con contraseñas conocidas por varias personas que no son habitualmente modificadas (FIGURA Nº 26). La respuesta común dada a este ítem se corresponde con "tanto personal de sistemas como del proveedor poseen accesos a utilizar usuarios administradores".

FIGURA Nº 26: Equipamiento con adecuada protección lógica para administración por parte del personal técnico



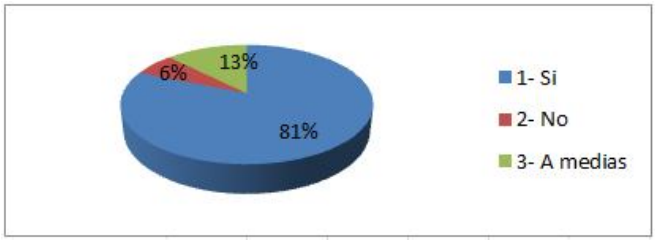
Fuente: distribución de las respuestas según adecuada protección lógica en cuanto a la utilización de usuarios con permisos de administración técnica (elaboración propia).

Dicha utilización la realizan de manera indiscriminada, sin dejar evidencia operativa o de trazabilidad en cuanto a lo actuado, y sin ningún tipo de monitoreo o supervisión posterior. Otra respuesta que engloba esta situación es que "por confianza y cultural, quedaron como de uso público y diario".

[16] Por sus siglas en inglés *Uninterruptible Power Supply*, corresponde a sistemas de suministro eléctrico de manera ininterrumpida.

No obstante, todos reconocen que el resto de los empleados utilizan sus propios usuarios para acceder a los sistemas, con permisos a ejecución de tareas acorde con sus roles y responsabilidades dentro de la empresa (FIGURA Nº 27).

FIGURA Nº 27: Adecuada protección lógica de usuarios finales

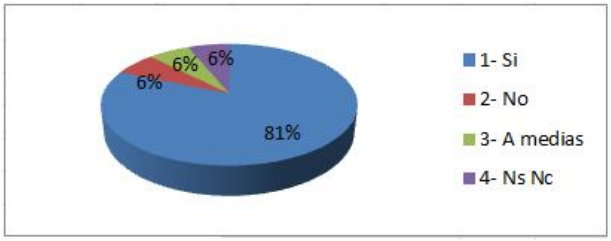


Fuente: distribución de las respuestas según adecuada protección lógica en cuanto a la utilización de los recursos informáticos por parte de los usuarios finales (elaboración propia).

No pasa lo mismo con las cuentas de correo, siendo habitual la utilización de cuentas genéricas compartidas por varios empleados.

La mayoría de las plataformas tecnológicas se encuentran configuradas y protegidas contra código malicioso y/o accesos no autorizados (FIGURA Nº 28). Una respuesta general es tener "instalado un antivirus corporativo y un cortafuego con filtros para accesos de Internet" y "con claves el wifi".

FIGURA Nº 28: Adecuada configuración de protección antimalware



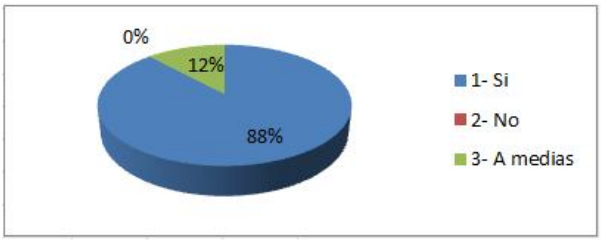
Fuente: distribución de las respuestas según dispongan de adecuada protección antimalware la tecnología informática utilizada (elaboración propia).

UNIVERSIDAD TORCUATO DI TELLA

3.3.3.4. Resguardo de información

Todas las empresas realizan un resguardo de la información en algún dispositivo de almacenamiento, ya sea movible (por ejemplo, discos externos y/o *pendrives*) o dentro de algún otro equipamiento, a través de tareas programadas de forma automática (la gran mayoría) y/o manual, copiando la información sin encripción (FIGURA Nº 29).

FIGURA Nº 29: Adecuada protección de resguardo



Fuente: distribución de las respuestas según posean adecuada protección de resguardo de la información administrada (elaboración propia).

La mayoría de estos resguardos se protegen externamente, en un lugar fuera de la empresa, siendo supervisados por los directivos y/o el personal técnico.

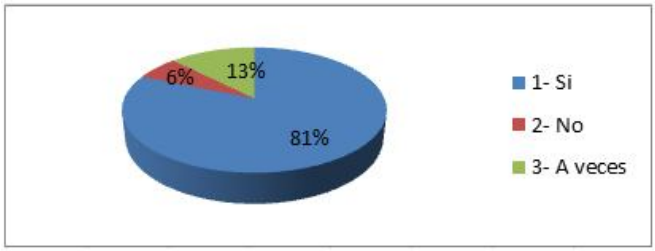
En una sola de las empresas entrevistadas se confirmó que se realizan pruebas para verificar la integridad de la información en caso de necesidad de recuperación.

3.3.3.5. Utilización de dispositivos móviles

Con excepción de una sola empresa, el resto utiliza dispositivos móviles, como ser notebooks y/o smartphones (FIGURA Nº 30).

UNIVERSIDAD TORCUATO DI TELLA

FIGURA Nº 30: Utilización de dispositivos móviles



Fuente: distribución de las respuestas según utilización de dispositivos móviles para las tareas diarias (elaboración propia).

Las notebooks cuentan con protección contra uso no autorizado e infecciones de malware, no así los teléfonos inteligentes.

Y en la mayoría de los casos, la información que se administra en estos dispositivos, como correos electrónicos, libreta de contactos y documentos de trabajo, no son considerados en los resguardos generales, debiendo los responsables de uso realizarlos de manera personal y manual.

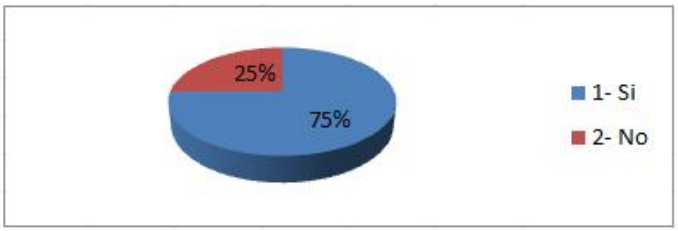
3.3.4. Preguntas finales sobre los conceptos conversados

Sobre los conceptos relacionados con seguridad de la información, correspondientes a las respuestas obtenidas a las preguntas de la Nº 56 a la 60 del Anexo IV, en todos los casos, finalizando la entrevista, han mencionado la consideración de reforzar los conceptos relacionados con protección de la información, bien sea para mejorar aspectos de control, asegurar la continuidad normal de las operaciones, mejorar las oportunidades de negocio y/o evitar daños colaterales por falta de protección (FIGURA Nº 31).

Algunas respuestas se corresponden con “algunos temas podrían ser considerados”, “sería conveniente formalizar tareas y conceptos relacionados.” y “es muy importante por las características del servicio que se brinda”.

UNIVERSIDAD TORCUATO DI TELLA

FIGURA Nº 31: Predisposición a contratar servicios de seguridad de la información



Fuente: determinación del conocimiento en cuanto a la predisposición de contratar servicios profesionales relacionados con seguridad de la información (elaboración propia).

Por último, la mayoría de los entrevistados han dado su predisposición a contratar servicios profesionales para analizar la situación de su empresa en este aspecto. Una de las respuestas obtenidas ha sido que “de hecho se está consultando para realizar un servicio de tales características”.

UNIVERSIDAD TORCUATO DI TELLA

4. CONCLUSIONES

4.1. Conclusiones generales

De las respuestas obtenidas se deduce el escaso conocimiento del concepto que abarca el término Seguridad de la Información y sus prácticas aplicables para la protección de la información administrada por las empresas entrevistadas.

Justamente, la mayor parte sólo lo relaciona con el término “seguridad informática”, reaccionando en consecuencia con la implementación de medidas básicas de protección a la tecnología informática utilizada.

Por otra parte, a pesar que las mismas empresas reconocen la importancia vital para el negocio el mantener activos sus procesos críticos, tecnología y sistemas de gestión para el tratamiento de la información y la toma de decisiones gerenciales, resulta llamativo que ninguno de los entrevistados, aun conociendo los riesgos a los que se exponen, dejen librado al azar aspectos fundamentales de protección, seguridad y planificación ante contingencias.

4.2. Detalle de las conclusiones arribadas

Del análisis a las entrevistas realizadas, y el cruzamiento con lo dispuesto en la norma IRAM-ISO/IEC 27002:2008 y la Ley Nacional 25.326 de Protección de Datos Personales mencionado en el Capítulo 3 del Marco Teórico, consideradas ambas para la realización del presente trabajo, se presenta el siguiente detalle técnico pormenorizado de las fortalezas y debilidades detectadas.

4.2.1. Fortalezas

- Las empresas entrevistadas señalan una amplia utilización de la tecnología, sistemas y herramientas informáticas en sus operatorias diarias, gestionando la información, considerada principal instrumento en las decisiones de negocio.
- En todos los casos se mencionó que las empresas fueron actualizándose forzosamente con la creciente evolución de las tecnologías disponibles,

UNIVERSIDAD TORCUATO DI TELLA

principalmente a partir de los nuevos canales de comunicación, publicidad y venta a través de Internet.

- Resaltaron además las dificultades que han tenido en los últimos 15 años relacionado con los vaivenes de la economía del país, dedicando un porcentaje de dicho esfuerzo en adecuar el hardware y software utilizado.
- En general, estas empresas declaran un notable grado de implementación de medidas básicas de seguridad, relacionadas con la protección anti malware, localmente en los equipamientos y analizando los correos electrónicos.
- También presentan configuraciones de seguridad en las conexiones con redes externas, como hardware y/o software corta-fuego, contraseñas de red Wifi y protocolos seguros de comunicación. Si bien no se efectuaron revisiones técnicas del equipamiento y su configuración, los entrevistados demostraron conocer estas medidas básicas de seguridad implementadas en sus empresas.
- Los resguardos en soportes externos relacionados con la información general de la empresa son realizados a consciencia, conociendo que de ellos dependerá la información a recuperar en caso de alguna urgencia o necesidad.
- Cabe destacar la predisposición de las personas entrevistadas para considerar la posibilidad de recurrir a profesionales en Seguridad de la Información para el asesoramiento sobre el estado de situación en su empresa. Es de mencionar que en cinco de las empresas entrevistadas se encontraban realizando una reingeniería de sus procesos y de la tecnología de información que los soporta, e incluirían algunas de los aspectos de seguridad conversados.

4.2.2. Debilidades

- En todos los casos entrevistados, los profesionales de Tecnología de la Información que actúan en las empresas, bien sean como empleados y/o personal contratado, acceden a la utilización de usuarios con permisos especiales y con altos privilegios de accesos, conociendo públicamente la identificación y contraseña de los mismos, no tomando ningún tipo de recaudos para su protección contra mal uso, divulgación y/o exposición.

UNIVERSIDAD TORCUATO DI TELLA

- Estas tareas tampoco son adecuadamente monitoreadas por personal responsable técnico, en caso de haber, o personal directivo, ni dejan trazabilidad o pistas de auditoría para un análisis de uso posterior.
- En todos los casos prevalece la confianza de la relación laboral que se tiene por el profesional técnico.
- La exposición de riesgos que se corren por permitir a los profesionales de tecnología y/o usuarios finales, la utilización de cuentas de administradores en las plataformas informáticas son infinitas, aunque sean no intencionales o por negligencia en su uso. Por ejemplo, brindando la posibilidad de instalación del mencionado *ransomware*, que podría desde encriptar todos los datos de un equipo, a seguir infectando al resto de las computadoras y servidores, llevando la infección a cabo en toda la red de computadoras, incluyendo los resguardos de información, todo ello por haberse filtrado como un usuario de privilegios especiales.
- También es llamativo que ante la importancia que manifiestan por la necesidad de asegurar la continuidad normal de las operaciones, ninguna de las empresas disponga de un plan concreto de continuidad del negocio, o que ni siquiera realice de manera sistemática el ejercicio de considerar y analizar posibles problemas que pudieran surgir a sus procesos, el impacto que podrían ocasionar, y alternativas para mitigar los riesgos y/o mantener en operaciones al menos aquellos más críticos.
- No disponer de un plan de gestión de continuidad del negocio en una empresa, con controles preventivos y de recuperación, impacta directamente en el intento por evitar posibles pérdidas de activos de información valiosos ante cualquier tipo de desastre, sean naturales o provocados por el hombre, intencionados o no, con implicancias que hasta podrían terminar con el cierre de la empresa.
- Los dispositivos móviles, básicamente equipos notebooks y smartphones, que están siendo utilizados se encuentran menos protegidos en comparación, considerando el riesgo por exposición al poder ser robados en la vía pública.

UNIVERSIDAD TORCUATO DI TELLA

- La información registrada en estos dispositivos móviles, no es resguardada y queda a cargo individual de los responsables recordar y ejecutar esta tarea. Tampoco se consideran realizar pruebas de recuperación de la información resguardada, en ninguno de los casos.
- No contar con una adecuada descripción de funciones, tanto para empleados como contratistas, podría ocasionar una mala asignación de roles y responsabilidades en sus tareas y acceso a la información, facilitando el riego de hurto, fraude o mal uso de las instalaciones y recursos.
- Además, realizar actividades formales y regulares de capacitación sobre políticas y procedimientos organizacionales, entrenamiento en tareas habituales del personal, relacionadas con concientización en temas de protección de la información, responsabilidades legales y controles del negocio, permitirían reforzar los conocimientos del personal para reconocer problemas e incidentes de seguridad, y responder de acuerdo con las necesidades de su rol de trabajo.

5. RECOMENDACIONES

5.1. Consideraciones generales

Con la intención de contemplar actividades básicas que sirvan como guía para la protección de los activos de información de cualquier organización, objetivo secundario de este trabajo, considerando un público que no necesariamente posee conocimientos de características metodológicas ni de tecnología informática, se recomienda abordar los siguientes conceptos de manera práctica, con lenguaje no técnico y de fácil comprensión, que permita implementar adecuadas configuraciones de seguridad a fin de minimizar los riesgos relacionados y asegurar la continuidad de las operaciones del negocio.

El documento a confeccionar debería incluir como mínimo los siguientes tópicos, alineado con los estándares y mejores prácticas presentadas, desarrollándolos genéricamente a continuación.

5.1.1. Políticas organizacionales relacionadas con Seguridad de la Información

Deberá considerarse el alcance que se deseará darle a las políticas a definir e implementar en temas relacionados con seguridad de la información, considerando e incluyendo los objetivos y estrategias de negocio de la organización, la tecnología de la información donde se encuentran soportados, las ubicaciones físicas y distribuciones del equipamiento, como así también delimitando aquellas actividades que no serán tenidas en cuenta quedando fuera del alcance.

A partir del alcance, se deberá trabajar en los lineamientos sobre los cuáles se sentarán las políticas y marco normativo organizacional de protección de la información, definiendo actividades, roles y responsabilidades por su ejecución y control. Tendrá que incluir principios y generalidades de uso, como así también las particularidades relativas a cada organización, detallando las normativas que se fueran a utilizar con el objeto de disponer de medidas de seguridad que permitan minimizar los riesgos relacionados y asegurar la continuidad de las operaciones.

UNIVERSIDAD TORCUATO DI TELLA

Es de mencionar, que para su redacción se deberán considerar todo tipo leyes, reglamentaciones y/o estándares internacionales que pudieran aplicar al tipo de organización en la que se esté operando (por ejemplo, Ley 25.326 de Protección de Datos Personales, Ley 26.529 de Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud, IRAM-ISO-9001:2015 aplicable para la Certificación de Calidad de Procesos, entre otras).

Otras consideraciones importantes que deberá incluir corresponde con la relación entre terceras partes involucradas tanto en los procesos de soporte tecnológico, como también aquellas que pudieran tener acceso a la información gestionada (clientes y/o proveedores a través de alguna plataforma web, por ejemplo). Una vez redactada y aprobada por la dirección, estas políticas deberán ser de dominio público para el resto de los empleados.

Para el desarrollo de las siguientes actividades y su repetición con determinada frecuencia, se recomienda establecer una metodología que establezca como mínimo los objetivos, alcances, participantes y responsabilidades, actividades a realizar, periodicidad de ejecución, productos/reportes a obtener, presentación y aprobación de los resultados, seguimiento y supervisión de las acciones de mejora, y ejecución de actividades de publicación y concientización a empleados.

5.1.2. Gestión de los activos de información

Inventariar los activos de información implicará considerar las distintas formas que pueden tener (como ser instalaciones, procesos de negocio, contratos, acuerdos comerciales, equipamiento, bases de datos, programas de software, correos electrónicos, entre los más habituales) y la fuente de su procedencia (por ejemplo, archivos digitales, soportes en papel, o mismo el conocimiento o tareas diarias no documentadas que realizan los empleados).

Para facilitar su recolección y registración, podrá ser conveniente diferenciarlos por alguna de las características antes mencionadas, o algún otro criterio que pudiera servir. Dado que no todos los activos tienen la misma importancia, será necesario establecer criterios de valoración cuantitativo y cualitativo, en función de su relevancia para las actividades del negocio.

5.1.3. Gestión y tratamiento de los riesgos

Analizar los riesgos implicará considerar los lineamientos generales vertidos en las políticas organizacionales de seguridad, como así también los recursos económicos, técnicos y humanos relacionados.

Por cada activo inventariado, en función de su participación y criticidad para las actividades de negocio, se identificarán las amenazas asociadas que pudieran afectarlo, siendo de interés aquello que pudiera causar un daño o afectar su normal funcionamiento para una correcta ejecución de los procesos de negocio.

Se identificarán también aquellos controles desplegados para las distintas amenazas que ya pudieran estar implementados y su nivel de eficacia en función de los registros del historial que se pudiera o no disponer (por ejemplo, registros de cuántas veces se cortó la luz durante el último año y por cuánto tiempo).

También para cada amenaza identificada, y controles relacionados, se consideraran las probabilidades de ocurrencia que pudiera materializarla y se estimará el nivel de impacto en caso de producirse. Para esta última estimación deberán valorarse, entre otras y según aplique, posibles consecuencias tales como pérdida económica, alteración de la integridad, confidencialidad y/o autenticidad de la información, alteración de la trazabilidad de operaciones, actividades y/o disponibilidad de servicios, pérdida, divulgación o modificación no autorizada de información, daño en la imagen o reputación de la organización, perjuicio a seres humanos, incumplimiento de obligaciones contractuales y/o regulatorias, entre otros.

Luego de ser estimados la probabilidad de ocurrencia y el impacto de las amenazas identificadas, se determinará el nivel de riesgo correspondiente, y se darán las recomendaciones de ajustes y/o control necesarias para aquellos riesgos de nivel crítico/alto, según el nivel de aversión al riesgo que posea cada organización.

UNIVERSIDAD TORCUATO DI TELLA

5.1.4. Gestión de la continuidad del negocio

Abarcará todas las fases y secuencias de actividades necesarias para desarrollar, implementar y mantener actualizado un plan que permita asegurar una adecuada recuperación de la información y la capacidad de procesamiento operativo en caso de alguna contingencia.

Dicho plan involucrará capacidades tácticas y estratégicas pre-aprobadas, y contemplará medidas preventivas y de recuperación, que permitan responder ante incidentes e interrupciones en los servicios, con el fin de poder continuar con los procesos y operaciones en niveles aceptables previamente definidos.

Partiendo de los resultados de la gestión de activos de información y de riesgos antes mencionadas, se identificarán los procesos de negocio más importante para la organización y se efectuará un análisis de impacto ante alguna posible interrupción de los mismos.

El acumulado de pérdidas suele ir creciendo linealmente a medida que pasan los días y las actividades están interrumpidas, no obstante, a partir de un momento las pérdidas sufren un aumento significativo y las funciones no podrán ser reasumidas; permitiendo determinar allí el tiempo de tolerancia máximo de interrupción para la recuperación y el tiempo de actualización que deberían tener los datos en caso de una contingencia.

En función de estos datos se diseñarán y seleccionarán estrategias de recuperación, que comprenderán desde métodos operativos alternativos, automáticos o manuales, garantizando la restauración de los procesos críticos afectados en los tiempos determinados.

Existen diferentes estrategias para mitigar el impacto de una interrupción. Cada una de estas estrategias tiene parámetros de tiempo, disponibilidad y costos asociados que serán más o menos apropiados dependiendo de las funciones de negocio que se deseen recuperar.

Una vez seleccionada la estrategia para cada proceso crítico se podrán desarrollar los siguientes planes, de corresponder según las particularidades, dimensiones y nivel de detalle que cada organización pretenda darle:

UNIVERSIDAD TORCUATO DI TELLA

- El plan de respuesta ante emergencias, incluyendo procedimientos internos a seguir por los empleados como respuesta ante un incidente de gravedad que se convierta en una amenaza potencial a la salud y/o seguridad del personal, del ambiente o la propiedad, como también procedimientos de evaluación inicial del daño y declaración de la contingencia,
- El plan de comunicación de crisis, incluyendo procedimientos internos y externos de notificación de inicio de la recuperación ante un desastre reconocido. Este plan deberá ser coordinado con la ejecución de los demás planes para asegurar que sólo comunicados aprobados sean divulgados y que sólo el personal autorizado sea el responsable de responder las inquietudes del estado de situación al personal interno y al público/medios en general.
- El plan de recuperación ante desastre, incluyendo procedimientos internos orientados a responder ante contingencias importantes que nieguen el acceso a la operatoria normal por un tiempo extendido. El alcance de este plan incluirá los planes y procedimientos relacionados con el soporte general, la logística y el traslado del personal al sitio de recupero (de corresponder), la provisión del material y equipamiento que fuere necesario, y la coordinación de la recuperación de la operatoria del negocio por cada proceso crítico y la contingencia asociada con la tecnología informática.
- Los planes de continuidad de las operaciones, donde se detallen los procedimientos internos a cargo de cada área/sector de la organización, orientados a restaurar los procesos críticos definidos, asegurando así su continuidad durante una emergencia o interrupción.
- El plan de contingencia tecnológica, incluyendo los procedimientos internos destinados a ofrecer métodos alternativos para la recuperación de la tecnología y sistemas de soporte en general, y aquella relacionada con los procesos críticos en particular.
- El plan de restauración del negocio, incluyendo los procedimientos internos que, una vez solventada la contingencia, permitan recuperar la total normalidad del funcionamiento original. Este plan deberá incluir un análisis de impacto con una

UNIVERSIDAD TORCUATO DI TELLA

valoración detallada de los equipos e instalaciones dañadas que permitiendo definir las estrategias de vuelta a la normalidad de las operaciones del negocio.

- Los planes de pruebas, que permitan asegurar la viabilidad de las soluciones adoptadas en los planes anteriores, a través de la ejecución de actividades de simulación que planteen escenarios de recuperación, evaluando la capacidad de respuesta ante una situación de desastre, probando la efectividad de los procedimientos y los tiempos de respuesta para comprobar su alineamiento con las definiciones de diseño, identificando las áreas a mejorar, y fomentando la capacitación de los participantes.

5.1.5. Gestión básica de la seguridad informática

Deberán considerarse acciones que permitan asegurar una adecuada protección de la información, en todas sus formas y medios, contra su modificación accidental o deliberada, utilización no autorizada, divulgación o interrupción, de modo de garantizar el cumplimiento del marco normativo definido en las políticas relacionadas con seguridad de la información.

A continuación se mencionan aquellos aspectos básicos generales que como mínimo que deberán ser considerados:

- La seguridad física del equipamiento, asegurando una adecuada protección física de los recursos informáticos utilizados. El esquema de seguridad deberá impedir el acceso no autorizado de personas, daños en las instalaciones y cualquier otra amenaza que haga peligrar el funcionamiento de todo dispositivo físico de procesamiento, restringiendo y controlado: la seguridad perimetral, de las instalaciones, el acceso físico a las mismas, equipos de detección y extinción de incendios, factores ambientales básicos de temperatura, higiene, aislamiento eléctrico y sonoro, y otras medidas similares de acuerdo a los requerimientos específicos del equipamiento informático utilizado, entre las principales.
- El control de acceso a los equipos por parte de personal especializado, asegurando razonablemente que la utilización de los accesos (contraseñas, claves, llaves, etc.), privilegiados o de emergencia, a los ambientes informáticos de la

UNIVERSIDAD TORCUATO DI TELLA

organización y/o a las ubicaciones físicas de acceso restringido y/o a los accesos a las plataformas en Internet (e-bancos, e-pagos, redes sociales, etc.), se realice en forma controlada y documentada. Dado que todos los dispositivos tecnológicos utilizados (computadoras, servidores, tablets, smartphones, smarttvs, etc.) necesitan ser inicializados, configurados y actualizados por un usuario administrador que posea súper privilegios en el acceso, los mismos deberán ser utilizados exclusivamente en caso de fuerza mayor, y solo cuando sea absolutamente necesario para garantizar la continuidad operativa. Para lo cual se recomienda proponer algún procedimiento de habilitación y utilización de dichos datos (usuario y contraseñas), como así también su custodia en algún lugar que se encuentre cerrado permanentemente con llave, fuera del alcance de personal ajeno a la misma.

- El control de software malicioso, asegurando razonablemente que la información computarizada no sufra ataques correspondientes a virus informáticos que produzcan daños en su contenido y/o disponibilidad de acceso (por ejemplo, equipamiento servidores, computadoras personales, redes, notebooks, tablets, smartphones, etc.). Para lo cual será necesario evaluar, instalar y actualizar periódicamente algún programa antivirus en cada ambiente tecnológico que pudiera estar expuesto.

- El control de acceso a los sistemas y herramientas informáticas, asegurando razonablemente la correcta definición de los accesos de los usuarios finales a los recursos informáticos instalados en los distintos ambientes tecnológicos y que los mecanismos de control de acceso configurados en cada ambiente cuente con características que permitan individualizar y controlar el uso de sus recursos. Los requerimientos básicos que deberán ser considerados, entre los principales, se corresponden con la protección de todos los recursos informáticos, datos y sistemas utilizados, la administración y gestión de los usuarios, contraseñas y permisos/roles de ejecución, las configuraciones de seguridad que cada plataforma tecnológica disponga, y la revisión periódica de los usuarios y accesos otorgados, al menos una vez al año.

UNIVERSIDAD TORCUATO DI TELLA

- El control de acceso a las comunicaciones, asegurando razonablemente la integridad, disponibilidad, confidencialidad, autenticidad y legalidad, cuando corresponda, de la información transmitida a través de los sistemas de correo electrónico, acceso remoto e Internet. Adicionalmente a las medidas de protección físicas y de accesos ya definidas, se deberán tener en cuenta consideraciones generales de configuración para las conexiones internas y externas del equipamiento utilizado para tal comunicación (algunos ejemplos como: la asignación y funcionalidad de la página de Web de la organización, la ubicación de los equipos para el acceso Wifi y la administración de sus claves, reglas para la utilización de correos electrónicos entrantes y salientes, protección y accesos a páginas de Internet, descarga de información digital desde el correo electrónico y/o Internet, entre otros).
- La utilización de dispositivos móviles, disponiendo medidas que establezcan la utilización del equipamiento que disponga la organización por parte del personal (como ser, notebooks, netbooks, smartphones, pendrives, otros), la aplicación de medidas de seguridad y protección (por ejemplo: antivirus, firewall, etc.), utilización de redes públicas (acceso a Internet en aeropuertos, restaurantes, u otras), y aquellas que impidan el acceso a la información en caso de pérdida o robo a través de la configuración de claves seguras de acceso, cifrados de dispositivos, ubicación por geolocalización, administración remota al encenderse el equipo, inclusión de copias periódicas de respaldo de información, entre las principales.
- El resguardo de información, definiendo las pautas generales para asegurar una adecuada recuperación de la información de la organización, en caso de pedidos de información histórica adicional o total por alguna contingencia, a través de tareas claramente definidas para efectuar, custodiar, verificar y recuperar copias de respaldo. Será necesario para ello considerar todos los diferentes tipos de información de todos los ambientes tecnológicos que se dispongan, o al menos de aquellos utilizados para soportar los procesos definidos como críticos.

UNIVERSIDAD TORCUATO DI TELLA

6. REFERENCIAS

6.1. Índice de ilustraciones

UNIVERSIDAD TORCUATO DI TELLA

7. BIBLIOGRAFIA

7.1. Informes

Cybsec (2008), Ardita, Julio, *Manejo y análisis de incidentes de seguridad informática*.

Eset (2016), *Security report Latinoamérica 2016.*

Fundación Observatorio Pyme (2013), *Informe especial. Definiciones de PyME en Argentina y el resto del mundo*.

Deloite (2015), *Gestión de cyber riesgos y seguridad de la información.*

Kaspersky Lab (2015), *Security bulletin*.

Kaspersky Lab (2016), *Ataques dirigidos y ciber fraude*.

Observatorio Pyme Regional (2007), Lapelle Hernán, *Los obstáculos de acceso al financiamiento bancario de las PyMEs.*

OEA-BID[17] (2016), *Ciberseguridad, ¿estamos preparados en América Latina y Caribe?*

PriceWaterhouseCoopers (2014), *Encuesta global sobre delitos económicos*.

PriceWaterhouseCoopers (2016), *Encuesta global de seguridad de la información, tendencias y desafíos.*

Research Usuaria (2015), *La visión TIC de los CIOs*.

Symantec (2012), *Reporte sobre el costo y manejo de la información empresarial, resultados América Latina.*

Symantec (2015), *Internet security threat report*.

Verizon (2013), *Data breach investigations report.*

[17] Organización de Estados Americanos y Banco Interamericano de Desarrollo.

UNIVERSIDAD TORCUATO DI TELLA

7.2. Libros

Collazo, Javier & Saroka, Raúl (2010), *Informática en las organizaciones*, Fondo Editorial Consejo.

FIEL (1996), *Las pequeñas y medianas empresas en la Argentina*, Fundación de Investigaciones Económicas Latinoamericanas.

Fridman, Thomas (2005), *The world is flat*, Farrar.

Hill, Charles & Gareth, Jones (1996), *Administración estratégica. Un enfoque integrado*, McGraw-Hill Interamericana.

Kuong, Javier (1987a), *Computer auditing, security, & internal control manual*, Englewood Cliffs.

Kuong, Javier (1987b), *How to prepare audit test plans for EDP Systems*, Management Advisory Publications.

Maggiore, Marcia & Prandini, María Patricia (2010), *Normas internacionales y nacionales vinculadas a la seguridad de la información*, Editorial Buyatti.

Maristany, Jaime (2006), *Fundación y crecimiento de las PyMEs*, Fondo Editorial Consejo.

Moeller, Robert (1989), *Computer audit, control, and security*, Wiley.

Monforte, Manfredo (1994), *Sistemas de información para la dirección*, Pirámide.

Pérez Lalanne, Roberto (2000), *Investigación social*, Facultad de Ciencias Sociales de la Universidad Nacional de Lomas de Zamora.

Photopoulos, Constantine (2008), *Managing catastrophic loss of sensitive data*, Syngress.

Romero, Luis (2011), *Breve historia contemporánea de la Argentina*, Fondo de Cultura Económica de Argentina.

Samaja, Juan (1994), *Epistemología y metodología - Elementos para una teoría de la investigación científica*, Editorial Universidad de Buenos Aires.

Senge, Peter & otros (1995), *La quinta disciplina en la práctica*, Granica.

Sharma, Dhruv (2007), *Datathef: an emerging crime in the information technology & intellectual property regime,* Social Science research network.

Sturzenegger, Federico (2012), *Yo no me quiero ir*, Planeta.

Welsh, Sandra (2014), *Seminario de tesis MBA*, Universidad Torcuato Di Tella.

7.3. Normas internacionales

IRAM-ISO/IEC 27002:2008, *Código de práctica para la gestión de la seguridad de la información.*

ISO 15408:2009, *Evaluation criteria for IT security.*

ISO 31000:2009, *Risk management.*

7.4. Notas

Cruces, Juan José (2012, diciembre 5), *Cara y ceca de la economía kirchnerista*, Foco Económico: www.focoeconomico.org/2012/12/05/cara-y-ceca-de-la-economia-kirchnerista/.

Di Pace, Damián (2015, junio 27), *Un estudio ratifica el difícil momento de las pymes en Argentina*, Infobae: www.infobae.com /2015/06/27/1737123-un-estudio-ratifica-el-dificil-momento-las-pymes-argentina.

Fanelli, Maximiliano (2015, noviembre 9), *Tips para sumar un proyecto de seguridad en las pymes*, Tecnopymes: www.tecnopymes.com.ar/2015/11/09/tips-para-sumar-un-proyecto-de-seguridad-en-las-pymes/.

Peña, Ignacio (2014, marzo 15), *El próximo tsunami tecnológico*, La Nación: www.lanacion.com.ar/1672343-el-proximo-tsunami-tecnologico.

Ramirez, María (2014, octubre 2), *Los riesgos de seguridad en las pymes*, Revista Pymes: www.revistapymes.es/tecnologia-2/tecnologia_noticias/los-riesgos-de-seguridad-en-las-pymes-201410025527.htm.

UNIVERSIDAD TORCUATO DI TELLA

7.5. Sitios Web

Crear, Agencia de Desarrollo del Ministerio de Economía del Gobierno de Rio Negro: http://www.crear.rionegro.gov.ar/noticias/item/26.

Euromed Marseille School of Management: http://www.chris-kimble.com/Courses/World_Med_MBA/Types-of-Information-System.html.

Información Legislativa: http://www.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm.

Instituto Argentino de Normalización y Certificación: www.iram.org.ar/index.php?IDM=14&IDN=98&mpal=56&alias=ISO-IEC-27001.

International Organization for Standarization: www.iso27000.es/iso27002.html.

Information Systems Audit and Control Association: www.isaca.org/about-isaca/Pages/default.aspx.

Ministerio de Industria: www.industria.gob.ar/pymes/.

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

Fundación Observatorio Pyme: www.observatoriopyme.org.ar/espacio-pyme/.

Congreso y Feria Iberoamericana de Seguridad de la Información: www.segurinfo.org/detalle.php?a=segurinfo-argentina-2016&t=90&d=489

Business Continuity Institute: www.thebci.org

Asociación Argentina de Usuarios de la Informática y las Comunicaciones: www.usuaria.org.ar

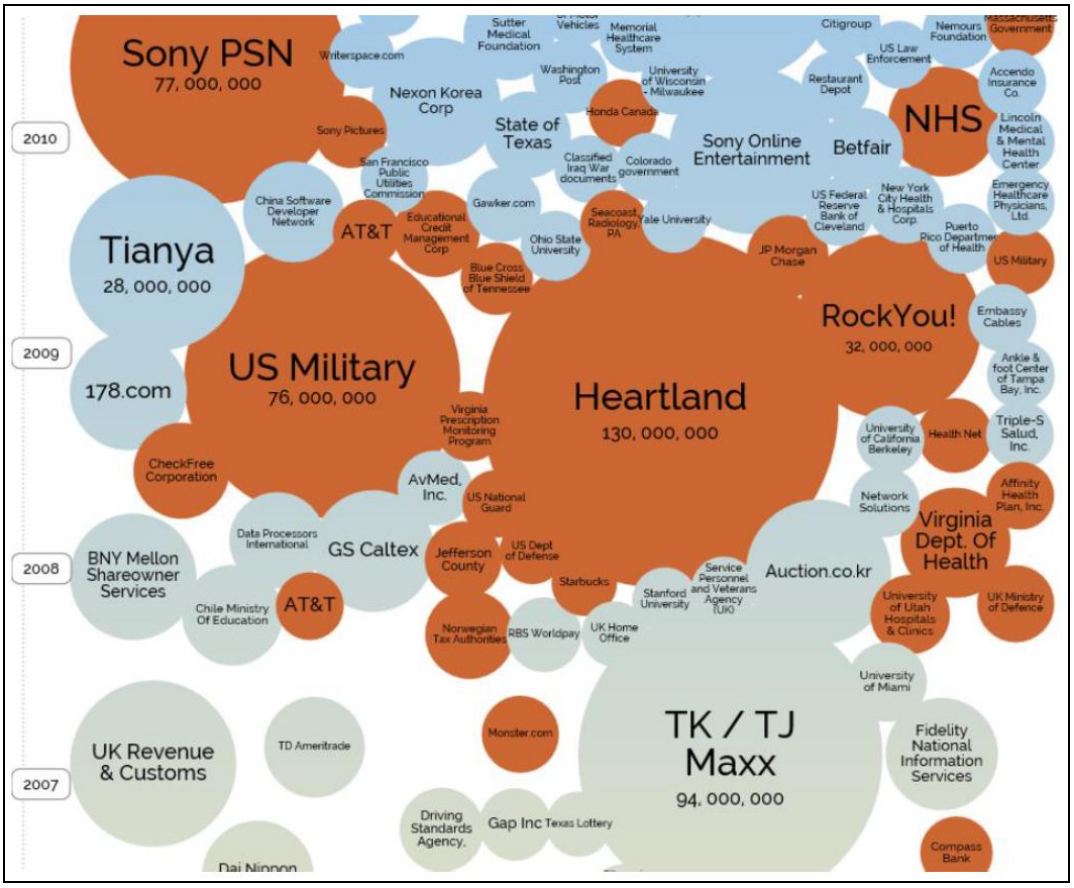
UNIVERSIDAD TORCUATO DI TELLA

8. ANEXOS

8.1. Anexo I: Infografía detallando las principales fugas de información en las organizaciones

En la infografía se detallan los principales hechos ocurridos alrededor del mundo a través de los años y el volumen de registros que han sido expuestos en cada incidente. Los casos con mayor impacto económico resultaron ser aquellos en los que se expusieron datos de tarjetas de crédito como ser los incidentes ocurridos en los sitios de comercio electrónico de TJ MAXX y Sony PSN, brindando a los atacantes el poder de realizar compras en otros comercios electrónicos sin mayores inconvenientes (FIGURA Nº 32).

FIGURA Nº 32: Infografía sobre fugas de información



Fuente: Deloite (2015), Gestión de cyber riesgos y seguridad de la información.

UNIVERSIDAD TORCUATO DI TELLA

No obstante, el caso con mayor impacto ha sido la fuga de documentos clasificados del ejército de los Estados Unidos y que han sido publicados en el sitio Wikileaks[18], marcando un quiebre en la concepción de fuga de información a nivel mundial.

[18] Organización internacional sin fines de lucro, que publica en su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes.

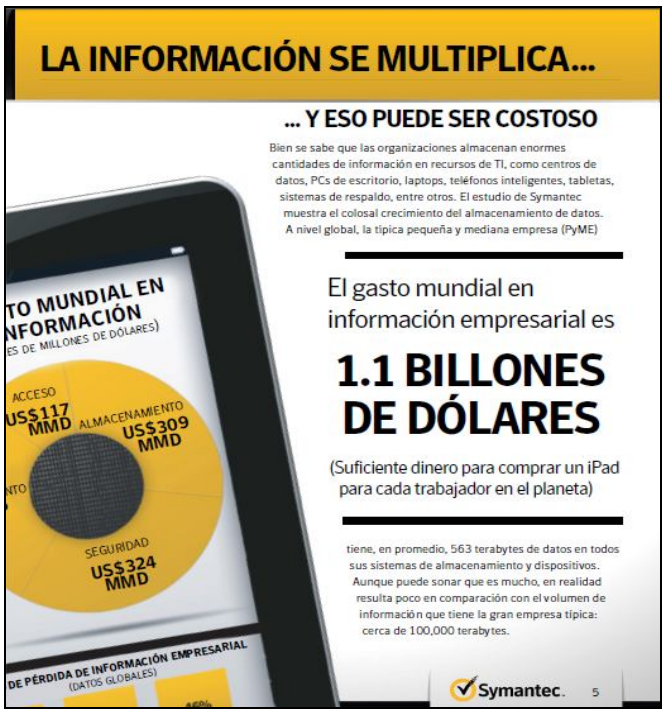
UNIVERSIDAD TORCUATO DI TELLA

8.2. Anexo II: Costo y manejo de la información empresarial

De acuerdo a la encuesta realizada por Symantec (2012), sobre el costo y manejo de la información empresarial, contactando a 4506 organizaciones en 36 países de América Latina, menciona que el gasto en el manejo de la información, cuando se extrapolan los números a todo el mundo, globalmente las organizaciones gastan US$1.1 billones de dólares en manejar su información (FIGURA N° 33), siendo la cantidad de información combinada para todas las empresas en todo el mundo de 2.2 zettabytes (un zettabyte equivale a mil millones de terabytes).

Un modo de visualizar esto es calcular que si 10 kilobytes de texto llenan una hoja de papel, todas las hojas apiladas tendrían una altura equivalente a 1,287 veces el Empire State, es decir 602 kilómetros de altura.

FIGURA Nº 33: Costos y manejo de la información empresarial



Fuente: Symantec (2012), Reporte sobre el costo y manejo de la información empresarial, resultados América Latina.

UNIVERSIDAD TORCUATO DI TELLA

En el mismo informe, se exponen porcentajes relacionada con el manejo de los datos. Dentro de los valores importantes de destacar, se menciona que en el último año, en promedio, cuatro de cada cinco empresas en América Latina perdió información importante, por causas tales como errores humanos falla de hardware o software, y pérdida o robo de dispositivos móviles (FIGURA Nº 34).

Además, casi tres cuartos de las empresas han experimentado la exposición de información confidencial importante fuera de la organización, y un tercio ha enfrentado cuestiones de cumplimiento normativo en el último año. Y una de cada tres organizaciones señaló que el crecimiento de la información es un factor importante cuando sucede algún imprevisto o pérdida de datos.

FIGURA Nº 34: Problemas reportados relacionados con información

Fuente: Symantec (2012), Reporte sobre el costo y manejo de la información empresarial, resultados América Latina.

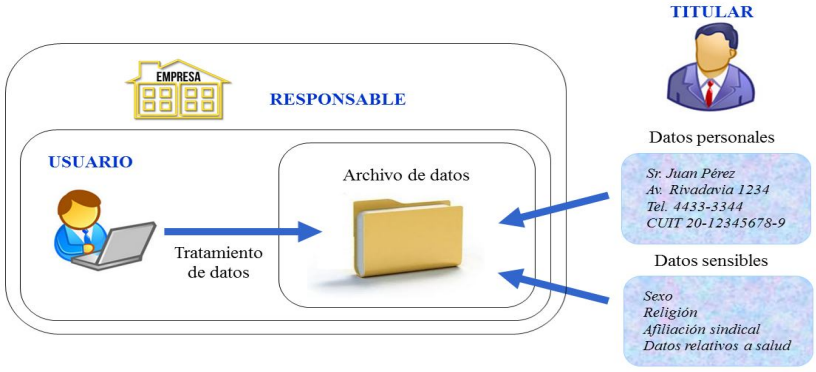
UNIVERSIDAD TORCUATO DI TELLA

8.3. Anexo III: Ley de Protección de Datos Personales

La Ley Nacional 25.326 de Protección de los Datos Personales adopta las siguientes definiciones (FIGURA Nº 35):

- Datos personales: de cualquier tipo referidos a personas físicas o jurídicas, determinadas o determinables.
- Datos sensibles: que revelen origen racial, étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.
- Titular: persona cuyos datos sean objeto de tratamiento.
- Responsable: persona física o de existencia ideal, pública o privada, que es titular de un archivo, registro, base o banco de datos.
- Usuario: persona pública o privada que realice el tratamiento de los datos, directamente o a través de conexión con los mismos.
- Archivo de datos: conjunto organizado de datos personales que sean objeto de tratamiento.
- Tratamiento: operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, almacenamiento, modificación, destrucción y en general, el procesamiento de datos personales, así como su cesión a terceros.

FIGURA Nº 35: Ley 25.326, roles y responsabilidades



Fuente: representación gráfica de roles y responsabilidades según dictamina la Ley 25326 de Protección de Datos Personales (elaboración propia).

UNIVERSIDAD TORCUATO DI TELLA

Las responsabilidades por parte de las organizaciones y los usuarios son:

- Administrar bases de datos registradas.
- Proteger los datos personales asentados en archivos, registros, bases o bancos de datos.
- Estén soportados en papel, planillas, bases de datos, CDs, pendrives, o cualquier dispositivo de almacenamiento.
- Proveer calidad, confidencialidad y seguridad a los datos asentados.
- Cumplir con los derechos de los titulares en cuanto al acceso, rectificación, actualización y/o supresión de los datos.
    - Brindar información de sus datos personales dentro de los 10 (diez) días corridos de solicitados.
    - Rectificar, actualizar y/o suprimirlos en un plazo máximo de 5 (cinco) días hábiles del reclamo, sin cargo alguno para el interesado.
- Tener los consentimientos informados para el tratamiento y cesión de datos.

Las principales medidas de seguridad emanadas por la Ley comprende:

- Nivel básico, obligatorio a partir de septiembre 2007:
    - Inclusión de rutinas de control de datos personales,
    - Disponer de documentación de seguridad,
    - Administración de contraseñas y perfiles de acceso,
    - Registración de incidentes de seguridad, otros.
- Nivel medio, obligatorio a partir de septiembre 2009:
    - Realización de auditorías,
    - Control de acceso físico, otros.
- Nivel crítico, obligatorio a partir de septiembre 2010:
    - Registros de accesos integrales para datos sensibles,
    - Encriptación y cifrado de datos en su traslado, otros.

UNIVERSIDAD TORCUATO DI TELLA

8.4 Anexo IV: Guía de preguntas realizadas durante las entrevistas

Preguntas sobre el conocimiento previo en seguridad de la información:

1. ¿Cómo definiría el significado del término “seguridad de la información”?

2. ¿Considera usted que la protección de la información podría ayudar a maximizar el retorno de la inversión de su empresa?, ¿de qué forma?

3. ¿Considera usted que la falta de protección de la información podría generarle problemas de alguna índole en su empresa?, ¿de qué forma?

Preguntas generales sobre temas relacionados con seguridad de la información:

4. ¿Poseen en su empresa un listado (inventario) de los distintos tipos de información que habitualmente utilizan/administran (por ejemplo: contratos y niveles de servicio con proveedores, resúmenes de cuentas bancarias, información de clientes, datos personales de los empleados, acuerdos de confidencialidad, tareas que se realizan diariamente, sistemas informáticos que utilizan, claves de cajas fuertes, contraseñas de ingreso al homebanking, etc.)?

   En caso afirmativo:

   5. ¿Está identificado este listado de manera escrita o sólo memorizado por aquellas personas según las funciones que realizan?

   6. ¿Está unificado en un único listado o cada sector dentro de la empresa tiene el propio (como ser: administración, recursos humanos y fábrica)?

   7. ¿Podría mencionarme aquellos que considere más importante para el negocio de su empresa?

8. ¿Clasifican en su empresa cada tipo de información de tal forma que permita determinar los niveles de importancia (por ejemplo: de conocimiento del personal para la ejecución de sus tareas diarias, de importancia para ser resguardada a conciencia, confidencial utilizada para la toma de decisiones, etc.)?

   En caso afirmativo:

   9. ¿Esta clasificación está escrita o memorizada?

   10. ¿Para su clasificación son conocidas y tenidas en cuenta las leyes y reglamentaciones vigentes relacionadas?, ¿podría mencionar cuáles aplican?

UNIVERSIDAD TORCUATO DI TELLA

11. ¿Analiza su empresa los posibles peligros que pudieran sufrir cada tipo de información (por ejemplo: una tarea de preparación de una máquina especial que sólo conozca un empleado a punto de jubilarse, corte de energía programado o de conexión al servicio de Internet por un período prolongado, que el antivirus no se haya actualizado y se instale un virus informático en todas las computadoras prohibiéndoles utilizarlas, etc.)?

    En caso afirmativo:

    12. ¿Este tipo de análisis incluye evaluar las posibilidades de ocurrencia que se produzcan, cuál sería su impacto para el negocio y qué tipo de controles serían convenientes implementar para minimizarlo?

    13. ¿Cada cuánto tiempo repite este análisis?

    14. ¿En las repeticiones se incluyen el tratamiento de nuevos peligros (por ejemplo: con la incorporación de nuevas máquinas para la producción, la fabricación de otros tipos de productos, la implementación de cambios en la funcionalidad de los sistemas, etc.)?

En caso afirmativo a algunas de las preguntas 4, 8 y 11:

15. Para las tareas de: confeccionar el listado, clasificar la información, analizar sus riesgos, implementar medidas de control y/o supervisar esta secuencia, ¿se tienen identificados los roles y designados los responsables directos que conocen sus funciones?

    En caso afirmativo:

    16. ¿Brinda la empresa a sus empleados algún instructivo de cómo realizar cada tarea o sólo se lo transmite verbalmente?

17. ¿Podría mencionar cuáles son los procesos más importantes relacionados con el negocio de su empresa?

18. Para estos procesos, ¿tienen analizados los posibles problemas que pudieran surgir y propuestas que permitan superarlos para continuar operando “casi” normalmente?

    En caso afirmativo:

    19. ¿Podría dar un ejemplo?

    20. ¿Estos planes están escritos?

    21. ¿Son conocidos por los empleados responsables de las tareas a desarrollar?

UNIVERSIDAD TORCUATO DI TELLA

22. ¿Son repasados y/o practicados cada lapso de tiempo prudencial?

23. ¿Brinda la empresa charlas de concientización en alguno de los temas conversados relacionados con seguridad de la información, a fin de fomentar la toma de conciencia e importancia en la operatoria?

Preguntas sobre la tecnología informática utilizada en la empresa:

24. ¿Tienen algún empleado que se encargue directa y exclusivamente de la tecnología, sistemas y herramientas informáticas que utilizan o alguna de estas tareas se encuentra tercerizada con un proveedor?

25. ¿Cuántos empleados atienden estos requerimientos?

En caso de contar con empleados propios:

26. ¿Tiene/n claramente definidas las funciones que realiza/n?

En caso de haber contratado servicios de terceros:

27. ¿Han firmado algún contrato/acuerdo de servicio con el proveedor?

28. ¿Han firmado algún acuerdo/cláusula de confidencialidad con el proveedor?

29. ¿Realizan visitas periódicas o sólo cuando requieren algún tema puntual?

30. ¿El proveedor envía siempre a las mismas personas?

31. ¿Luego de sus visitas, entrega el personal del proveedor algún informe de lo realizado?

32. ¿Alguna vez se han llevado algún equipo o información para analizar fuera de la empresa?

33. ¿Se encuentran documentadas estas actividades, ya sea las internas o las efectuadas por el proveedor?

34. ¿Son monitoreadas por algún responsable o superior?

En caso afirmativo:

35. ¿El superior a cargo posee los conocimientos técnicos necesarios que le permita comprender la magnitud de las operaciones realizadas, los riesgos implícitos para el negocio, los controles necesarios que deberían existir por cada tecnología/sistema y los planes de contingencia en caso de ocurrir alguna falla?

UNIVERSIDAD TORCUATO DI TELLA

36. ¿Cuentan los equipos principales con una adecuada protección física, dentro de algún recinto protegido bajo llave, con temperatura, instalaciones eléctricas y prevenciones contra incendio e inundación adecuadas? Hacer una breve descripción de cuáles y cuántos son los equipos y las características de resguardo con las que cuenta.

37. Debido a que todos los dispositivos utilizados (computadoras, servidores, tablets, smartphones, smarttvs, etc.) necesitan ser inicializados, configurados y actualizados por un usuario administrador que posea súper privilegios en el acceso, ¿tales cuentas de usuarios administradores se encuentran identificadas y protegidas?, ¿y los usuarios utilizados para la banca electrónica?

38. ¿Sus contraseñas están escritas y resguardadas, o son conocidas y usualmente utilizadas por las personas que las necesitan?, ¿son conocidas por el personal técnico, el supervisor y/o algún responsable de la empresa?, ¿se cambian periódicamente las contraseñas de estas cuentas de usuario? Hacer una breve descripción sobre la utilización de las cuentas de usuarios administradores y el estado de sus contraseñas.

39. ¿Poseen todos los dispositivos utilizados protección contra virus informáticos?, ¿los correos electrónicos tienen también configurado algún tipo de protección?, ¿la red inalámbrica y la navegación por Internet? Hacer una breve descripción del estado de situación y herramientas utilizadas.

40. ¿El resto de los empleados de la empresa que utilizan los sistemas y herramientas informáticas poseen una identificación unívoca y contraseñas propias para ingresar?

41. ¿Las funciones dentro de cada sistema se corresponden con las responsabilidades y roles que aplican a sus puestos de trabajo?

42. ¿Todos los empleados poseen cuentas propias de correo electrónico o sólo utilizan cuentas genéricas e impersonalizadas para enviar correos?

43. ¿Todos los sistemas informáticos y sus datos se encuentran resguardados en algún soporte de información?

    En caso afirmativo:

    44. ¿Habitualmente se llevan a cabo estas tareas después de cada actualización importante?

    45. ¿Qué tipo de soporte es?

    46. ¿El resguardo se hace manualmente o ejecutando algún programa?

    47. ¿Se protege este soporte en algún lugar fuera de la empresa?

48. ¿El soporte lo guarda el personal técnico, el supervisor o alguno de los responsables de la empresa?

49. ¿La información que se resguarda está encriptada de alguna forma o posee algún impedimento para que se acceda por personal no autorizado?

50. ¿Se hacen pruebas que permitan verificar que su contenido se encuentra íntegro en caso de necesidad de tener que recuperarlo?

51. ¿Utilizan los empleados y/o directivos información de la empresa almacenada en algún dispositivo fuera de sus instalaciones?

En caso afirmativo:

52. ¿Estos dispositivos son propios o de propiedad de la empresa?

53. ¿La información que allí reside se encuentra protegida para el acceso no autorizado por parte de alguna persona ajena?

54. ¿Se incluyen en los soportes de resguardos periódicos esta información?

55. ¿Existe un listado de las personas que los utilizan?, ¿es revisado periódicamente incluyendo las altas y bajas correspondientes, asegurándose que se hacen efectivamente?

Últimas preguntas generales:

56. Luego de haber respondido sobre aquellos temas que conforman los distintos ejes de la práctica de seguridad de la información, ¿considera que aplicando estos conceptos le permitiría a su empresa estar mejor preparada para afrontar algún tipo de situación anómala, con el fin de asegurar la continuidad normal de las actividades?

En caso afirmativo:

57. ¿De qué manera considera usted que aplicando estos conceptos le permitiría a su empresa mejorar las oportunidades de negocio?

58. ¿En qué forma piensa que le afectaría la falta de protección de la información de su empresa?

59. ¿Estaría usted dispuesto a contratar servicios profesionales que le brinden asesoramiento sobre el estado de situación en su empresa sobre temas de seguridad de la información, ofreciéndole sugerencias de cómo mejorarlo en caso de corresponder?

UNIVERSIDAD TORCUATO DI TELLA

60. ¿En caso afirmativo, cuál sería el rango que estaría dispuesto a pagar por dicho servicio, entre $1.000 y $5.000, entre $5.000 y $15.000, o entre $15.000 y $30.000?