Graduate School of Business
Masteren Dirección de Empresas

Tesis para optar al grado de Máster de la Universidad de Palermo en Dirección de Empresas

ADMINISTRACION DE LA SEGURIDAD DE LA INFORMACION BASADA EN LA GESTION DE RIESGOS EN LATINOAMERICA
Propuesta de mejoras en el proceso

Tesista: Guillermo F. Frick

Legajo: 74294

Director de tesis: Dr. Leandro A. Viltard

2016

Buenos Aires – Argentina

EVALUACIÓN DEL COMITÉ

AGRADECIMIENTOS

Quisiera agradecer a todos aquellos que genuina y desinteresadamente me han ayudado de una manera u otra para avanzar en el presente trabajo, y que con paciencia, apoyo, ánimo o conocimientos me han facilitado avanzar en la redacción de estas páginas.

Ninguno de ellos espera ser nombrados en estas páginas porque ellos ya han recibido su premio, mi más sincero agradecimiento, una sonrisa, un abrazo, un beso…

PRÓLOGO

"Es mucho mejor comprender el universo como lo que realmente es

que persistir en el engaño,

sin embargo satisfactorio y reconfortante."

Carl Sagan

En la actualidad, la información que las organizaciones crean, consumen, procesan y administran –siendo esta un activo clave y, en muchos casos, distintivo en la entrega de valor– debe ser protegida para evitar su pérdida, garantizar su disponibilidad, asegurar su integridad y proteger su confidencialidad. Todas estas actividades son englobadas bajo el nombre de "seguridad de la información".

El éxito de estos esfuerzos está determinado no sólo por la efectividad de los controles de seguridad que se implementan, sino que también, deviene de asegurar, mediante los mencionados controles, la mitigación de aquellos riesgos presentes en el contexto de operación de la organización. Allí es donde aparece el concepto de gestión de riesgos, aplicado específicamente al campo de la seguridad de la información, como el medio para su adecuada identificación y tratamiento.

El presente trabajo encuentra sus motivaciones principales en la importancia y relevancia de la gestión de riesgos de la información, proceso que, además, conlleva las siguientes exigencias y desafíos:

- La necesidad de contar con una cultura organizacional adecuada y de disponer

del apoyo de la dirección para implementar este proceso que, por sus características, alcanza todas las áreas de la organización;

- La exigencia de lidiar con un contexto vasto, complejo y en constante cambio, donde las amenazas y vulnerabilidades se renuevan día a día;
- La complejidad propia del proceso, que puede observarse en cada una de sus etapas, y que alcanza aspectos tales como la necesidad de disponer de la metodología de trabajo adecuada, los recursos humanos capacitados para llevar a cabo la tarea, la obligación de determinar el costo de activos intangibles, entre otros.

El alcance de la presente tesis contempló el estudio de los aspectos teóricos y formales en torno a la gestión de riesgos, así como también un estudio de campo que incluyó encuestas a distintas organizaciones, entrevistas a informantes-clave y análisis de un caso, para concluir resaltando los aspectos más relevantes que la gestión de riesgos –en el campo de la seguridad de la información– presenta en la actualidad.

A lo largo del presente estudio, se han encontrado algunas limitaciones a su alcance, que se encuentran expuestas a continuación:

- El Marco Teórico que brinda sustento a la presente investigación ha abarcado la bibliografía y publicaciones más relevantes en relación al tema bajo estudio. No obstante, no resulta posible afirmar que involuntariamente no se haya omitido otro material que pueda ser considerado de relevancia para los objetivos perseguidos por la presente tesis.

- Durante el desarrollo de la investigación, se pudo observar una limitación en la cantidad de participantes de laencuesta debido a la sensibilidad del tema abordado. Siendo que la encuesta buscaba explorar temas que la gran mayoría de las organizaciones considera confidenciales–esto es, la posición de seguridad de la organización– la encuesta se concentró en obtener respuestas de representantes de distintas organizaciones con algún tipo de vínculo personal, académico o profesional que sustente la confianza necesaria para brindar respuestas ciertas, lo cual significó una importante restricción a la hora de recabar datos del campo.
- Las conclusiones obtenidas como resultado de la presente investigación se basan en los elementos que se han tenido bajo consideración y que forman parte de este trabajo.

En cualquier caso, es importante clarificar que las limitaciones anteriormente indicadas no han representado un impedimento para obtener conclusiones razonables en relación a los objetivos e hipótesis del presente proyecto de investigación.

RESUMEN DE LA TESIS

Desde los orígenes de la historia el hombre se ha preocupado por resguardar la confidencialidad de aquella información considerada en modo alguno valiosa. Sin embargo, en los últimos años esta actividad ha cobrado una mayor relevancia, a partir del rol central de la información en las organizaciones modernas.

La hipótesis de la presente tesis considera la existencia de organizaciones que carecen de un enfoque integral de gestión de riesgos que garantice la adecuada protección de la información.

A partir de esto, se ha analizado el enfoque utilizado por diversas empresas para proteger sus activos de información, y en qué medida se encuentra extendida la práctica de la gestión de riesgos en el ámbito de la seguridad de la información.

A partir de la investigación realizada, fue posible validar la hipótesis de trabajo, así como también obtener importantes conclusiones acerca del proceso de gestión de riesgos y su aplicación práctica.

TABLA DE CONTENIDOS

INTRODUCCIÓN 1

METODOLOGÍA 8

1. MARCO TEÓRICO 13

1.1. Riesgo 13

1.2. Gestión de riesgos 17

1.3. Evaluación de riesgos 23

1.4. Tratamiento de los riesgos identificados 49

1.5. Marcos de gestión de riesgos, estándares y mejores prácticas 52

1.6. Conclusiones 56

2. MARCO INVESTIGATIVO 59

2.1. Encuesta a profesionales de seguridad de la información 59

2.2. Entrevistas a informantes-clave 69

2.3. Análisis del caso 72

2.4. Conclusiones 83

3. CONCLUSIONES, PROPUESTAS Y APORTES PARA FUTURAS INVESTIGACIONES 86

3.1. Generalización de los hallazgos 88

3.2. Conclusiones generales 88

3.3. Propuestas 99

3.4. Aportes para futuras investigaciones 103

3.5. Consideraciones finales 104

BIBLIOGRAFÍA 107

ANEXO I 109

ANEXO II 116

CURRíCULUM VITAE 118

LISTA DE CUADROS

Cuadro 1. Metodología de la investigación 11

Cuadro 2. Riesgo 16

Cuadro 3. Gestión de riesgos 22

Cuadro 4. Matriz de riesgos 36

Cuadro 5. Comparación de métodos de evaluación de riesgos 38

Cuadro 6. Métodos para el análisis de riesgos 40

Cuadro 7. Tratamiento de los riesgos 51

Cuadro 8. Marcos de gestión de riesgo 53

Cuadro 9. Estándares de gestión de riesgos 54

Cuadro 10. Prácticas líderes de gestión de riesgos 55

Cuadro 11. Detalle de informantes-clave 116

LISTA DE DIAGRAMAS

Diagrama 1. Lineamientos generales del presente trabajo I

Diagrama 2. Ejemplo de modelo de riesgos 29

Diagrama 3. Proceso de evaluación de riesgos 42

Diagrama 4. Organización corporativa inicial para la gestión de riesgos 75

Diagrama 5. Organización corporativa actual de seguridad 76

LISTA DE GRÁFICOS

Gráfico 1. Existencia de área responsable de la seguridad de la información 61

Gráfico 2. Propósito de la implementación de controles de seguridad 62

Gráfico 3. Ejecución de una evaluación de riesgos 63

Gráfico 4. Postura de la organización hacia la gestión de riesgos 64

Gráfico 5. Metodología de gestión de riesgos utilizada 65

Gráfico 6. Revisión regular de riesgos 66

Gráfico 7. Noción de la efectividad en la mitigación de riesgos 66

INTRODUCCIÓN

Antecedentes y motivos de la presente investigación

Las organizaciones en general, sin importar su propósito, buscan a través de distintos medios, alcanzar ciertos objetivos que éstas para sí mismas han establecido. En pos de esto, desarrollan diversas actividades e iniciativas que buscan aprovechar, e inclusive generar determinadas oportunidades, las cuales conllevan, no obstante, ciertos riesgos que se encuentran presentes en cada una de ellas. Estos riesgos deben ser debidamente administrados para alcanzar un balance adecuado entre las necesidades de la organización y el nivel de riesgo que esta desea asumir, actividad que es conocida bajo el nombre de "gestión de riesgos empresarial", según destaca Hubbard (2009).

Más específicamente, es posible decir que la gestión de riesgos consiste en "la identificación, evaluación y priorización de riesgos, seguido de aplicación coordinada y económica de recursos para minimizar, monitorear y controlar la probabilidad y/o el impacto de eventos desafortunados" (Hubbard, 2009, p. 10). Esta visión general acerca de la gestión de riesgos se aplica a los distintos procesos que la organización ejecuta, así como también a los activos que la organización posee, entre ellos, la información. Sin embargo, antes de profundizar sobre este aspecto, es preciso comprender la relevancia que en las organizaciones actuales la información posee, así como también la necesidad de protegerla que de ello se desprende.

En referencia a este tema, diferentes autores, entre los que es posible encontrar a Haag

y Cummings (2004) y Castells (2010), resaltan la importancia del conocimiento en la llamada "Era de la información". Profundizando sobre este aspecto, Haag y Cummings (2004) hacen hincapié en la relevancia de la información en las organizaciones del siglo XXI para obtener y sostener una ventaja competitiva, hecho que no solo afecta de múltiples formas a las organizaciones, sino que también impacta en los individuos que de ellas son parte y en la manera en que estos ejecutan sus tareas. Sin importar el rubro o industria en el que la organización se desarrolle, una gran cantidad de la población laboral se empeña en actividades que tienden a la generación y transmisión de información. En un contexto como el mencionado, Haag y Cummings (2004) también señalan la relevancia de tres factores distintos que se articulan en el contexto actual, a saber: información, tecnología de la información, y personas. Más aún, una visión mucho más amplia acerca del modo en que la tecnología y la información han impactado, no solo en el mundo de los negocios, sino en la sociedad como un todo es desarrollada por Castells (2010), aunque para los fines del presente estudio se tomaron sólo aquellos aspectos que a las organizaciones refiere.

Es entonces a partir del entendimiento sobre la preeminencia de la información en las organizaciones actuales que se desprende la necesidad de las organizaciones de proteger un activo tan crítico y determinante, del cual surge el concepto de protección de la información o seguridad de la información.

En última instancia, y como resultado de los dos conceptos principales expuestos en la presente sección, la gestión de riesgos y la importancia de la información en las

organizaciones actuales, es dable asumir que las actividades tendientes a proteger la información corporativa se realizan dentro del marco formal y metodológico de la gestión de riesgos, tanto en lo que respecta a la información considerada como un bien, así como también a los procesos de manipulación de la información. Sin embargo, es el objetivo del presente estudio desafiar esta creencia y profundizar sobre este aspecto en particular, según se podrá observar a lo largo de las páginas del presente estudio.

Definición del problema y las preguntas de la investigación

A partir de los conceptos presentados en la sección anterior es posible comprender, en términos generales, la necesidad de realizar una gestión adecuada de los riesgos relacionados a la información, de forma tal que el nivel de exposición de la organización a los mencionados riesgos se mantenga dentro de parámetros aceptables. Esto se logra mediante un correcto tratamiento de los riesgos, entendiéndose por esto la implementación de diversos controles de seguridad que permitan mitigar ya sea la probabilidad de ocurrencia o el impacto asociado a un riesgo específico (posteriormente en este trabajo se profundizará sobre las distintas alternativas para el tratamiento de los riesgos).

En este orden de ideas, es posible establecer que la implementación de controles de seguridad debe surgir como consecuencia de un análisis y evaluación detallada de los riesgos identificados. De no ser así, aquellos controles que sin esta evaluación se

desarrollen e implementen no dispondrán de un punto de referencia que permita hacer un análisis costo/beneficio del control, establecer su efectividad en lo que a la mitigación del riesgo refiere, comprender cuál será el riesgo residual –concepto sobre el cual también se indagará posteriormente–, y garantizar, adicionalmente, que todos los riesgos se encuentran dentro del rango de aceptación definido por la dirección.

Por el contrario, aquellas entidades que, aun dedicando recursos económicos a la protección de la información, lleven adelante la implementación de controles de seguridad basándose únicamente en las mejores prácticas del mercado, bajo la creencia de la universalidad de los controles de seguridad que en ellas se encuentran detallados, o en la percepción del riesgo que la empresa posea, se hallan expuestas a la posibilidad de encontrarse realizando tanto a un tratamiento deficiente de los riesgos. Esto puede darse sea que la organización se encuentre expuesta a riesgos particulares, inherentes a su actividad, que no estén cubiertos por las prácticas comunes del mercado, como así también podría darse en el caso que la organización invierta en controles para la mitigación de riesgos a los cuales no se encuentra expuesta, con una consecuente sobreinversión en controles de seguridad.

A partir de lo anteriormente expuesto, se desprenden los siguientes interrogantes que han permitido orientar la presente investigación:

- ¿De qué forma las organizaciones establecen sus requerimientos de protección de la información?
- ¿En qué medida las organizaciones llevan a cabo una práctica formal de gestión de riesgos en el campo de la seguridad de la información?

- ¿Cuáles son los principales aspectos que influyen en esta situación?
- ¿Cuáles son los desafíos que dicha actividad representa?

Hipótesis

El planteo del presente estudio responde a temas teóricos y prácticos que, a partir de los conceptos de seguridad de la información y gestión de riesgos anteriormente expuestos, permite establecer como hipótesis de trabajo la existencia de organizaciones con un enfoque de seguridad de la información predominantemente intuitivo, basado en la percepción que de los riesgos de la información se posee, pero que carecen de una visión formal de gestión de riesgos que abarque los procesos de negocio y la forma en que clientes, proveedores y los colaboradores de la entidad generan, consumen y almacenan la información, que permitiría identificar con claridad los riesgos de la información a los que la organización se encuentra expuesta y consecuentemente los controles de seguridad necesarios.

Objetivo general

Estudiar cuán extendida se encuentra la práctica de la gestión de riesgos dentro del campo de la seguridad de la información en Latinoamérica, analizando las causas que determinan dicha situación, a la vez de proponer mejoras que faciliten el proceso de evaluación de riesgos y permitan obtener mejores resultados.

Objetivos específicos

En pos de alcanzar el objetivo general establecido, los siguientes objetivos específicos fueron delineados:

- Estudiar los conceptos de riesgos y gestión de riesgos, profundizando sobre el proceso de evaluación de riesgos, sus etapas y las metodologías existentes para tal fin.

- Analizar cuál es la posición general de las organizaciones bajo estudio en relación a la gestión de riesgo empresarial, la gestión de riesgos de la información y la forma en que esto influye en la implementación de los controles de seguridad.

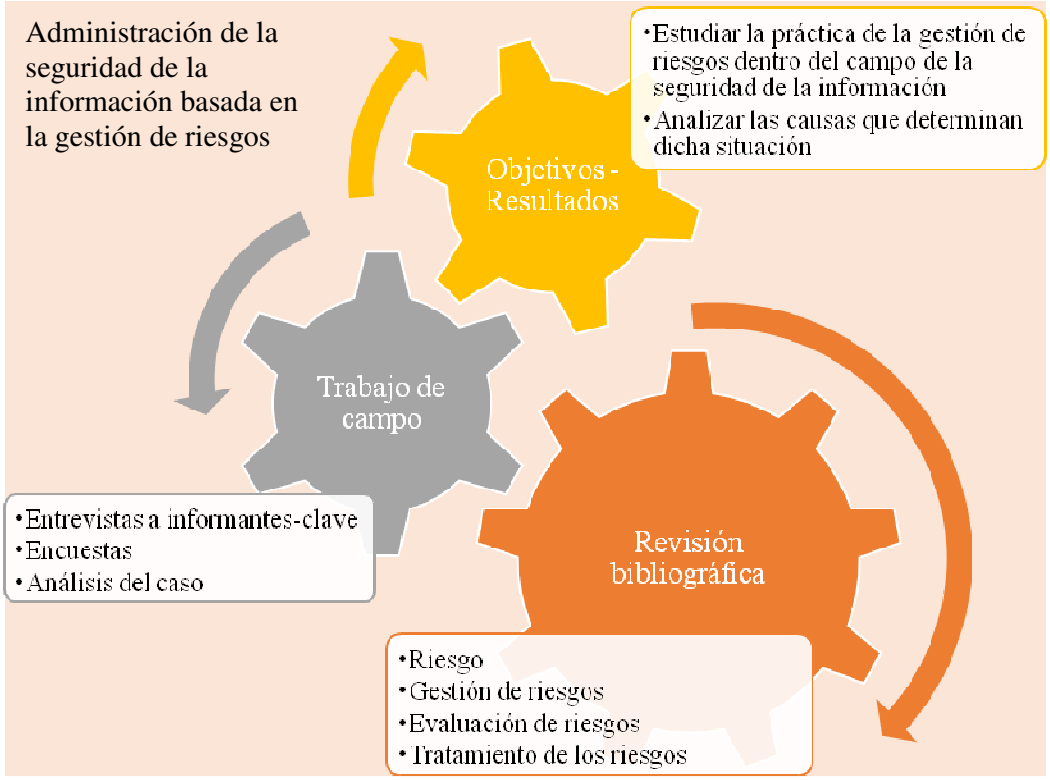
- Determinar cuáles son los factores que dificultan o impiden a las organizaciones desarrollar una estrategia de seguridad de la información basada en la gestión de riesgos.

- Proponer mejoras en el proceso de gestión de riesgos aplicado al campo de la seguridad de la información.

Lineamientos del presente trabajo

A los efectos de facilitar la lectura del presente estudio, en el diagrama conceptual expuesto a continuación se enseñan los principales lineamientos relativos a su contenido general:

Diagrama 1. Lineamientos generales del presente trabajo



Fuente: Elaboración Propia (2016)

METODOLOGÍA

El presente estudio es de carácter exploratorio descriptivo y, en general, se ha recurrido a una metodología cuali-cuantitativa, con predominio de trabajo cualitativo. Su diseño es no experimental y transversal, siendo que no se han manipulado las variables bajo estudio y la recolección de la información fue realizada en un momento dado de tiempo.

La unidad de análisis se encuentra conformada por las empresas incluidas en la muestra, tanto aquellas alcanzadas por la encuesta como para el análisis del caso. El criterio para la selección de la muestra no fue probabilístico sino intencional y dirigido, donde primó –por sobre otros aspectos– la posibilidad del acceso a la información, siendo que los tópicos consultados durante la investigación –relacionados a los controles de seguridad existentes– son considerados confidenciales en la amplia mayoría de los casos. A partir de esto, no se han realizado estimaciones cuantitativas, sino que el estudio realizado buscó interpretar conductas y situaciones, por lo que la presente muestra ha sido analizada como tendencia. De este modo, el estudio fue dirigido principalmente a empresas nacionales e internacionales de distinta envergadura, que incluyó desde empresas medianas hasta corporaciones multinacionales.

En lo que respecta a la encuesta utilizada durante la investigación, el tamaño de la muestra fue de 15 empresas, sobre un total de 30 cuestionarios enviados (sólo se recibió ese número de respuestas debido, seguramente, a la confidencialidad de la

información solicitada). Es importante recordar que al tratarse de una investigación cuali-cuantitativa, el tamaño de la muestra no implica una limitación al alcance. El análisis del caso se enfocó en una empresa particular según se podrá observar con mayor detalle posteriormente.

La unidad de respuesta han sido, en el caso de la encuesta mencionada, los profesionales a los que se les ha dirigido la consulta, diferentes profesionales del campo de la seguridad de la información para el caso de las entrevistas y, en última instancia, un ejecutivo de la organización bajo estudio en el análisis del caso.

El universo se encuentra definido por empresas que desarrollan sus actividades en el continente Americano en distintos segmentos de la economía, siendo que estas también difieren en su volumen de operación, países en los que poseen presencia y actividad principal.

La recolección de los datos ha implicado tres actividades clave: la construcción del instrumento de recolección, la aplicación del mencionado instrumento, y el posterior análisis de los datos obtenidos.

De entre las distintas técnicas para la recolección de datos disponibles, en primer lugar se ha optado por el envío de un cuestionario conteniendo preguntas abiertas y cerradas, que puede se puede encontrar en el ANEXO I, Formulario de encuesta a las empresas, y que fuera enviado a los distintos profesionales de las organizaciones incluidas en la muestra en forma electrónica durante el segundo semestre del año 2015. Este cuestionario buscó obtener información acerca de la situación de las

empresas incluidas en la muestra en relación a la implementación de controles de seguridad de la información y a la práctica de la gestión de riesgos.

La mencionada encuesta ha sido complementada con entrevistas semi-estructuradas realizadas a profesionales con amplia experiencia en el campo de la seguridad de la información y la gestión de riesgos, con el objetivo revisar la hipótesis planteada a la luz de la experiencia y visión de los especialistas consultados. A través de las mismas ha sido posible cubrir diversos interrogantes y aspectos del estudio en cuestión, según se puede observar en elANEXO II, Guía de entrevistas. Las entrevistas duraron aproximadamente una hora cada una, y se ha permitido al entrevistado, a partir de los lineamientos expuestos en el anexo citado anteriormente, exponer libremente sobre el tema en cuestión.

En último lugar, también fue utilizado, dentro de las técnicas de recolección de datos empleadas, el análisis de un caso correspondiente a una muy importante empresa de servicios radicada en Argentina, la cual, por motivos de confidencialidad, se ha mantenido en el anonimato. Como fuera mencionado anteriormente, su elección radica en el hecho de que, en una revisión preliminar, esta organización demostró tener una marcada evolución en la órbita de la gestión riesgos de la información en los últimos años, constituyéndose así en una importante fuente de información agregando profundidad al presente estudio al permitir una comparación entre los aspectos prácticos relevados y la teoría consultada en el presente trabajo.

Por último, es importante mencionar que este caso también ha sustentado, en gran medida, las recomendaciones y conclusiones finales de este estudio,

debido a su gran riqueza y la posibilidad de profundizar sobre todos y cada uno de los aspectos prácticos del objeto de estudio de la presente tesis.

Con el objeto de asegurar la validez de los resultados arrojados por el presente estudio, se ha efectuado una triangulación entre las distintas técnicas de recolección de datos empleadas -encuesta, entrevistas a informantes-clave y análisis del caso-, garantizando así la consistencia del análisis realizado. Adicionalmente, esto permitió enriquecer las conclusiones resultantes y facilitar la consistencia interna de la investigación.

La ubicación espacial de la presente investigación es la ciudad de Buenos Aires, Argentina, y su ubicación temporal abarcó desde marzo del 2015 hasta abril del año 2016.

Lo expuesto en el presente capítulo se puede observar en el siguiente cuadro:

Cuadro 1. Metodología de la investigación

Tipo de investigación	Exploratorio-descriptiva.
Metodología	Cuali-cuantitativa.
Diseño de la investigación	No experimental, transversal.
Unidad de análisis	Empresas.
Muestra	Intencional, dirigida y no probabilística.
Unidad de respuesta	Profesionales a los que se les ha dirigido la encuesta, especialistas del campo de la seguridad de la información y un importante ejecutivo de la organización bajo estudio en el análisis del caso.
Técnica de recolección de datos utilizadas	Cuestionario con preguntas abiertas y cerradas,entrevistas semi-estructuradas y análisis del caso.

Entrevistas	Semi-estructuradas a profesionales del campo de la seguridad de la información

Fuente: Elaboración Propia (2016)

1. MARCO TEÓRICO

El presente capítulo tiene por objetivo abarcar las temáticas necesarias que permitirán soportar, desde un punto de vista teórico, la presente investigación. Entre ellas es posible encontrar, en primera instancia, la definición del término "riesgo", a partir del cual se desarrollarán conceptos tales como la gestión, evaluación y mitigación de riesgos, revisando a su vez los distintos enfoques técnicos, metodológicos y conceptuales que se presentan para cada uno de ellos. Finalmente, también se realizará un breve resumen de los diferentes marcos de gestión, estándares y prácticas líderes reconocidas por el mercado que dan soporte a los conceptos presentados en este capítulo.

1.1. Riesgo

Siendo que el presente estudio tiene por objetivo realizar un análisis de la administración de la seguridad de la información basada en la gestión de riesgos, es de suma importancia tener una clara noción del concepto riesgo. Por tratarse de un término comúnmente utilizado, resulta sencillo tener una idea aproximada del significado de éste, aunque a los fines del presente trabajo deviene importante lograr un entendimiento preciso de su connotación y alcance.

Tomando como punto de partida la norma ISO 31000 (2009), es posible realizar una

primera definición del término riesgo como:“el efecto de la incertidumbre en la consecución de los objetivos” (p. 10).En esta breve definición, se observa la aparición de un elemento que se encuentra íntimamente relacionado con el riesgo, tanto en esta publicación como en otras, que es la incertidumbre. Más allá de lo mencionado, esta concepción tan general del término pareciera resultar – por si misma– insuficiente, por lo que se encuentra acompañada en la misma publicación de varias notas complementarias que permiten una mayor comprensión de su noción:

- Se comprende por efecto al desvío de aquello que es esperado, ya sea esto positivo o negativo;
- Incertidumbre es el estado de deficiencia de información, entendimiento o conocimiento, ya se parcial o total, sobre un evento, sus consecuencias o su probabilidad de ocurrencia;
- El riesgo es comúnmente relacionado a eventos potenciales, sus consecuencias y la probabilidad de ocurrencia de éstas.

A partir de estas notas, es factible resumir la definición de riesgo planteada por ISO 31000 (2009)como la posibilidad de observar desvíos del camino originalmente trazado para la consecución de objetivos, producto de la incertidumbre, los cuales resultarán en consecuencias que pueden ser cuantificadas, a la vez que resulta posible asignarles a dichos desvíos una determinada probabilidad de ocurrencia.

Adicionalmente, COSO (2004) entiende al riesgo a partir de la ocurrencia de eventos, los cuales pueden tener un impacto negativo, positivo, o de ambos tipos a la vez. La publicación establece que, producto de un contexto global complejo, una diversa

cantidad de factores generan incertidumbre que se presentan como resultado de la incapacidad para determinar con precisión la probabilidad de ocurrencia de los eventos y su respectivo impacto. Así, aquellos eventos que tengan impacto negativo representan un riesgo que pueden impedir la creación de valor o bien provocar una pérdida del valor existente. Los eventos con impacto positivo, por el contrario, representan oportunidades que derivan de la posibilidad que ocurra un acontecimiento que afecte positivamente al logro de los objetivos, facilitando la creación de valor o su conservación. Se concluye que un factor determinante en la definición de riesgo expresada en esta publicación se encuentra relacionada a la generación de valor, siendo que considera que toda organización, ya sea que tenga fines de lucro o no, tiene por objetivo la generación de valor para sus grupos de interés.

SEI (2010), con un enfoque ligeramente distinto, establece –como punto de partida para avanzar luego en una definición del riesgo– tres condiciones que deben ser satisfechas:

1. Debe existir la probabilidad de pérdida;
2. Debe presentarte una incertidumbre sobre el resultado final; y
3. Alguna decisión debe tomarse para administrar la incertidumbre y la potencial pérdida.

Los autores consideran que estos 3 conceptos son fundamentales a los efectos de forjar una definición muy básica del término riesgo, que se reduce al entendimiento del mismo como la posibilidad de sufrir una pérdida. También, presentan dos componentes básicos del riesgo, si se piensa en este concepto en términos de

causa-efecto, que son: las amenazas y las consecuencias. En este contexto, se entiende por amenaza a aquella circunstancia que podría producir una pérdida, en tanto que la consecuencia representa la pérdida que se sufriría en caso de que se materialice dicha amenaza. Adicionalmente surgen –relacionados a estos dos conceptos– la probabilidad de ocurrencia (resultante de la amenaza) y el impacto (como medida de magnitud de la consecuencia). Se observa que la publicación entiende al riesgo como un concepto con una denotación netamente negativa, ya que se lo asocia con la posibilidad de pérdidas y no como una potencial oportunidad.

Por otro lado, Hubbard (2009) realiza una definición del concepto de riesgo íntimamente relacionado con la incertidumbre, entendiéndola como la falta de una certeza absoluta, resultante en la existencia de más de una posibilidad. Siendo así, resulta desconocido el resultado, estado o valor de una determinada actividad o situación. En este orden de ideas, Hubbard define el concepto de riesgo como el estado de incertidumbre donde alguna de las posibilidades pueda incurrir en una pérdida, daño, catástrofe o cualquier otro resultado no deseado.

Los principales conceptos expresados en este apartado se presentan en el siguiente cuadro resumen:

Cuadro 2. Riesgo

ISO 31000	COSO	SEI	Hubbard

Es el efecto de la incertidumbre sobre los objetivos. Puede ser positivo o negativo.	Surge a partir de eventos cuyos efectos, positivos o negativos, facilitan o dificultan respectivamente la creación de valor.	Es la posibilidad de sufrir una pérdida. Las pérdidas surgen como consecuencia de la materialización de amenazas.	Es el estado de incertidumbre donde alguna de las posibilidades pueda incurrir en una pérdida, daño, catástrofe o cualquier otro resultado no deseado.

Fuente: Elaboración Propia (2016)

Si bien las distintas publicaciones establecen un factor común asociado al riesgo, que es la incertidumbre, la principal diferencia que se evidencia entre ellas radica en que tanto la ISO 31000 (2009) como COSO (2004) platean que los riesgos pueden tener efectos tanto positivos como negativos. Diferenciándose de esto, SEI (2010) y Hubbard (2010) establecen que el concepto de riesgo se encuentra necesariamente asociado a una pérdida.

Luego de haber revisado las posiciones de los diferentes autores citados, teniendo en consideración además el entendimiento socialmente aceptado de la palabra riesgo, es posible concluir, y será el significado que se asumirá para el desarrollo del presente trabajo, que la palabra riesgo representa la posibilidad (resultante de la incertidumbre) de ocurrencia de un evento que afecte en forma negativa los procesos y/o patrimonio de una organización.

1.2. Gestión de riesgos

A partir de las nociones desarrolladas en el apartado anterior, y habiendo logrado establecer claramente el significado del concepto de riesgo, es posible adentrarse

en la gestión de éstos, con el objetivo de lograr un entendimiento sobre sus implicancias y alcance.

COSO (2004) define a la gestión de riesgos como un proceso que se ejecuta en todos los niveles de la organización y estrechamente relacionado con la estrategia cuya finalidad es:

- Detectar la existencia de eventos potenciales que puedan repercutir en la organización, esto es, según se pudo observar en el apartado anterior, enfrentar determinados riesgos;
- Administrar los riesgos identificados dentro del marco de tolerancia establecido por la organización; y
- Proporcionar un nivel de certidumbre razonable en cuanto a la consecución de los objetivos.

A partir de estos entendimientos, la publicación establece una serie de componentes que conforman el proceso, los cuales resultan de utilidad para lograr una comprensión más amplia del concepto expresado, y que se detallan a continuación:

1. Ambiente interno: desarrollo de la cultura organizacional requerida para el tratamiento adecuado de los riesgos.
2. Establecimiento de objetivos: la relación entre objetivos y riesgos resulta sumamente estrecha, siendo que ambos se alimentan mutuamente para establecer objetivos que permitirán alcanzar la misión de la organización dentro del nivel de riesgo aceptado.

3. Identificación de eventos: detección de acontecimientos internos o externos que puedan afectar los objetivos, diferenciando riesgos y oportunidades (recordar que, según fue observado en el apartado anterior, esta publicación entiende que dentro del marco de gestión de riesgos existen eventos cuyo impacto puede ser tanto positivo como negativo).
4. Evaluación de riesgos: análisis de los riesgos identificados para determinar su probabilidad de ocurrencia e impacto.
5. Respuesta a los riesgos: a partir de los riesgos identificados y evaluados, determinación de las acciones a tomar para que se mitiguen, ya sea reduciendo su impacto o probabilidad de ocurrencia (este tema será desarrollado con mayor detalle en el apartado 1.4Tratamiento de los riesgos).
6. Actividades de control: observación y medición de la eficacia en la mitigación de riesgos.
7. Información y comunicación: identificación, elaboración y distribución de la información pertinente.
8. Supervisión: integral del proceso.

Resulta importante mencionar que las actividades indicadas no necesariamente deben ejecutarse en serie, donde cada una afecta a la siguiente, sino que se trata de componentes que deben ser articulados correctamente entre sí para lograr el éxito en la gestión de riesgos.

Por último, si bien todas las acciones que fueron detalladas anteriormente contribuyen al proceso como un todo, dos de ellas, sobre las cuales se profundizará

posteriormente, son claves para el resultado del proceso: la evaluación de riesgos y las acciones de respuesta o mitigación de estos.

Por su parte, NIST SP800-39 (2011) también define a la gestión de riesgos como una actividad multifacética que requiere la participación de todos los miembros de la organización. La publicación establece cuatro componentes que conforman el proceso:

1. Establecer el marco necesario para la toma de decisiones relacionadas al riesgo.
2. Evaluar los riesgos.
3. Responder a los riesgos identificados.
4. Monitorear permanentemente los riesgos (ya identificados y nuevos que puedan llegar a surgir).

El primero de estos componentes se refiere a la determinación de un marco o contexto organizacional para la gestión de los riesgos. Este componente busca establecer una estrategia clara en relación a los otros componentes del proceso; esto es, fijar la forma en que los riesgos serán evaluados, mitigados y monitoreados. Esto conlleva, además, establecer presunciones, restricciones, niveles de tolerancia a los riesgos y prioridades que serán utilizadas para guiar el proceso durante su ejecución.

El segundo de los componentes mencionados está relacionado con la identificación de los riesgos, a partir del análisis de amenazas, vulnerabilidades, probabilidad de ocurrencia e impacto, según se podrá observar con mayor detenimiento en el

apartado1.3Evaluación de riesgos. El proceso de gestión de riesgos debe establecer, en relación a este componente, roles y responsabilidades, herramientas y metodologías a utilizar, frecuencia de las evaluaciones, fuentes de información, y cualquier otro aspecto relacionado con la evaluación de riesgos.

Una vez determinados los riesgos, el tercer componente del proceso busca dar respuesta a éstos, mediante el desarrollo de distintos cursos de acción, la evaluación de cada uno de ellos y la selección del curso de acción más apropiado, de acuerdo con la estrategia de riesgos y el nivel de tolerancia que fueron determinados en el primero de los componentes del proceso. Al igual que en el componente anterior, la organización debe determinar herramientas y técnicas para la identificación de los cursos de acción posibles, su evaluación y –también– su comunicación dentro y fuera de la organización, cuando esto último fuese requerido por la legislación o regulación local.

El último componente establece la forma en que los riesgos serán monitoreados a lo largo del tiempo, con el objetivo de verificar que los planes de respuesta sean correctamente implementados, determinar su efectividad, e identificar nuevos riesgos que puedan surgir o bien cambios (como por ejemplo, en el impacto o probabilidad de ocurrencia) en los ya detectados. La organización requiere establecer la manera en que se determinará el nivel de efectividad de la respuesta a los riesgos y los mecanismos necesarios para monitorear los cambios en el contexto que puedan impactar en la efectividad de los controles ya implementados.

Es posible advertir que si bien –a simple vista– la cantidad de componentes del

proceso pareciera ser menor, el alcance de las actividades resulta similar al planteado en COSO (2004), y en esta publicación se puede notar también, tal vez con mayor claridad aun, la preponderancia de la evaluación de riesgos y los planes de mitigación o respuesta.

En último lugar, Hubbard (2009) define a la gestión de riesgos como la identificación, evaluación y priorización de los riesgos, seguido de la aplicación de recursos para minimizar, monitorear y controlar la probabilidad y/o impacto de eventos que puedan afectar los objetivos de la organización.

Una vez más, se puede destacar –como ejes del proceso– a la evaluación de riesgos y a las acciones que de ella resultan.

En el siguiente cuadro, se observan los conceptos clave desarrollados en este apartado:

Cuadro 3. Gestión de riesgos

COSO	NIST SP800-39	Hubbard
Detección y administración de riesgos dentro del marco de tolerancia establecido, con el objetivo de proporcionar un nivel de certidumbre razonable sobre el cumplimiento de los objetivos.	Definición del marco organizacional necesario, evaluación y respuesta a los riesgos identificados, seguido del monitoreo permanente.	Identificación, valuación y priorización de los riesgos, seguido de la aplicación de recursos para minimizar su probabilidad y/o impacto, acompañado del monitoreo de estos.

Fuente: Elaboración Propia (2016)

Como se advierte en el Cuadro 3, los autores y publicaciones citados realizan una definición muy similar del proceso de gestión de riesgos, con mayor o menor nivel de

detalle en cada caso. Tal vez, la mayor diferencia se puede advertir en Hubbard (2009), donde el autor omite mencionar la necesidad de establecer un contexto organizacional propicio para el desarrollo de esta actividad.

Finalmente, y a los fines del presente trabajo, es posible concluir que el proceso de gestión de riesgos tiene por objetivo proporcionar un determinado nivel de certeza sobre la consecución de los objetivos de la organización, cualesquiera sean éstos, conforme con el nivel de tolerancia al riesgo establecido. Éste se compone de diferentes actividades, entre las cuales se destacan –como principales– la evaluación de los riesgos y su mitigación o tratamiento, las cuales se estudiarán en detalle en los apartados siguientes.

1.3. Evaluación de riesgos

El apartado anterior permitió revisar el concepto de gestión de riesgos, dentro del cual se mencionó la relevancia de la evaluación de riesgos como uno de los pasos más determinantes del proceso, la que, tal vez, representa su punto más sensible, no sólo porque representa el punto de partida para las acciones que, a partir de la identificación de un riesgo se desatan, sino –también– porque cualquier error u omisión en el análisis puede poner en riesgo la consecución de los objetivos de la organización, y hasta a la propia organización. Es preciso considerar que esto puede ocurrir no solo en aquellos casos en que potenciales riesgos no sean detectados, sino –también– en situaciones donde los riesgos identificados no sean adecuadamente mensurados. Riesgos que sean subestimados expondrán a la organización a situaciones de peligro bajo una falsa sensación de seguridad, mientras que, por

el contrario, otros que sean sobreestimados implicarán planes de mitigación más costosos de lo necesario, generando una ineficiencia en el uso de los recursos, ya sean éstos humanos o económicos.

A partir de lo mencionado, en el presente apartado se revisará con detalle los pasos que son precisos recorrer con el fin de realizar una evaluación de riesgos, a la vez que se abordarán los distintos enfoques y variantes para el desarrollo de esta actividad.

Metodología de evaluación de riegos

NIST SP800-30 (2012) establece, como puntapié inicial para avanzar en este proceso, la necesidad de disponer de una metodología de evaluación de riesgos que desarrolle los siguientes componentes:

- El proceso de evaluación de riesgos.
- Un modelo de riesgos, que defina los términos que serán utilizados, los factores de riesgo a evaluar y la relación entre estos.
- Un enfoque o método para la evaluación de los riesgos (entre los que se encuentran el cuantitativo, cualitativo y el semi-cualitativo), que determine los valores que los distintos factores de riesgo pueden tomar durante el análisis y la forma en que estos factores pueden ser combinados para evaluar el riesgo.
- Un enfoque o método para el análisis de los riesgos (por ejemplo: enfocado en las amenazas, enfocado en las vulnerabilidades), que describa de qué manera las combinaciones de los factores de riesgos serán identificadas y

analizadas para garantizar una completa cobertura de la situación a evaluar.

La metodología de evaluación de riesgos es parte de la estrategia de riesgos y debe ser claramente establecida por la organización, la que implica el marco de trabajo que determinará la forma en que las actividades de evaluación de riegos deben ser conducidas.

Asimismo, diversos aspectos pueden influir en las organizaciones a la hora de desarrollar la metodología a utilizar, tales como la madurez o complejidad de los procesos de la organización, la sensibilidad de la información y los sistemas que dan soporte a los procesos de negocio, los plazos requeridos para la planificación de inversiones, entre otros.

En los apartados que se presentan a continuación se analizará –con mayor detenimiento– los componentes de la metodología de evaluación de riesgos propuestos por NIST SP800-30(2012).A los fines de obtener un mayor entendimiento del proceso de evaluación de riesgos, se profundizará –en último lugar– en este componente de la metodología.

Sin embargo, antes de avanzar en el mencionado análisis, es posible adelantar que la metodología de evaluación de riesgos establece el marco organizacional y las reglas que deben ser observadas para el desarrollo de todas las actividades para llevar a cabo la evaluación de riesgos.

Modelos de riesgos

De acuerdo a lo que se observa en NIST SP800-30 (2012), los modelos de riesgo definen los factores de riesgo que serán tenidos en cuenta en la evaluación y –además– la relación que entre ellos existe.

Los factores de riesgo comúnmente considerados son:

- Amenazas.
- Vulnerabilidades.
- Condiciones predeterminantes.
- Probabilidad de ocurrencia.
- Impacto.

Deviene importante que la organización posea un claro entendimiento del significado de estos términos, siendo que –a partir de ellos– se establecerá la potencial existencia de riesgos y el impacto que éstos tendrían en la organización.

Antes de proseguir con el análisis de los factores de riesgo, es necesario destacar que NIST SP800-30 (2012) desarrolla estos conceptos con un notable enfoque hacia el análisis de los riesgos de seguridad de la información. Siendo que esta aproximación se encuentra alineada con el objeto de estudio de la presente tesis, se tomará esto como una oportunidad para lograr un acercamiento a la evaluación de riesgos dentro del mencionado campo.

Aclarado este punto, y continuando con el análisis que NIST SP800-30 (2012) realiza,

es posible establecer que se considera una amenaza a cualquier evento o situación que podría afectar negativamente la operación de la organización, sus activos, individuos u otras organizaciones a través de los sistemas de información, ya sea mediante un acceso no autorizado, la destrucción, divulgación o modificación de información y/o la denegación de servicios. Estos eventos que representan amenazas son causados por una o varias fuente de amenazas.

Una vulnerabilidad, en cambio, es una debilidad presente en un sistema de información, procedimientos o controles internos que podría ser explotado por una fuente de amenazas. Muchas veces las vulnerabilidades son el producto de la implementación deficiente o defectuosa de controles de seguridad, pero en muchas ocasiones son el resultado de la introducción de nuevas tecnologías, cambios en los procesos o contexto, o sencillamente la detección de vulnerabilidades preexistentes sobre las que no se tenía visibilidad. Como resultado, los controles de seguridad existentes pueden no ser suficientes y deben ser revisados a los efectos de verificar su efectividad y vigencia.

Además de las vulnerabilidades mencionadas, las organizaciones deben –asimismo– considerar la existencia de condiciones predeterminantes, las que –existentes en los sistemas de información, procesos de negocio, o el entorno de operación, citando solo algunos ejemplos– afectan la probabilidad de ocurrencia de las amenazas, ya sea aumentando o disminuyendo esta. A modo de ilustración, es posible considerar como una condición predeterminante la ubicación física de instalaciones en zonas de terremotos o huracanes, lo cual aumentaría la probabilidad de ocurrencia de alguno de

estos eventos. Otro ejemplo, relacionado con la tecnología, se puede encontrar en la existencia de sistemas de información obsoletos, que podrían facilitar el acceso no autorizado a estos, y por lo tanto aumentarían su probabilidad de ocurrencia.

La probabilidad de ocurrencia se encuentra establecida a partir de la probabilidad de una amenaza determinada de explotar una vulnerabilidad específica o un conjunto de ellas. Esta representa una combinación de la probabilidad de que una amenaza se inicie junto con la probabilidad de que dicha amenaza logre algún impacto adverso.

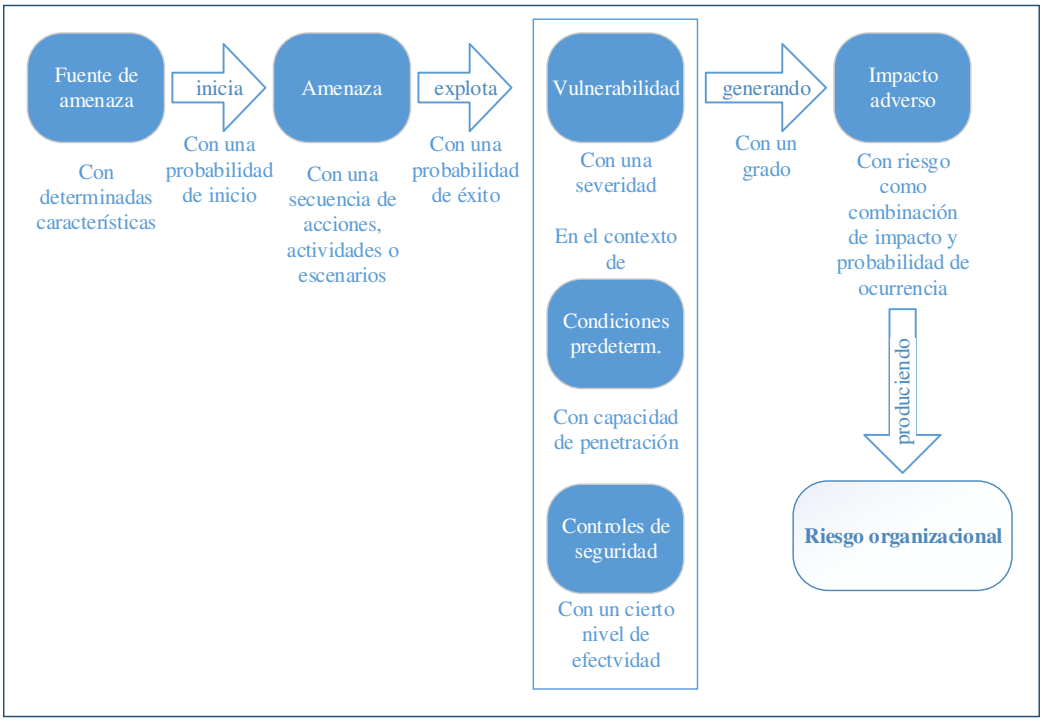
Distintos aspectos deben ser considerados al momento de evaluar la probabilidad que una amenaza se inicie, tales como la evidencia histórica, datos empíricos, y –también– la posibilidad de ser objetivo de ataques específicamente dirigidos hacia la organización. Asimismo, se deben considerar las condiciones predeterminantes que fueron previamente mencionadas, y la existencia y efectividad de controles de seguridad que limiten la presencia de vulnerabilidades y minimicen el impacto que de la explotación de ellas resultaría. Específicamente, en lo que respecta al análisis de la probabilidad que una determinada amenaza resulte en un impacto adverso, se deben considerar todos los eventos que puedan incurrir en algún tipo de daño, sin importar la dimensión de éste.

En último lugar, el nivel de impacto de un evento representa la magnitud del daño que puede resultar del éxito de una amenaza en explotar una vulnerabilidad. Este impacto tanto puede observarse como un resultado directo en los activos, sistemas o procesos que puedan verse afectados, así como también, en forma indirecta en otros procesos

organizacionales o inclusive la misión de entidad.

En el diagrama que se observa a continuación, se observa un ejemplo de modelo de riesgos que incluye y permite visualizar claramente todos los factores de riesgo anteriormente mencionados, así como también, la relación entre ellos:

Diagrama 2. Ejemplo de modelo de riesgos



Fuente: NIST SP800-30 (2012)

Lo observado en el presente apartado permite determinar que el modelo de riesgos es aquel que establece los diferentes factores que deben ser tenidos en cuenta a la hora de analizar el contexto en el que la organización se desempeña, a la vez que –también– indica cómo dichos factores deben ser articulados entre sí. Estos factores y su interrelación deben ser estudiados a los fines de poder identificar la presencia de

riesgos. La forma en que dicho estudio se llevará a cabo dependerá de los métodos para la evaluación y análisis de riegos que la organización adopte, y que se revisarán a continuación.

Métodos para la evaluación de riesgos

En primer lugar, se permite distinguir, según presenta NIST SP800-30 (2012) y Harris (2013), entre el enfoque cuantitativo y el cualitativo. En el primero de éstos se asignan valores numéricos a todos los elementos del análisis. Cada uno de ellos (tales como valor del activo, probabilidad de ocurrencia, daño del impacto y otros que son parte del proceso) es cuantificado e incluido en la ecuación del riesgo para determinar el riesgo total. En cambio, el enfoque cualitativo utiliza una aproximación menos precisa en el análisis de los distintos elementos de la evaluación de riesgos, aunque no necesariamente signifique que no se utilizan valores numéricos. En este tipo de análisis se utilizan estimaciones para establecer escalas numéricas del 1 al 5, o niveles de riesgo tales como crítico, alto, medio y bajo.

Cada uno de estos métodos cuenta con sus ventajas y desventajas, y los defensores y detractores de cada uno de ellos son fervientes en sus convicciones. Hubbard (2009) hace una fuerte crítica a los métodos cuantitativos, sobre el cual señala múltiples fallas en cada uno de sus pasos, atribuibles a la falta de precisión de los individuos para calificar objetivamente una determinada situación o circunstancia, (claro está, al prescindir de los métodos estadísticos que son utilizados en el método cuantitativo),

dificultades para lograr un entendimiento común sobre los distintos niveles de riesgo, y ausencia de un enfoque holístico, entre otros. Por su parte, aquellos autores y publicaciones defensoras del análisis cualitativo señalan que el enfoque cuantitativo resulta sumamente complejo de aplicar y hasta impracticable en alguno casos donde los eventos son discretos y de baja recurrencia (como podría serlo un terremoto o un atentado terrorista) y –además– resultan más complejos de comprender, según señala NIST SP800-30 (2012). Inclusive, esta mención hace referencia al elevado costo que podría ser requerido para desarrollar un análisis cuantitativo.

ISACA (2014) presenta un breve resumen de las ventajas y desventajas de ambos métodos. En lo que respecta al método cuantitativo, señala los siguientes beneficios:

- Permite la clasificación y contabilización de los datos recolectados.
- Admite el uso de modelos estadísticos para explicar el comportamiento observado.
- Facilita la extrapolación de datos y la comparación entre distintas muestra estadísticas.
- Produce resultados estadísticamente confiables.
- Permite descubrir fenómenos con alta probabilidad de ocurrencia y diferenciarlos de aquellos que raramente pueden presentarse.

Por el contrario, ISACA (2014) también expresa los siguientes desafíos que plantea este método:

- No siempre resulta fácil recolectar datos asociados a todos los procesos

relevados.

- Los datos pueden no estar en el formato necesario para ser analizados y procesados por este método.
- Puede resultar difícil obtener información histórica confiable que permita la cuantificación de las fallas de procesos o los riesgos resultantes de ellas.
- La información del pasado no siempre permite predecir eventos futuros.
- Resulta difícil aplicar modelos estadísticos a eventos poco frecuentes.
- El costo del análisis cuantitativo es generalmente muy superior al costo del análisis cualitativo.

En cuanto al método cualitativo, ISACA (2014) indica los siguientes beneficios:

- El costo del análisis cualitativo es generalmente inferior al costo del análisis cuantitativo.
- Generalmente este análisis permite un mejor entendimiento de las dependencias entre unidades de negocios y la interacción entre ellas.
- Este tipo de análisis se encuentra basado en el consenso alcanzado entre los analistas, y generalmente representa más acertadamente los puntos de vista utilizados como fuentes de información del proceso.
- Generalmente es mejor para evaluar riesgos intangibles, como aquellos relacionados con cuestiones éticas o que afecten la reputación.

En último lugar, ISACA (2014) destaca también los desafíos del método cualitativo:

- Subjetividad en la recolección de datos.

- Énfasis exagerado en eventos de relevancia menor.
- No provee información relevante para un análisis costo-beneficio.
- Los niveles de riesgo utilizados pueden no tener significado fuera del contexto de la organización.

Adicionalmente, NIST SP800-30 (2012) hace mención a los métodos semi-cuantitativos de análisis, en donde, en lugar de utilizar niveles o categorías de riesgo como en el caso del análisis cualitativo, se utilizan rangos numéricos. Esta clasificación es difícil de encontrar en otras publicaciones o referenciadas por otros autores y, siendo que en su esencia, no se basa en análisis estadísticos y sí utiliza, en cambio, estimaciones para determinar cuál sería el rango más apropiado para una determinada situación o circunstancia, es posible considerar que se trata de una variante más del método cualitativo.

Método cuantitativo

Según se pudo observar, la utilización del método cuantitativo para el análisis de riesgo implica utilizar ecuaciones matemáticas para el proceso de interpretación de datos. Harris (2013) propone, como las ecuaciones más utilizadas para tal fin, a la "expectativa de perdida individual" (SLE, por su nombre en inglés *Single Loss Expectancy*) y la "expectativa de pérdida anual" (ALE, por su nombre en inglés *Annual Loss Expectancy*).

El SLE es el costo asignado a un determinado evento que representa la

pérdida que la organización sufriría de acontecer una amenaza específica. La fórmula del SLE es la siguiente:

costo del activo x EF = SLE

El EF es el "factor de exposición" (por su nombre en inglés, *Expossure Factor*), que representa el porcentaje de pérdida de un determinado activo en caso que suceda un evento específico. Tomando el ejemplo de Harris (2013), si un depósito de una empresa (activo) se encuentra valuado en $150.000, y se estima que en caso de incendio un 25% de este se vería afectado, entonces el SLE sería de $37.500.

costo del activo ($150.000) x EF (25%) = SLE ($37.500)

Este valor indica que, en caso que se produzca un incendio, la pérdida sería de $37.500. Sin embargo, continuando con lo establecido en este método, el valor debe ser anualizado, utilizando la siguiente ecuación:

SLE x ARO = ALE

EL ARO es el "ratio anual de ocurrencia (por su nombre en inglés *Annual Rate of Ocurrence*), que representa la frecuencia de ocurrencia de un determinado evento en el plazo de un año. Este ratio se encuentra entre los valores 0,0 (nunca) hasta 1,0 (una vez al año). Continuando con el ejemplo anterior, en el caso que la frecuencia de un incendio es de uno en 10 años, el valor correspondiente de ARO sería de 0,1, con un ALE de $3.750.

SLE ($37.500) x ARO (0,1) = ALE ($3,750)

Este valor sugiere que, en caso que la organización deseara establecer medidas para mitigar este riesgo, el costo de dichas medidas no debiera ser superior a los $3,750 que resultarían de la ocurrencia del evento analizado.

Nótese que, aun cuando el presente desarrollo corresponde a un ejemplo de análisis cuantitativo, algunos de los elementos que lo componen son meramente subjetivos, tales como el porcentaje de daño que se produciría en el depósito en caso de incendio, o bien la frecuencia de ocurrencia anual del evento. Hubbard (2009) propone–como solución a los fines de lograr una aproximación más científica para obtener estos valores que deben ser estimados– el uso de la simulación Monte Carlo, la que permite, aún en situaciones de incertidumbre, establecer rangos de probabilidades que pueden ser utilizados con una mayor base científica que la mera especulación de los especialistas consultados.

Método cualitativo

En lo que respecta al análisis de riesgos utilizando el método cualitativo, Harris (2013) establece que este método, a diferencia del anteriormente planteado, no asigna valores numéricos y monetarios a los distintos componentes del análisis y los riesgos identificados, sino que –en base al juicio, opiniones y experiencia de los analistas– recorre diferentes escenarios de riesgo y asigna distintos niveles de gravedad o

exposición, según sea el caso.

El equipo de análisis debe estar conformado por personas con la suficiente experiencia y conocimiento acerca de las amenazas a ser evaluadas para determinar el nivel de exposición de las vulnerabilidades presentes en los activos a la amenazas anteriormente identificadas, su probabilidad de ocurrencia (no en términos numéricos) y el daño potencial que podría resultar.

A partir de esto, se asignan valores discretos a la probabilidad de ocurrencia y al impacto que, de acuerdo al criterio seleccionado, pueden obtener valores numéricos en una escala del 1 al 5, se puede utilizar una escala de valores alto, medio y bajo, o cualquier otro criterio que permita determinar distintos niveles para los factores evaluados.

En el cuadro que se muestra a continuación, se podrá observar –a modo de ejemplo– una matriz de riesgo, la cual permite obtener, a partir de valores discretos de probabilidad de ocurrencia e impacto, distintos niveles de riesgo (a modo de referencia, se considera B: bajo, M: medio, A: alto, E: extremo):

Cuadro 4. Matriz de riesgos

Probabilidad de ocurrencia	**Impacto**				
	Ínfimo	Menor	Moderado	Mayor	Severo
Casi certeza	M	A	A	E	E
Muy probable	M	M	A	A	E
Posible	B	M	M	A	E

Poco probable	B	M	M	M	A
Excepcional	B	B	M	M	A

Fuente: Harris (2013)

Para observar el uso que se le da a la matriz expuesta en el Cuadro 4, se tomará como ejemplo el análisis del riesgo que un virus infecte una computadora. Si como resultado de dicho análisis se determina que la probabilidad de que este evento suceda es "Poco probable", y a la vez se establece que, en caso que dicho evento suceda, el impacto sería "Moderado", entonces es posible determinar que el riesgo que un virus infecte una computadora es un riesgo "Medio".

Se observa que, a diferencia del método analizado anteriormente, donde se obtenía como resultado final un valor numérico (ALE = $3.750), en el caso del método cuantitativo el resultado en este caso es una ponderación "Medio", que sólo tiene sentido dentro del marco planteado por la metodología de evaluación de riesgos definido por la organización.

Observaciones finales sobre los métodos de evaluación de riesgos

Luego de haber estudiado con detalle los métodos cuantitativos y cualitativos de evaluación de riesgos, en el siguiente cuadro se observan las características más representativas de cada uno de ellos:

Cuadro 5. Comparación de métodos de evaluación de riesgos

Método	Cuantitativo	Cualitativo
Enfoque	Se asignan valores numéricos a todos los elementos del análisis, que son cuantificados e incluidos en la ecuación del riesgo para determinar el riesgo total.	Se utilizan estimaciones para establecer escalas discretas o niveles de riesgo tales como crítico, alto, medio y bajo a los factores de riesgo y, por consiguiente, al riesgo resultante.
Ventajas	• Admite el uso de modelos estadísticos. • Produce resultados estadísticamente confiables. • Los datos pueden ser clasificados y contabilizados.	• El costo de este análisis es generalmente inferior. • Es mejor para evaluar riesgos intangibles. • Los resultados surgen a partir del consenso de los participantes.
Desventajas	• Dificultad para recolectar datos. • La información del pasado no siempre permite predecir eventos futuros. • El costo de este análisis es generalmente superior.	• Subjetividad en la recolección de datos. • Énfasis exagerado en eventos de relevancia menor. • No provee información relevante para un análisis costo-beneficio.

Fuente: Elaboración Propia (2016)

Finalmente, es posible concluir, a partir de los conceptos observados, que no existe un método que sea necesariamente mejor que el otro, sino que la selección de aquel que resulte apropiado dependerá de varios factores, entre los que es posible citar: la experiencia de los analistas, la madurez de la organización en relación a la gestión de riesgos, la factibilidad de obtener información cuantificable, el alcance u objeto del análisis, entre otros. A partir de esto, es responsabilidad de cada entidad establecer el método a utilizar como parte de su metodología de evaluación de riesgos.

Métodos para el análisis de riesgos

Continuando con lo expuesto por NIST SP800-30 (2012), es posible identificar distintos métodos para la evaluación de riesgos, los cuales difieren entre sí en relación a punto de partida para el análisis, el nivel de detalle en la evaluación y la forma en que el riesgo resultante de escenarios con amenazas similares es tratado.

Se presentan tres tipos de enfoques:

- Orientado a las amenazas.
- Orientado al activo/impacto.
- Orientado a las vulnerabilidades.

El primero de ellos, orientado a las amenazas, se inicia con la identificación de fuentes de amenazas y las amenazas que de ellas resultan, y se enfoca en el desarrollo de escenarios a partir de ellas. Siendo así, las vulnerabilidades son identificadas a partir de dichas amenazas.

El enfoque orientado al activo/impacto toma como punto de partida la identificación del impacto o consecuencias que podría resultar de la afectación de activos críticos de la organización, para luego determinar cuáles son los eventos o amenazas que podrían resultar en dicha afectación.

Por último, el enfoque orientado a las vulnerabilidades comienza con la identificación de condiciones predeterminantes y vulnerabilidades existentes en los sistemas de información y procesos organizacionales, para luego identificar amenazas que podrían

explotar dichas vulnerabilidades con el consecuente impacto.

En el siguiente cuadro se observa un sencillo resumen de las características de los distintos enfoques para el análisis de riesgos mencionados:

Cuadro 6. Métodos para el análisis de riesgos

Orientado a las amenazas	Orientado al activo/impacto	Orientado a las vulnerabilidades
Toma como punto de partida la identificación de amenazas para luego detectar vulnerabilidades que pudieran ser explotadas.	Partiendo de la identificación del impacto que podría resultar de la afectación de activos críticos de la organización, analiza los eventos o amenazas que podrían resultar en dicha afectación.	A partir de la identificación de condiciones predeterminantes y vulnerabilidades, desarrolla aquellas amenazas que podrían explotar las mencionadas vulnerabilidades.

Fuente: Elaboración Propia (2016)

Nuevamente, es necesario advertir que ninguno de los distintos enfoques que se han revisado en el presente apartado resulta –necesariamente– mejor que el otro, sino que dependerá de la situación a ser evaluada y su contexto, así como también de la experiencia de los analistas, lo que determinará la mejor aproximación para el análisis de los factores de riesgo. Es importante resaltar también que todos estos enfoques tienen en cuenta los mismos factores de riesgo, sólo que en diferente orden y, por lo tanto, cualquier de ellos debiera arrojar un resultado similar. De este modo, es posible concluir que la selección de uno u otro sólo debiera afectar la complejidad o facilidad para conducir el análisis, más no el resultado final en términos de riesgos detectados.

El proceso de evaluación de riesgos

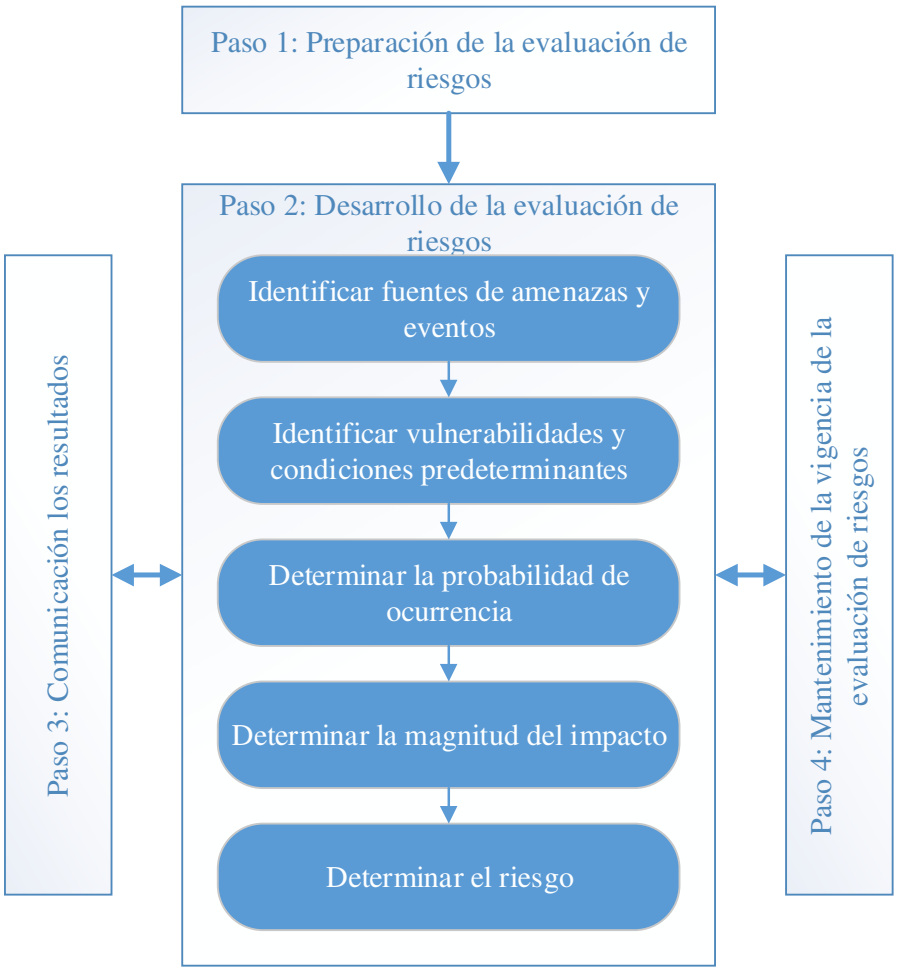
Finalmente, luego de haber planteado el concepto de modelo de riesgo y los distintos métodos de evaluación y análisis de riesgos, se profundizará en el proceso de evaluación, propiamente dicho.

NIST SP800-30 (2012) propone un proceso compuesto por los siguientes pasos:

1. Preparación de la evaluación de riesgos.
2. Desarrollo de la evaluación de riesgos.
3. Comunicación de los resultados.
4. Mantenimiento de la vigencia de la evaluación de riesgos.

Estos pasos los se observan esquematizados en el siguiente diagrama:

Diagrama 3. Proceso de evaluación de riesgos



Fuente: NIST SP800-30 (2012)

Cada uno de estos pasos se divide, a su vez, en diferentes tareas que desarrollarán a continuación.

Preparación de la evaluación de riesgos

El primer paso en el proceso de evaluación de riesgos consiste en la preparación de la actividad en sí. Siendo así, este paso busca establecer el contexto para el desarrollo de

la evaluación, mediante la creación de un marco de riesgos que identifique las políticas y requerimientos de la organización para la conducción de las evaluaciones de riesgo, los métodos a utilizar, los procedimientos para seleccionar los factores de riesgo, alcance de la evaluación, y demás aspecto relevantes.

Las tareas que se encuentran incluidas en este paso son las siguientes:

- Identificar el objetivo de la evaluación: en relación a la información que se espera obtener como resultado de la evaluación y las decisiones que dicha información debe sustentar.
- Identificar el alcance de la evaluación: en relación a las áreas de la organización y sistemas que serán considerados.
- Identificar los supuestos y restricciones: las cuales deben ser tenidas en cuenta durante el desarrollo de la evaluación.
- Identificar las fuentes de información: para los distintos factores de riesgo que serán utilizadas durante el proceso.
- Identificar el modelo de riesgos y los enfoques analíticos (evaluación y análisis) que serán utilizados durante la evaluación.

Para concluir, es posible observar que este paso busca, dentro de los límites establecidos por la metodología de evaluación de riesgos, indicar en forma detallada la forma en que cada uno de los pasos de la evaluación será ejecutado y los criterios a ser observados, así como también delinear en forma precisa el alcance de la evaluación y el resultado esperado.

Desarrollo de la evaluación de riesgos

El segundo paso del proceso contempla la ejecución de la evaluación de riesgos en sí. El objetivo de este paso es producir una lista de riesgos que luego será priorizada y utilizada para determinar los planes de acción necesarios que eventualmente serian requeridos para cada uno de ellos. Es importante destacar que esta evaluación debe desarrollarse dentro del marco establecido en el paso anterior.

Las tareas que se encuentran incluidas en este paso se detallan a continuación:

- Identificar fuentes de amenazas: incluyendo su capacidad para desarrollar amenazas, intencionalidad, probabilidades de establecer a la organización como blanco de ataques.
- Identificar las amenazas que dichas fuentes podrían materializar: analizando su potencial y relevancia.
- Identificar vulnerabilidades y condiciones predeterminantes: las cuales podrían afectar, ya sea aumentando o reduciendo, la probabilidad de las amenazas de generar un impacto adverso.
- Determinar la probabilidad de ocurrencia: de eventos, considerando las características de las fuentes de amenazas, las vulnerabilidades, las condiciones predeterminantes identificadas y los controles de seguridad implementados.
- Determinar la magnitud del impacto: que los eventos podrían ocasionar a la organización.

- Determinar el riesgo: considerando la probabilidad de ocurrencia de eventos y su impacto asociado.

Aun cuando estas tareas se presenten en orden, es necesario, y hasta esperable, que se desarrolle más de una iteración para lograr una lista completa de riesgos. Inclusive, es posible que distintas organizaciones puedan recorrer estas tareas en distinto orden, si así es requerido para alcanzar los objetivos establecidos.

Este paso constituye el corazón del proceso de gestión de riesgos, y es donde se articulan y ponen en práctica todos los componentes, métodos, factores y criterios de evaluación que se han observado anteriormente para determinar en forma precisa cuales son los riesgos a los que la organización se encuentra expuesta, cuál es la importancia o gravedad que estos revisten, y cuál es el impacto que de la ocurrencia de estos eventos podría resultar.

Comunicación de los resultados

El tercer paso del proceso de evaluación de riesgos contempla la adecuada comunicación de los riesgos identificados, con el fin de garantizar que los individuos encargados de la toma de decisiones en la organización posean la información relevante sobre los riesgos y puedan guiar las decisiones relativas a ellos.

Dos tareas se encuentran contempladas en este paso:

- Comunicar los resultados de la evaluación de riesgos: con el fin de apoyar la toma de decisiones en relación a los riesgos identificados.
- Compartir la información desarrollada durante la ejecución de la evaluación de riesgos: con el objetivo de apoyar otras actividades de gestión de riesgos.

Este paso permite que la información generada como resultado de la evaluación de riesgos pueda ser consumida por aquellas personas en la organización que deban tomar decisiones tanto en relación al tratamiento de los riesgos como también de las actividades ejecutadas por la organización de la cuales los riesgos se desprenden.

Mantenimiento de la vigencia de la evaluación de riesgos

El cuarto y último paso del proceso de evaluación de riesgos tiene por objetivo mantener vigente la información resultante de la evaluación. En un contexto de permanente cambio, este paso busca, mediante actividades de monitoreo, determinar el nivel de efectividad de las medidas adoptadas para el tratamiento de los riesgos y detectar cualquier cambio que pueda afectar el nivel de riesgo ya identificado, ya sea por la aparición de nuevas amenazas y/o vulnerabilidades, o cambios en las condiciones que determinan la probabilidad de ocurrencia o impacto de eventos.

Las tareas comprendidas en este paso son:

- Monitorear los factores de riesgo identificados durante la evaluación de riegos en forma regular: y a partir de esto, analizar en qué medida se han presentado cambios que afectan los riesgos ya detectados.
- Actualizar los componentes de la evaluación de riesgos: cuando esto sea requerido, a partir de las actividades de monitoreo ya mencionadas.

Resulta fundamental mencionar que la gestión y evaluación de riesgos representa una actividad recurrente y –por lo tanto–los resultados del análisis deben ser regularmente revisados con el objetivo de garantizar que el nivel de riesgo se mantiene invariable a lo largo del tiempo, o bien informar a la gerencia para que ésta pueda tomar las acciones que considere pertinentes a los fines de mantener a la organización dentro de los niveles de riesgo aceptables.

Observaciones finales sobre la evaluación de riesgos

Este extenso apartado ha permitido analizar en detalle todos y cada uno de los aspectos relativos al proceso de gestión de riesgos. En primer lugar, se destacó la importancia que para una organización representa disponer de una metodología de gestión de riesgos que establezca el marco organizacional dentro del cual será desarrollada la actividad. A la vez, se ha mencionado también la necesidad de disponer de un modelo de riesgos que indique aquellos factores que serán considerados durante el análisis, entre los que se encuentran: amenazas,

vulnerabilidades, condiciones predeterminantes, probabilidades de ocurrencia e impactos. Construyendo sobre estos conceptos, fueron planteados los métodos disponibles tanto para la evaluación como para el análisis de los riesgos, para –finalmente– abordar en profundidad el proceso de evaluación desde su inicio hasta su fin.

Además de revisar cada uno de estos componentes, fue posible observar la forma en que ellos deben ser articulados y los diversos enfoques existentes para su abordaje, indicándose las ventajas y desventajas que cada uno de ellos conlleva.

Como fue advertido anteriormente en referencia a los métodos de evaluación de riesgos, aspecto que también aplica al proceso de evaluación como un todo, no existe un método o enfoque particular que sea necesariamente mejor que el otro, sino que la elección de método más apropiado para ejecutar cada uno de los pasos y actividades que componen el proceso dependerá de diversos factores y características de la organización, tales como: la cultura organizaciones, propósito de la organización, contexto en el que esta desarrolla sus actividades, conocimientos y capacitación del personal asignado a la tarea de evaluación de riesgos, entre otros.

En última instancia, luego de haber alcanzado un acabado entendimiento del proceso, es posible observar con claridad la relevancia de esta actividad dentro de la gestión de riesgos, siendo que, a partir de la identificación de riesgos, la organización deberá entender de qué manera estos afectan su misión, objetivos y procesos, para luego iniciar un proceso de toma de decisión y darle un tratamiento a los riesgos

mencionados.

1.4. Tratamiento de los riesgos identificados

Como se ha podido observar en el apartado anterior, existen distintos modelos que pueden ser utilizados para el análisis o evaluación de riesgos. Sin embargo, en lo que respecta al tratamiento de los riesgos, diferentes autores y publicaciones, tales como COSO (2004), Hubbard (2009), NIST SP800-39 (2011) y Harris (2013), coinciden en acotar el espectro de oportunidades que se presentan, a los siguientes cuatro posibles cursos de acción:

- Reducir o mitigar.
- Compartir o transferir.
- Aceptar.
- Evitar.

En el primero de los posibles cursos de acción mencionados, mitigar o reducir un riesgo, implica tomar medidas para reducir la probabilidad de ocurrencia y/o el impacto de éstas. La reducción o mitigación de riesgos generalmente requiere de algún tipo de inversión por parte de la organización y, siendo que en muchos casos las alternativas para mitigar los riesgos son múltiples, se realiza un análisis de costo-beneficio para determinar cuál de las alternativas mitigaría el riesgo en mayor medida con los menores costos. Un ejemplo muy sencillo de mitigación de riesgos, que es posible observar-tanto en el mundo corporativo como en el uso personal de la tecnología- es el software antivirus. Mediante la inversión en este tipo de software, se

reduce la posibilidad de afectar a una computadora en su funcionamiento y –a la vez– se protege la integridad de la información contenida en ella. Deviene importante tener en cuenta que, en la gran mayoría de los casos, resulta imposible mitigar los riesgos en su totalidad, a partir de lo que surge el concepto de riesgo residual, el que representa el riesgo remanente luego de mitigar un determinado riesgo.

En segundo término, compartir o transferir un riesgo implica trasladar a un tercero su impacto, ya sea total o parcial, generalmente a cambio del pago de una prima determinada. En este escenario, ante la ocurrencia de un evento no deseado, sería el tercero en cuestión quien debería asumir los efectivos negativos que el evento pudiera causar. El ejemplo más común de este tipo de estrategia de tratamiento de los riesgos es el seguro automotor. Individuos y organizaciones, ante la posibilidad de un accidente automovilístico que pudiera afectar la integridad del vehículo o bien el patrimonio de su propietario de algún modo, contratan un seguro que, ante la ocurrencia de un accidente, debiera asumir los costos que de este resultaran. Nótese que quien contrata el seguro debe abonar una prima mensual o anual en compensación por el traslado del riesgo a la compañía de seguros.

Como ya fue aludido, las dos alternativas de tratamiento de riesgos mencionadas hasta el momento representan un costo para la organización. A partir de esto, si el costo del tratamiento del riesgo es mayor al beneficio que se percibiría como producto de la actividad que da origen al riesgo, no tendría sentido mitigarlo de ningún modo, dando lugar a alguno de los dos últimos cursos de acción mencionados: aceptar o bien evitar el riesgo.

Aceptar el riesgo implica no tomar medida alguna en relación al riesgo, siendo que los costos de la mitigación o transferencia del riesgo no son viables desde el punto de vista costo-beneficio. Adicionalmente, para que el riesgo pueda ser aceptado debe encontrarse dentro de los niveles de tolerancia establecidos para la organización.

En cambio, en aquellos casos donde el costo de mitigar o transferir el riesgo resulte excesivo, y a su vez el nivel de riesgo exceda el marco de tolerancia al riesgo definido, evitar el riesgo implica no realizar la actividad que da origen al riesgo en cuestión.

En el cuadro que se observa a continuación se presentan las cuatro alternativas de tratamiento de los riesgos mencionadas:

Cuadro 7. Tratamiento de los riesgos

Reducir o mitigar	Compartir o transferir	Aceptar	Evitar
Reducir el impacto o probabilidad de ocurrencia del riesgo.	Transferir el riesgo a un tercero.	Aceptar el riesgo sin tomar medida alguna en relación a este.	No ejecutar las acciones o actividades que dan origen al riesgo.

Fuente: Elaboración Propia (2016)

En último lugar, deviene importante notar que, desde el momento en que un riesgo es detectado, resulta imposible evadirse de tomar una posición en relación a dicho riesgo. La entidad puede optar por mitigar o transferir el riesgo, evitar este o aceptarlo explícitamente, en forma consciente y estudiada, pero en el caso en que no se decida tomar acción alguna al respecto, necesariamente se incurre en la

aceptación del riesgo. No seguir ningún curso de acción implica aceptar el riesgo en su condición original. Es por esto que resulta factible afirmar que, tan pronto como un riesgo es identificado, la organización se encuentra obligada a darle algún tipo de tratamiento, ya sea por acción u omisión.

1.5. Marcos de gestión de riesgos, estándares y mejores prácticas

A lo largo del presente apartadose han mencionado y referenciado una gran cantidad de autores, normas y estándares, todos ellos relacionados –de modo alguno– con las actividades de gestión de riesgos. ISACA (2014) presenta un breve resumen de los marcos de gestión, estándares y prácticas más relevantes relacionadas con la gestión de riesgos de seguridad de la información, que se encuentran citados en el presente apartado. Sin embargo, antes de proceder con cada uno de ellos, es importante revisar la definición que ISACA (2014) realiza de cada tipo de publicación:

- Marcos de gestión: son estructuras generalmente aceptadas, orientadas a los procesos de negocio, que establecen un lenguaje y procesos organizacionales comunes.
- Estándares: son requerimientos mandatorios, normas o especificaciones aprobadas por una organización externa reconocida, como por ejemplo la International Organization for Standardization (ISO).
- Prácticas líderes: son acciones frecuentemente ejecutadas como resultado de la aplicación de conocimiento. Se entiende como práctica líder a aquella que

hace una aplicación óptima del conocimiento en un área particular.

Marcos de gestión

Los marcos de gestión relacionados a la gestión de riesgos más relevantes indicados por ISACA (2014) se pueden observar en el siguiente cuadro:

Cuadro 8. Marcos de gestión de riesgo

Organización	Publicación
ISACA	The Risk IT Framework
ISACA	Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0
ISACA	COBIT 5
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	Enterprise Risk Management – Integrated Framework
US National Institute of Standards and Technology (NIST)	Risk Management Framework, NIST Special Publication (SP) 800-39, Managing Information Security Risk

Fuente: ISACA (2014)

Estándares

ISACA (2014) también presenta los siguientes estándares como aquellos más relevantes en el campo de la gestión de riesgos de seguridad, que se presentan en el cuadro a continuación:

Cuadro 9. Estándares de gestión de riesgos

Organización	Publicación
ISACA	IT Audit and Assurance Standards
International Organization for Standardization (ISO)	ISO 31000:2009
ISO/International Electrotechnical Commission (IEC)	ISO/IEC 2700x (for Information Security Management Systems)
International Organization for Standardization (ISO)	ISO 22301:2012, Societal Security – Business Continuity Management Systems
Payment Card Industry (PCI) Security Standards Council	PCI Data Security Standard (PCI DSS)

Fuente: ISACA (2014)

Prácticas recomendadas

En último lugar, ISACA (2014) presenta las prácticas líderes de mercado en materia de gestión de riesgos de seguridad, indicadas en el siguiente cuadro:

Cuadro 10. Prácticas líderes de gestión de riesgos

Organización	Publicación
ISACA	The Risk IT Practitioner Guide
ISO/IEC	ISO/IEC 2700x (for Information Security Management Systems)
US National Institute of Standards and Technology (NIST)	NIST Special Publication (SP) 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems NIST Special Publication (SP) 800-37, Risk Management Guide for Information Technology Systems
Software Engineering Institute (SEI)	Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
Ministerio de Hacienda y Administraciones Públicas	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT versión 2)

Fuente: ISACA (2014)

Observaciones finales acerca de los marcos de gestión, estándares y mejores prácticas

Como fue observado anteriormente en el presente apartado, existe una gran variedad de autores y publicaciones relacionadas con la gestión de riesgos. Algunas de ellas, con un enfoque generalista, en tanto que otras fueron específicamente desarrolladas para observar las necesidades de una industria o actividad específica, o bien con el objeto de especializarse en la protección de determinados activos de la organización.

Más allá de lo planteado, es posible observar que los conceptos desarrollados en los apartados anteriores se encuentran presentes en todas las publicaciones

citadas, en la medida en que todas ellas comparten un objetivo común, que es la identificación de riesgos, y que –para ello–se disponen de distintas herramientas, enfoques y visiones que conducen indefectiblemente hacia el objetivo buscado.

1.6. Conclusiones

En el presente capítulo se han revisado diversos aspectos relacionados con la gestión de riesgos que aplican a corporaciones y entidades en general, sin importar cuál es su tamaño y propósito. A partir de lograr un claro discernimiento del concepto de riesgo, que se entiende como la posibilidad de ocurrencia de un evento que afecte negativamente a una determinada organización, se ha avanzado sobre los pasos que es preciso recorrer para detectar la presencia de riesgos en el contexto donde la dicha institución se desenvuelve, cómo y en qué medida estos podrían afectar la misión y objetivos de la entidad, y –también– la forma en que es posible afrontar los riesgos identificados.

Como primer paso –luego de la revisión del término "riesgo" propiamente dicho–, fue introducida la idea de gestión de riesgos, entendiéndose como el proceso organizacional que tiene por objetivo la detección y administración de los riesgos de forma tal de obtener un determinado nivel de certeza en relación al logro de los objetivos de la organización.

Posteriormente, profundizando sobre el mencionado proceso, se realizó un análisis exhaustivo sobre las dos actividades principales en él incluidas, que son la

evaluación de riesgos y el tratamiento de aquellos riesgos que hubieran sido identificados.

En relación a la primera de ellas, la evaluación de riesgos, se advirtió la necesidad de disponer de una metodología que establezca la forma en que dicha actividad será llevada a cabo, así como también de un modelo de riesgos que indique cuáles serán los factores que serán analizados. Del mismo modo, fueron presentadas las alternativas disponibles para el desarrollo de la evaluación propiamente dicha –métodos cualitativos y cuantitativos– y también para el análisis de los riesgos –orientado a las amenazas, al activo/impacto o a las vulnerabilidades–. Con todos estos elementos apropiadamente dispuestos, finalmente se han revisado todas y cada una de las tareas que se encuentran comprendidas dentro de esta actividad, que tiene por finalidad determinar la existencia de riesgos a partir de un análisis del contexto organizacional.

Como último concepto relacionado con la gestión de riesgos, también se han tipificado los posibles cursos de acción a seguir como resultado de la identificación de riesgos.

En última instancia, también fue presentado un breve resumen de las metodologías, estándares y mejores prácticas existentes al día de hoy que dan proporcionan un marco de referencia para llevar a la práctica los conceptos anteriormente mencionados.

Las nociones desarrolladas en el presente capítulo permitirán disponer de los

elementos teóricos suficientes para avanzar en el estudio de la administración de la seguridad de la información a partir de la gestión de riesgos, objetivo del presente trabajo, y que se desarrollará en el Capítulo 2, Marco Investigativo, que se encuentra a continuación.

2. MARCO INVESTIGATIVO

El presente capítulo tiene por objetivo exponer el trabajo investigativo realizado en el marco de la presente tesis y detallar las conclusiones a través de este alcanzadas. En el contexto de la mencionada investigación, y con el propósito de recabar información en relación a la práctica de la gestión de riesgos en el campo de la seguridad de la información, tres tipos de herramientas fueron utilizadas: encuesta a profesionales de seguridad de la información, entrevistas a informantes-claves, y estudio o análisis de un caso. En las subsiguientes páginas se realizará una detallada descripción de ellas y los resultados obtenidos.

2.1. Encuesta a profesionales de seguridad de la información

Con el objeto de obtener un mayor conocimiento acerca del nivel de desarrollo y madurez de la práctica de la gestión de riesgos en el campo de la seguridad de la información, se realizó una encuesta entre representantes de diversas empresas y organizaciones.

La mencionada encuesta incluyó diversas preguntas a través de las cuales los participantes volcaron sus puntos de vista en lo que respecta a la existencia y contexto en el cual se desarrollan las actividades de seguridad de la información en las organizaciones en las que se desempeñan profesionalmente, con un fuerte foco en la

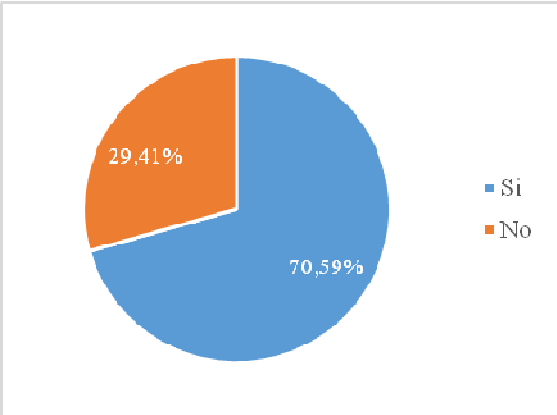
gestión de riesgos. La misma fue enviada a un total de 30 participantes, cada uno de ellos pertenecientes a organizaciones o empresas diferentes, con el objetivo de relevar, más allá de las opiniones personales que los participantes pudieran tener en relación al tema bajo estudio, la situación de las instituciones que ellos representan. Sobre el total de encuestas enviadas, fueron recibidas 17 respuestas. Sobre este punto, resulta importante aclarar que la limitación en la cantidad de encuestados y, consecuentemente, la cantidad de respuestas obtenidas, surge del hecho que la encuesta explora temas que la gran mayoría de las organizaciones considera confidenciales, esto es, la posición de seguridad de la organización. Siendo así, resulta en extremo difícil, si no imposible, obtener respuestas de personas sin algún tipo de vínculo personal, académico o profesional, lo cual significó una importante restricción a la hora de recabar datos del campo.

A continuación se podrán observar los resultados obtenidos a través de la encuesta.

Existencia de un área responsable de la seguridad de la información

En lo que respecta a la existencia de un área encargada de la gestión de la seguridad de la información, el 70,59% de los encuestados respondió afirmativamente, en tanto que el 29,41% restante informó que sus respectivas organizaciones no cuentan con el mencionado sector.

Gráfico 1. Existencia de área responsable de la seguridad de la información

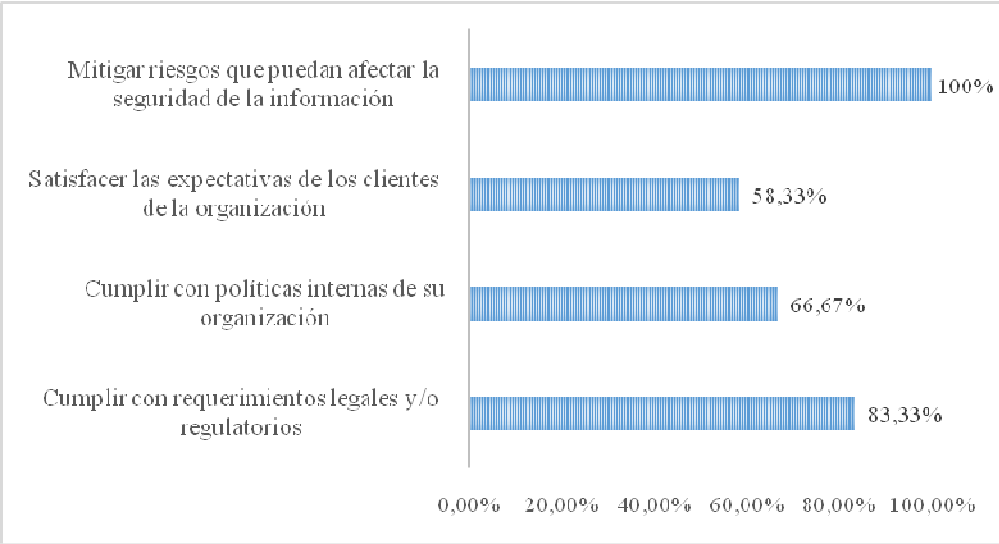


Fuente: Elaboración Propia (2016)

Propósito de la implementación de controles de seguridad

Consultados sobre el objetivo perseguido mediante la implementación de controles de seguridad, la totalidad de los encuestados informaron que se busca mitigar riesgos relacionados con la seguridad de la información, resultando este dato sumamente relevante. Adicionalmente, el 83,33% informó que la necesidad de implementar distintos controles de seguridad también responde a requerimientos legales y/o regulatorios, y el 66,67% mencionó la necesidad de cumplir con políticas internas de la organización. En último lugar, el 58,33% mencionó la búsqueda de la satisfacción a requerimientos de clientes como motivación para la implementación de estos controles.

Gráfico 2. Propósito de la implementación de controles de seguridad

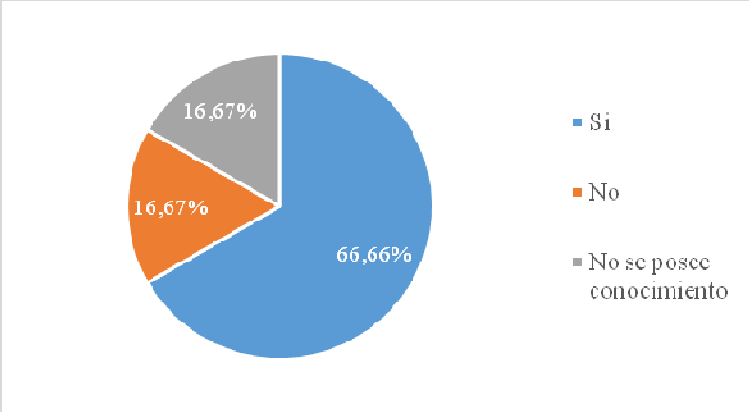


Fuente: Elaboración Propia (2016)

Ejecución de una evaluación de riesgos

Adentrándonos en el objeto de estudio de la presente tesis, los encuestados fueron consultados acerca de la ejecución de una evaluación de riesgos formal en la organización. Sobre este aspecto, el 66,67% respondió afirmativamente, mientras que un 16,6% informó que no se había ejecutado dicha actividad, y en igual medida otro 16,67% mencionó que no disponía de suficiente información para responder esta pregunta.

Gráfico 3. Ejecución de una evaluación de riesgos

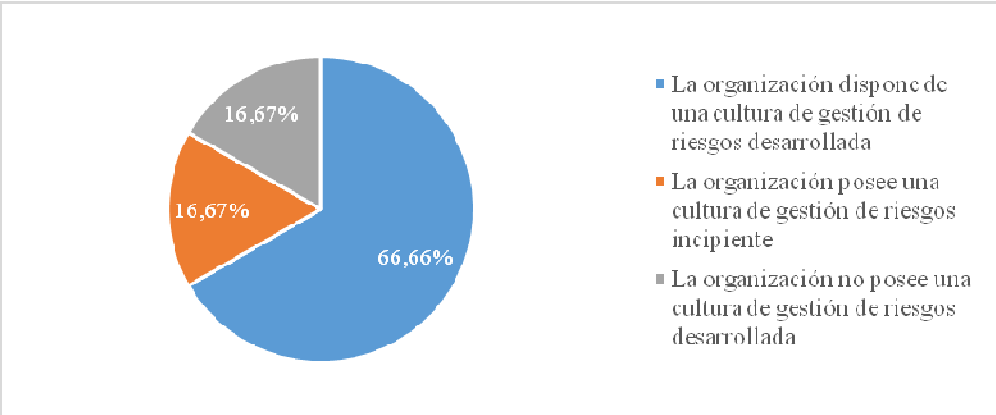


Fuente: Elaboración Propia (2016)

Postura general de la organización en relación a la gestión de riesgos

Cuando los encuestados fueron consultados acerca de la postura general de la organización hacia la gestión de riesgos, todos aquellos que informaron haber realizado evaluaciones de riesgos han detallado también que sus respectivas organizaciones posee una cultura corporativa de gestión de riesgos, lo cual representa nuevamente el 66,67% de las respuestas. Otro 16,67% de los participantes de la encuesta mencionan que las organizaciones a la que pertenecen poseen una cultura de riesgos corporativa incipiente, mientras que el restante 16,67% informa que esta no se encuentra desarrollada en modo alguno.

Gráfico 4. Postura de la organización hacia la gestión de riesgos

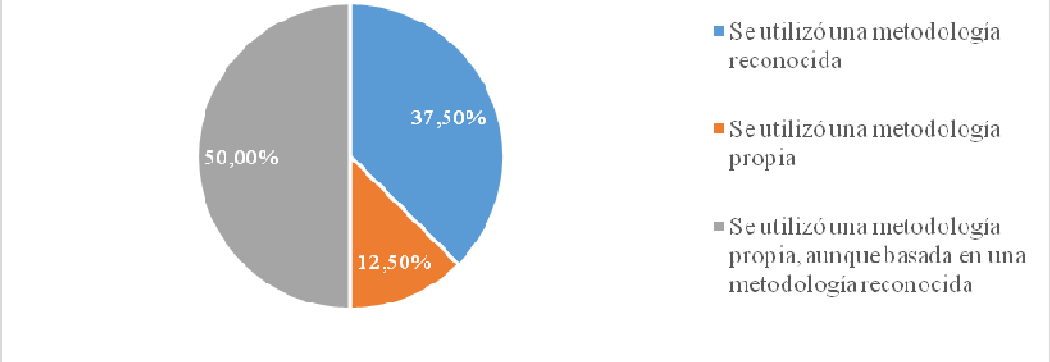


Fuente: Elaboración Propia (2016)

Metodología de gestión de riesgos utilizada

Entre aquellos encuestados que han informado haber conducido una evaluación de riesgos en sus organizaciones, el 37,5% mencionó haber utilizado un estándar o marco metodológico reconocido de mercado (tales como ISO 31000:2009 o ISO/IEC 27005), en tanto que un 12,5% detalla haber utilizado una metodología desarrollada por la propia organización. El 50% restante de los encuestados informa haber desarrollado una metodología propia, aunque tomando como base una metodología o norma de público reconocimiento como las anteriormente indicadas.

Gráfico 5. Metodología de gestión de riesgos utilizada



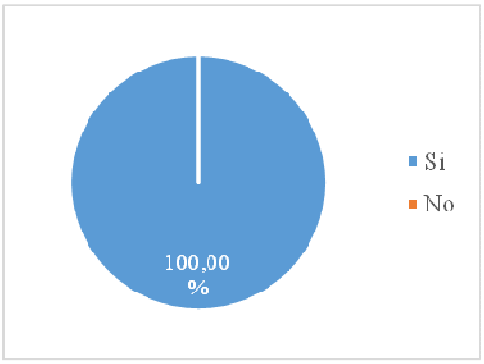
Fuente: Elaboración Propia (2016)

Revisión regular de riesgos y efectividad de los controles de seguridad

Los encuestados también fueron consultados acerca de la existencia de un proceso regular de revisión de los riesgos identificados y nuevos riesgos que pudieran surgir, así como también acerca del nivel de conocimiento de la organización sobre la efectividad de los controles de seguridad para mitigar los riesgos identificados.

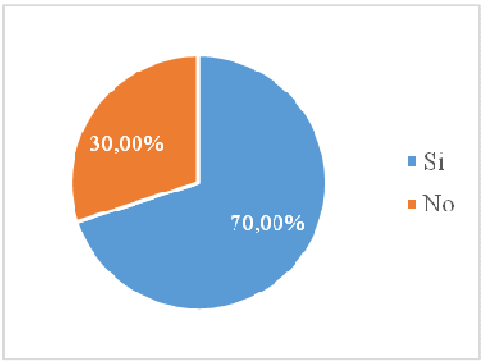
Sobre el primero de los aspectos mencionados, la totalidad de los participantes de la encuesta informó realizar una revisión regular de los riesgos, en tanto que tan solo el 70% de ellos mencionó tener conocimiento acerca de la medida en que los controles de seguridad implementados mitigan los riesgos detectados.

Gráfico 6. Revisión regular de riesgos



Fuente: Elaboración Propia (2016)

Gráfico 7. Noción de la efectividad en la mitigación de riesgos



Fuente: Elaboración Propia (2016)

Acerca de la necesidad y dificultades de la gestión de riesgos

Adicionalmente a los aspectos anteriormente señalados, los participantes de la encuesta fueron consultados sobre su opinión en lo que respecta a la necesidad y dificultades de la gestión de riesgos en el campo de la seguridad de la información.

Sobre el primero de los puntos mencionados, los participantes han resaltado de forma unánime la importancia de esta actividad para preservar la integridad, confidencialidad y disponibilidad de la información, siendo esta un activo clave de las organizaciones. Sin embargo, en lo que respecta a las dificultades que el proceso de gestión de riesgos conlleva, los encuestados han identificado diversos desafíos que merecen ser mencionados:

- Necesidad de las organizaciones de obtener resultados en el corto plazo,

postergando actividades “importantes” en pos de aquellas “urgentes”;

- Disponibilidad de personal capacitado y conocimientos sobre la materia;
- Necesidad de disponer de fondos y esfuerzos significativos para llevar adelante la actividad.

Adicionalmente, mencionan dos aspectos relevantes para el éxito de la actividad:

- Compromiso y apoyo de la dirección;
- Eficaz coordinación con otras áreas de gestión de riesgos.

Observaciones sobre los resultados de la encuesta

Las respuestas provistas por los participantes de la encuesta permiten hacer importantes observaciones que se detallarán a continuación.

Como primera lectura relevante, se observa que una porción destacada de las organizaciones encuestadas aún no dispone de un área específica responsable por la seguridad de la información. Cabe aclarar que esto no necesariamente significa que no se hayan implementado controles de seguridad en ellos, pero sí que no se dispone de una función establecida y formalizada dentro de la organización para tal fin. Siendo así, es posible concluir que las empresas en esta situación se encuentran aún en una etapa temprana en lo que a la seguridad de la información respecta, y más aún en lo que respecta a la gestión de riesgos de seguridad.

Entre aquellas empresas que sí cuentan formalmente con una función de

seguridad de la información, deviene importante notar que todas ellas consideran entre las principales razones para implementar controles de seguridad la necesidad de mitigar riesgos que puedan afectar la seguridad de la información (adicionalmente a otros objetivos). Esto permite establecer que la noción de riesgo se encuentra presente en todas ellas.

Sin embargo, y aunque pueda resultar contradictorio, sólo el 66,67% de las mencionadas organizaciones indicó haber invertido esfuerzos en determinar claramente cuáles son esos riesgos. Dicho en otras palabras, 1 de cada 3 empresas que ha expresado la necesidad de mitigar riesgos de seguridad, ha afirmado no haber conducido un proceso formal para determinar con precisión cuáles son los riesgos que enfrenta. Siendo así, es factible concluir que la implementación de los controles de seguridad en aquellas entidades donde no se ha ejecutado un análisis de riesgo se realiza en forma intuitiva, sin que esto responda a una necesidad concreta identificada (la mitigación de un riesgo específico).

Coincidentemente, aquellas organizaciones que realizaron una evaluación de riesgos de seguridad son las mismas que mencionaron disponer de una fuerte cultura de riesgos corporativa. A partir de esto, resulta posible establecer la importancia de contar con un marco cultural organizativo, así también con el consecuente apoyo de la dirección, para poder desarrollar una adecuada gestión de riesgos en el campo de la seguridad de la información.

Un dato curioso aportado por la encuesta surge a partir del hecho que, si bien en todas las organizaciones donde se ha conducido una evaluación de riesgos, se revisa

regularmente el análisis realizado en pos de mantenerlo vigente, no en todas ellas cuentan con una clara visibilidad sobre la efectividad de los controles de seguridad implementados para mitigar los riesgos, lo que pareciera indicar la existencia de una falta de articulación entre las actividades enfocadas en detectar riesgos y aquellas que buscan mitigarlos. Más relevante aún, esto deriva en el hecho que se desconoce a ciencia cierta del nivel de riesgo al que se encuentra expuesta la organización, al no poder establecerse con precisión cual es el riesgo residual de cada uno de los riesgos detectados.

En último lugar, es importante destacar, de entre las observaciones realizadas por los encuestados en lo que respecta a las dificultades de la gestión de riesgos, aquellas que refieren a poca disponibilidad de personal capacitado para la función, siendo que este factor se encuentra fuera del control de las organizaciones.

2.2. Entrevistas a informantes-clave

Con el objetivo de obtener las perspectivas de distintos profesionales del campo de la seguridad de la información en relación a la gestión de riesgos, se han realizado entrevistas con Pablo Correnti y Diego Taich. En el caso de Pablo Correnti, se ha desempeñado, a lo largo de su trayectoria profesional, en distintas organizaciones, encontrándose entre las más destacadas PwC y la Presidencia de la Nación, así como también realizado distintas actividades como consultor independiente y en el campo de la docencia universitaria. En lo que respecta a Diego Taich, posee una larga

experiencia en consultoría de tecnología y seguridad de la información, desempeñándose actualmente como Director del área *Security & Technology* de la división de consultoría de PwC Argentina.

Consultados sobre cuán extendida se encuentra la práctica de la gestión de riesgos en el campo de la seguridad de la información, ambos han sostenido que todavía existe un gran camino por recorrer, tanto en organizaciones del sector privado como público, e inclusive en muchas de ellas se puede observar una resistencia a avanzar en este sentido. En términos generales, han observado que existen solo unas pocas organizaciones con una gestión de la seguridad de la información eficiente, formal y sistematizada, y dentro de estas, sólo algunas realizaban una gestión de riesgos formal.

Sobre este particular, se observó que el tamaño de la organización no siempre es determinante, sino que resulta de mayor relevancia el rubro en el cual la empresa desarrolla sus actividades. A modo de ejemplo, resaltaron que instituciones financieras y de seguros contaban con una posición más sólida en todos los temas relacionados a la seguridad de la información, y específicamente en lo que hace a la gestión de riesgos, en tanto que empresas dedicadas a la comercialización de productos de consumo masivo y otras se encontraban aún varios pasos detrás.

En cuanto a las causas de este comportamiento, mientras que Diego Taich lo relacionó mayormente a la falta de inversión en esta actividad, posiblemente debido a las dificultades para identificar un retorno de la inversión, en tanto que Pablo Correnti lo asoció mayormente a la falta de conocimiento de los niveles ejecutivos

respecto de los tema asociados a la seguridad de la información, y también a la inmadurez de los líderes de seguridad para presentar de manera efectiva y en términos de negocio la problemática. Más allá de esto, ambos coincidieron en que desde la dirección de las organizaciones se minimizaba el tema y no se tomaba en consideración la verdadera magnitud de los riesgos. Adicionalmente, tampoco se observaba un marco legal o regulatorio que empujara a las empresas hacia la implementación de una efectiva gestión de riesgos.

En lo que respecta a las dificultades que las organizaciones enfrentan a la hora de realizar una evaluación de riesgos, los especialistas han resaltado dos aspectos principales: la dificultad de contar con profesionales capacitados para la tarea, y la complejidad del proceso en sí. En cuanto al primero de los aspectos referidos, resaltaron la necesidad de disponer de un perfil profesional poco común, ya que se requerían conocimientos metodológicos, una gran capacidad analítica, habilidades comunicacionales, y también desarrollar un acabado entendimiento del negocio. En este sentido, resultaba más fácil encontrar profesionales capaces de implementar controles de seguridad predefinidos que de desarrollar un análisis de la organización y sus riesgos asociados. En lo que respecta al segundo punto observado, acerca de la complejidad de la evaluación de riesgos, mencionaron que el desafío radicaba en tener una visión integral de la situación de la empresa y su contexto, siendo que resultaba fácil caer en un análisis sesgado, parcial, que excluyera riesgos que podrían ser de relevancia.

Independientemente de la situación a ese momento, ambos especialistas fueron

optimistas en lo que respecta a la generalización de la práctica de la gestión de riesgos de seguridad de la información en un futuro cercano, en la medida en que también se lograra un mayor nivel de conciencia en lo que concernía a la seguridad de la información. Estos movimientos ya se estaban observando en los países más desarrollados y se esperaba que decanten en los países de la región en el lustro siguiente, impulsado por un aumento en la regulación y también por mayores exigencias de los clientes en las empresas.

2.3. Análisis del caso

A los fines del presente estudio, fue entrevistado el Gerente Seguridad de la Información y Soporte a la Operación de una de las empresas de servicios más importantes de la República Argentina, la cual cotiza en la Bolsa de Comercio de Buenos Aires y también en el *New York Stock Exchange*, con el objetivo de analizar la experiencia desarrollada por dicha organización en el campo de la gestión de riesgos de la información. Con motivo de preservar la confidencialidad de la información provista durante las entrevistas, mantendré en el anonimato tanto el nombre del entrevistado como de la empresa bajo estudio, sin que ello resulte en un perjuicio para los objetivos de la investigación.

Mediante las entrevistas mencionadas anteriormente, las cuales se realizaron tanto en persona como también mediante la herramienta de videoconferencias Skype, se buscó lograr un acabado entendimiento de la experiencia desarrollada por la organización

bajo estudio en relación a la gestión de riesgos de seguridad de la información, que resultará de gran relevancia para las conclusiones generales del presente trabajo.

El contexto organizativo y los antecedentes

En primer lugar, y a los fines de lograr un acabado entendimiento de la evolución de la gestión de riesgos de la información en la empresa analizada, es preciso conocer el contexto organizativo en el que esta actividad se desarrolló, como así también la evolución de dicho marco organizacional junto con aquella del marco metodológico para la gestión de riesgos de la información, íntimamente relacionados.

Siendo así, como punto de partida para este análisis, se considerará como primer hito relevante hacia la gestión de riesgos de la información de la empresa bajo estudio la creación de la Gerencia de Seguridad de la Información, hecho que ocurrió en el año 2008, llamativamente dentro de la órbita de la Dirección de Capital Humano.

Dicha gerencia tenía por misión realizar la gestión de riesgos de la información, para lo cual sería preciso identificar procesos y activos críticos y no críticos, para luego determinar los riesgos a ellos asociados y plantear, en último lugar, un adecuado plan de mitigación.

Este nuevo enfoque resultó ser toda una novedad dentro de la empresa, siendo que la organización no disponía de una cultura sólida de gestión de riesgos. Previamente a la creación de la gerencia mencionada, las únicas actividades de gestión de riesgos

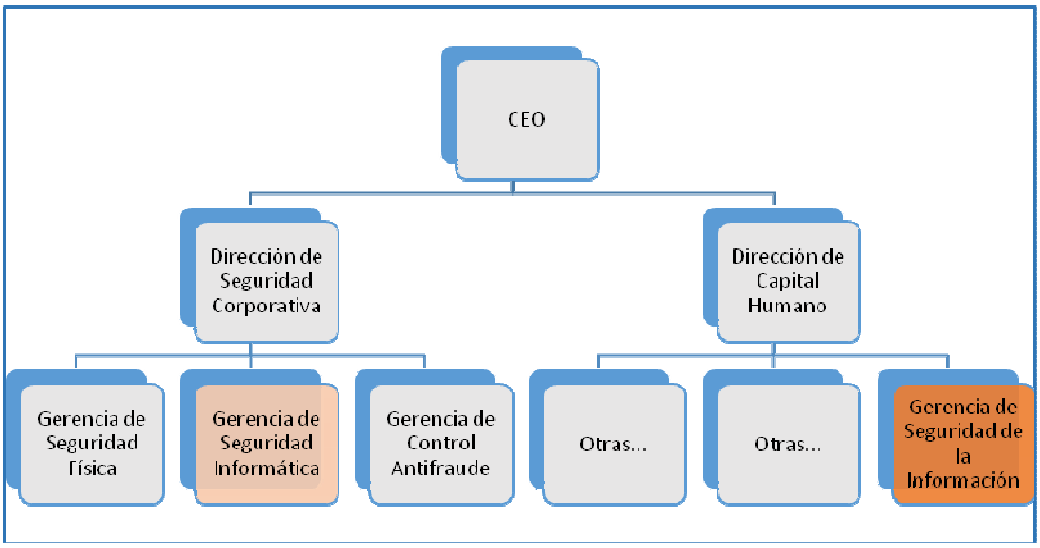
estaban orientadas exclusivamente a identificar riesgos financieros, sin prestar mayor atención a otros tipos de riesgos corporativos.

Al momento en que la Gerencia de Seguridad de la Información fuera creada, existía también en la empresa la Gerencia de Seguridad Informática, bajo la dirección de Seguridad Corporativa, la cual tenía por objetivo la protección de los activos informáticos de la empresa. Es importante notar que, más allá del parecido en el nombre entre ambas gerencias, los objetivos de estas y el enfoque metodológico de cada una de ellas era considerablemente distinto.

Hasta ese entonces, el área de Seguridad Informática se encontraba muy enfocada en la seguridad perimetral, esto es, prevenir que terceros pudieran acceder a la infraestructura de IT de la organización, así como también contener otras amenazas externas, siempre con un marcado foco en los activos informáticos de la empresa. Sin embargo, se dedicaba nulo o muy poco esfuerzo a las amenazas internas y otros riesgos de seguridad. Si bien el nivel de seguridad perimetral era excelente, y se encontraba entre los más avanzados de Latinoamérica, existía todo un universo de riesgos amenazando la seguridad de la información que no estaba siendo debidamente gestionado, e inclusive, del que no se había tomado conocimiento.

En el diagrama a continuación se puede observar se encontraba conformada la estructura organizacional descripta:

Diagrama 4. Organización corporativa inicial para la gestión de riesgos



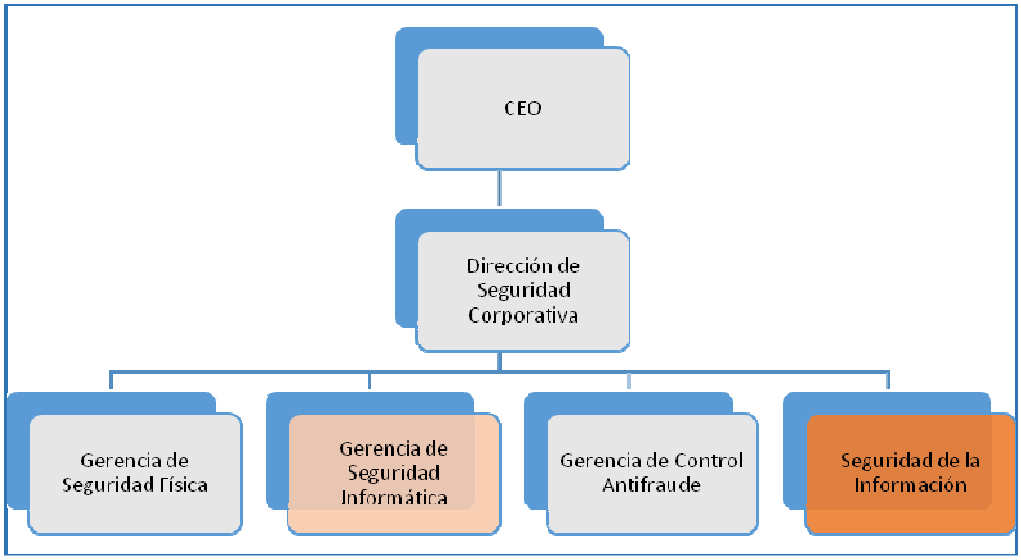
Fuente: Elaboración Propia (2016)

Volviendo sobre los orígenes de la Gerencia de Seguridad de la Información, es dable mencionar también que el área surge como resultado de la detección de un incidente de seguridad; más específicamente, la fuga de información confidencial de la empresa. Esto motivó a la dirección a avanzar hacia la creación de un área de seguridad de la información con un enfoque distinto al que se había seguido hasta ese momento, el cual se percibía como insuficiente.

Desde su creación y hasta la actualidad, la gerencia de Seguridad de la Información sufrió diversas reestructuraciones, acompañadas también de cambios en su misión y enfoque de trabajo, que impactaron en el alcance de la gestión de riesgos de la información. A lo largo de las próximas secciones, ser observará cómo estos fueron desarrollándose desde el año 2008 hasta la actualidad, y en qué medida estos cambios alteraron también la postura de la organización hacia los riesgos de

seguridad de la información. Sin embargo, antes de proceder en esta dirección y, con motivo de conocer la situación actual de la organización en este ámbito, es importante mencionar que en una última reestructuración de la función, realizada en diciembre del año 2014 y actualmente vigente, las distintas funciones de seguridad de la organización se encuentran agrupadas bajo la Dirección de Seguridad Corporativa, la cual cuenta con las gerencias de: Seguridad Física, Seguridad Informática, Control Antifraude y Seguridad de la Información. La estructura organizacional mencionada puede observarse a continuación:

Diagrama 5. Organización corporativa actual de seguridad



Fuente: Elaboración Propia (2016)

Los primeros pasos hacia la gestión de riesgos

En el año 2008, nuestro entrevistado inició su gestión en la organización liderando la Gerencia de Seguridad de la Información, con el objetivo de implementar un proceso sistemático y coordinado para la detección de riesgos de seguridad de la información. Sin embargo, como fue mencionado anteriormente, la empresa carecía tanto de una cultura de gestión de riesgos corporativa como de seguridad de la información. Adicionalmente, la gerencia, en sus pocos meses de existencia, tampoco había logrado una articulación adecuada con la gerencia de Seguridad Informática.

Como consecuencia de esto, en la primera reestructuración del área, realizada a principios del año 2009, y a tan sólo 6 meses de la creación de la Gerencia de Seguridad de la Información, esta fue trasladada debajo de la órbita de Seguridad Informática, a la vez que se acotó el alcance de su misión. Sin haber tenido el tiempo necesario ni la oportunidad de desarrollar las condiciones necesarias para avanzar en un proceso integral de gestión de riesgos de seguridad, su propósito dentro de la organización fue redefinido para proporcionar el marco y sustento metodológico necesario para obtener la certificación ISO 27001.

Es importante aclarar que aun cuando la norma ISO27001 requiere de una gestión adecuada de los riesgos, el enfoque adoptado en ese momento limitó el alcance del análisis considerando únicamente riesgos informáticos, particularmente sobre la infraestructura y sistemas de IT. De esta forma, otros riesgos que podrían afectar a activos de información, más allá de aquellos anteriormente mencionados, fueron excluidos del alcance, tales como: información impresa, dispositivos de

almacenamiento externos –*pen drives*–, dispositivos móviles, entre otros.

Como resultado de este primer análisis de riesgos, fueron detectaron tres grandes aspectos que debían ser revisados y mejorados:

1. El primero y más importante relacionado a la falta de planes de continuidad de negocio;
2. La gestión de incidentes de seguridad;
3. Por último, la falta de un marco normativo actualizado.

En relación al primero de los puntos mencionados, se detectó que al momento de realizar el análisis, sólo unos pocos sistemas de IT contaban con un plan de continuidad; esto es, un plan alternativo que la organización debía ejecutar ante la imposibilidad de disponer por un tiempo prolongado de ese componente de entorno de IT. Adicionalmente, tampoco se disponía de análisis de impacto de negocio de cada uno de los sistemas y activos informáticos de la organización, que pudiera orientar las inversiones en este sentido.

En cuanto a la gestión de incidentes de seguridad, si bien la organización disponía de una probada capacidad para responder cuando estos se presentaba, se carecía de un proceso formal y una metodología para este fin, que adicionalmente contemple aspectos tales como: planes de mejora continua, análisis de causa raíz, y otras herramientas que permitieran identificar el origen de los incidentes repetitivos.

En último lugar, y en lo que respecta al marco normativo, se observó la ausencia de

un marco normativo actualizado y vigente.

A partir de este análisis, la Gerencia de Seguridad de la Información lideró los planes de adecuación necesarios, siendo que finalmente, la certificación ISO 27001 fue obtenida a principios del año 2010, y se trabajó durante los 3 años posteriores a este hecho continuando con enfoque en riesgos de IT descripto.

Un cambio en la visión corporativa hacia los riesgos

En el año 2013, la organización crea la Dirección de Gestión de Riesgos Corporativos, cuya misión era gestionar en forma integral los riesgos que la organización enfrentaba en las distintas áreas operativas, extendiendo de este modo la visión inicial de gestionar únicamente los riesgos financieros y, parcialmente, aquellos de seguridad de la información. Producto de este cambio, la Gerencia de Seguridad de la Información comenzó a trabajar en forma articulada con la reciente creada área en la definición de una metodología corporativa para la gestión de riesgos. Es preciso resaltar que dichas áreas no tenían dependencia entre sí, aunque se trabajó en forma conjunta para unificar criterios de trabajo, que finalmente serían formalmente establecidos cuando, ese mismo año, desde la casa matriz se envió una metodología de gestión de riesgos que fuera adoptada por toda la organización.

Esta metodología fue ampliamente difundida y adoptada por toda la empresa, como parte de una iniciativa corporativa que tenía por objetivo identificar aquellos riesgos que pudieran afectar de modo alguno el patrimonio de la empresa, con un enfoque

estrictamente cuantitativo. La metodología no contemplaba la posibilidad de realizar análisis cualitativos, motivo por el cual se encontraron dificultades en distintas etapas del análisis de riesgos, tales como:

- Estimación de la probabilidad de ocurrencia eventos discretos;
- Estimación del impacto que los riesgos identificados podrían tener en la organización;
- Cálculo del valor de algunos activos de información.

De este modo, y como consecuencia de esta restricción metodológica, fueron excluidos del análisis riesgos que eran sumamente tangibles o visibles pero que, al no poder ser cuantificados, debían ser omitidos.

Es preciso resaltar también que el cambio introducido en la gestión de riesgos fue tan importante, tanto en lo que respecta a la metodología de análisis como a su alcance, que el trabajo anteriormente realizado para alcanzar la certificación ISO 27001 de poco sirvió en este nuevo escenario, y fue preciso revisar absolutamente todos los riesgos bajo la luz de la nueva metodología de trabajo. Esto se debió, mayormente, a que el nuevo enfoque funcional, orientado a procesos de negocio, no estaba relacionado en modo alguno a la visión anteriormente utilizada, resultando la nueva metodología mucha más completa y abarcadora.

A pesar de las limitaciones observadas, esta iniciativa contaba con un fuerte apoyo de la presidencia de la empresa, lo cual sirvió para allanar el camino, superar los obstáculos que se presentaron, y permitió disponer, por primera vez en la historia de

la organización, en el año 2013, de un completo análisis de riesgos corporativo soportado sobre una base metodológica. Como resultado, fue posible dimensionar el nivel de exposición a los riesgos de la empresa; los de la organización como un todo y en particular de aquellos relacionados a la seguridad de la información.

Bajo la perspectiva del entrevistado, y en particular en lo que refiere a la gestión de los riesgos de seguridad de la información, este nuevo enfoque permitió a la organización mejorar en múltiples aspectos, entre los que se pueden encontrar: la posibilidad de priorizar las iniciativas de seguridad según la criticidad de los riesgos, justificar las inversiones antes los accionistas, realizar análisis de tipo ROSI (*Return Over Security Investment*), entre otros. Un último aspecto positivo, de gran relevancia, resulta del hecho que, a través del enfoque cuantitativo de la nueva metodología, fue posible dialogar con el directorio de la organización en el lenguaje del negocio, alcanzando así un mayor entendimiento de la relevancia de la seguridad de la información, sin detenerse en detalles técnicos.

Una evolución sobre el renovado enfoque

Dos años después de haber implementado la primer versión de la metodología de riesgo corporativo, en el año 2015, la organización inició un proceso de evolución en este aspecto, adoptando una nueva metodología, más flexible, que contemplaba el análisis de riesgos ya sea utilizando tanto el enfoque cuantitativo como el cualitativo, permitiendo así resolver los problemas y conflictos metodológicos observados en el

uso de la metodología originalmente utilizada desde el año 2013.

A los fines de comprender el impacto que la metodología de análisis de riesgos utilizada tiene sobre el resultado final del análisis, resulta necesario destacar que, utilizando la primer versión de la metodología, la organización había identificado 160 riesgos de criticidad alta para la organización (los riesgos eran clasificados en tres categorías: bajo, medio y alto), de entre los cuales 5 riesgos asociados a la seguridad de la información se encontraban entre los 20 riesgos de mayor impacto. El más importante de ellos relacionado ala posibilidad de acceso de *hackers* a la base de datos de clientes. Como resultado del nuevo enfoque metodológico, estos 5 riesgos se redujeron a tan sólo uno, asociado con la fuga de información.

Estas diferencias tan notorias en los resultados obtenidos mediante uno y otro tipo de análisis permiten destacarla importancia de utilizar una metodología de gestión de riesgos adecuada, siendo que resulta fundamental para la lectura que de la situación de la empresa se desprende.

Situación actual y desafíos de vista hacia el futuro

Al presente, luego de varios años de esfuerzo de la compañía en pos de realizar una adecuada gestión de riesgos, es posible afirmar que la organización dispone de un nivel de madurez moderado en lo que respecta a la ejecución de esta actividad. Se ha logrado avanzar de manera considerable en la identificación y gestión de los riesgos en las distintas gerencias y direcciones de la organización, pero es preciso

desarrollar aún una visión holística de la posición de riesgos de la empresa que surja como resultado de aquellos riesgos presentes en cada una de las áreas.

Al día de hoy, existe un gran detalle de los riesgos existentes en los distintos sectores de la organización, pero se dispone también de una acotada lista de riesgos corporativos, de alcance general a la organización, que no resultan de la agregación de los riesgos particulares de cada una de las áreas, sino que es informado sin el rigor de un análisis de riesgo detallado o proceso analítico alguno.

Esto conlleva diferentes desventajas, no sólo porque los riesgos corporativos no están relacionados con los riesgos detallados que permitiría una adecuada correlación en caso de un incidente, sino que además, más allá de los errores involuntarios en que se podría incurrir al informar estos riesgos de alcance general, también podría presentarse situaciones de conflicto de intereses, ya que es responsabilidad de cada uno de los directores informar los riesgos existentes en cada una de sus áreas, así como también el avance en la mitigación de estos.

A partir de lo expresado, y en vistas hacia el futuro, la organización deberá trabajar para lograr una mayor visibilidad sobre la forma en que cada uno de los riesgos de las distintas direcciones contribuye al riesgo corporativo y en qué medida.

2.4. Conclusiones

A través de las páginas del presente capítulo ha sido posible tomar conocimiento de

cuán extendida se encuentra la práctica de la gestión de riesgos en distintas organizaciones, el nivel de madurez que dicha actividad presenta en el mercado, y también los desafíos y dificultades que se encuentran vigentes al momento del presente estudio para su realización.

A partir de la información recabada mediante el uso de encuestas, se identificó la existencia de organizaciones donde la función de seguridad no se encontraba formalizada, así como también fue posible apreciar que sólo algunas de las entidades donde efectivamente existía la mencionada función, la estrategia de seguridad se constituía a partir de una adecuada evaluación de riesgos. Profundizando sobre este aspecto, también se advirtió que, aún en aquellas organizaciones en las cuales existía un proceso de gestión de riesgos establecido, no en todos los casos existía una retroalimentación adecuada que posibilite determinar el nivel de riesgo residual luego de la implementación de los controles de seguridad. Adicionalmente, fue posible notar, entre las dificultades para llevar adelante el proceso de gestión de riesgos, la importancia de disponer de personal debidamente capacitado en la materia, así como también la relevancia de un marco organizativo apropiado.

Coincidentemente, algunas de estas observaciones también fueron mencionadas por los informantes-clave consultados, los cuales han resaltado la importancia de disponer del apoyo de la dirección para avanzar en una adecuada gestión de riesgos. Sobre este aspecto, señalaron la falta de conocimiento de la dirección sobre el ámbito de la seguridad de la información en general y en relación la gestión de riesgos en particular, así como también la necesidad de justificar las inversiones en esta materia

mediante un análisis de retorno de inversión, el cual no resulta apropiado en estos casos. Adicionalmente, han resaltado la importancia de una apropiada comunicación por parte de los responsables de la seguridad de la información para transmitir correctamente la relevancia de este tema. Los informantes-clave también coincidieron en la importancia y dificultad para disponer del personal calificado para el desarrollo de la función, siendo que han destacado la complejidad que el proceso de evaluación de riesgos conlleva.

En última instancia, y mediante el análisis del caso, fue posible observar el papel que los mismos factores que fueron mencionados por los encuestados e informantes-clave tuvieron en la evolución de la gestión de riesgos en la organización bajo estudio. Aspectos tales como el apoyo de la dirección, la cultura organizacional, y la visión sobre la articulación entre la implementación de controles de seguridad y la gestión de riesgos fueron identificados a lo largo del análisis.

Las observaciones detalladas en el presente capítulo permitirán, junto con los conceptos desarrollados en el Capítulo 3, “Marco Teórico”, establecer importantes conclusiones para el presenta trabajo que se expondrán en el Capítulo 5, “Conclusiones, propuestas y aportes para futuras investigaciones”, que se encuentra a continuación.

3. CONCLUSIONES, PROPUESTAS Y APORTES PARA FUTURAS INVESTIGACIONES

La hipótesis propuesta al inicio del presente estudio afirma que en la actualidad existen una cantidad considerable de organizaciones que realizan una gestión de la seguridad de la información sobre un enfoque técnico, orientado a la protección de los activos informáticos aunque dejando de lado así una visión más amplia de la información que podría obtenerse a través de una adecuada gestión de riesgos.

Sobre la base que esta hipótesis ofrece, fue definido como objetivo general estudiar cuan extendida se encuentra la práctica de la gestión de riesgos en el campo de la seguridad de la información. En este sentido, se definieron también objetivos específicos que buscaron estudiar el concepto de riesgo y su aplicación al proceso de gestión de riesgos, la adopción de dicho proceso en organizaciones, su relación con la implementación de los controles de seguridad y también los desafíos que dicho proceso representa.

A los fines de sentar las bases teóricas para desarrollar los objetivos planteados, fue posible estudiar en detalle, en el "Marco Teórico", los pasos requeridos para desarrollar una evaluación de riesgos, revisando también las distintas metodologías y enfoques para la ejecución de esta actividad, observando en detalle las ventajas y desventajas de cada una de ellos.

Finalmente, en el Marco Investigativo fue posible detallar la información obtenida de

las distintas fuentes consultadas, para lo cual tres diferentes técnicas de recolección de datos fueron utilizadas: encuestas, entrevistas con informantes-clave y análisis del caso. Las encuestas permitieron conocer la situación, en relación a la gestión de riesgos, en la que se encontraban organizaciones de diverso tamaño y rubro. A través de las entrevistas a los informantes-claves, fue posible profundizar en los aspectos prácticos de la gestión de riesgos, tomando conocimiento de la visión de estos profesionales sobre los desafíos que la gestión de riesgos conlleva, así como también conocer sus apreciaciones sobre las razones que determinan la situación actual del mercado en lo que respecta a la práctica de la gestión de riesgos. En última instancia, a través del análisis del caso fue posible estudiar en detalle las distintas etapas que la empresa bajo estudio debió superar en su camino hacia gestión de la seguridad de la información basada en la gestión de riesgos.

A partir de la investigación realizada, y habiendo alcanzado los objetivos establecidos para la presente tesis, es posible determinar que la hipótesis fue corroborada, siendo que fue posible comprobar la existencia de una gran cantidad de organizaciones que implementan controles de seguridad con un enfoque orientado hacia los activos informáticos, esto es, con una visión netamente técnica. Entre estas organizaciones se hallan tanto a aquellas que no poseen establecida un área de seguridad de la información, como también las que, aun cuando formalmente realizan actividades en este sentido bajo un esquema organizacional definido, no han desarrollado una práctica de gestión de riesgos de la información.

Más allá de esto, la investigación también permitió obtener importantes precisiones

sobre la situación actual de las organizaciones que sí realizan una gestión de la seguridad de la información basada en la gestión de riesgos en lo que a este proceso respecta. Estos aspectos se encuentran detallados en las conclusiones generales que se exponen más adelante.

3.1. Generalización de los hallazgos

Por ser una investigación de tipo exploratorio-descriptiva, con enfoque predominantemente cualitativo, diseño no experimental y una muestra dirigida y no probabilística, no resulta posible la generalización de los hallazgos. En este tipo de estudios no se pretende trasladar los resultados del análisis a una población más amplia, ni tampoco interesa tal extrapolación, aunque sí se ha tenido como objetivo el ayudar a la toma de decisiones en los temas tratados.

3.2. Conclusiones generales

A partir del material teórico consultado y las observaciones resultantes del trabajo de campo realizado, es posible obtener distintas conclusiones en relación a la gestión de riesgos de la información que se encuentran detalladas a continuación y expuestas en distintos títulos a efectos de una mejor organización.

Acerca de la cultura organizacional en relación a la seguridad de la información

A lo largo de las páginas del presente estudio se han podido recorrer aquellos aspectos teóricos relacionados con el concepto de riesgo, su evaluación y tratamiento, así como también se ha podido obtener un entendimiento sobre la aplicación de dichos conceptos teóricos en la actualidad. Sin embargo, existe un aspecto preliminar que resulta de vital importancia para la gestión de riesgos de la información, y refiere a la valoración de la información como activo fundamental de las organizaciones modernas, y consecuentemente la necesidad de resguardarlo.

Toda institución moderna dispone de una gran cantidad de información, sin importar si se trata de organizaciones sin fines de lucro, organismos gubernamentales, instituciones educativas o empresas, entre otras. En mayor o menor medida, todas estas entidades almacenan, transportan y procesan información, ya sea mediante complejos sistemas informáticos, o sencillamente impresa en papel. En algunos casos se trata de información generada por la misma entidad –tales como registros contables, políticas, procedimientos, o información de productos–, en tanto que en otros casos se trata de información cedida por terceros y puesta bajo custodia de la organización en cuestión –como por ejemplo, información personal de los colaboradores o datos de clientes–.

Cualquiera que sea el origen de la información, su propósito, y el medio de soporte en el que se encuentre, representa un activo valioso, que, como cualquier otro, debe ser adecuadamente protegido. Preservar la confidencialidad, integridad y disponibilidad de la información resulta así imperioso para garantizar la continuidad de las

operaciones y mantener la posición competitiva, resguardando a la vez la imagen y reputación de la organización, y observando además el cumplimiento de los requisitos legales y regulatorios.

A partir del trabajo de campo realizado en el marco de la presente tesis, fue posible identificar la existencia de una importante cantidad de organizaciones en las que todavía no existe un área o sector específicamente destinado a la protección de la información. Si bien este aspecto en particular –el marco organizativo de la función de seguridad– se encuentra fuera del alcance del presente estudio, resulta relevante ser mencionado en cuanto es una muestra cabal de la importancia que las organizaciones asignan a esta problemática.

Siendo así, es dable concluir que todavía existe una porción considerable de organizaciones que, aun cuando entiendan en toda su magnitud la importancia de la información para la consecución de los objetivos propuestos, no han asimilado la posibilidad de que dicha información pueda ser vulnerada en forma alguna, y por consiguiente no destinan esfuerzos para evitar que esto suceda. En estos casos, sin duda es este el primer escollo a superar en pos de realizar una eficiente gestión de los riesgos de la información.

Acerca del enfoque adoptado para la protección de la información

Otro aspecto relevante observado se encuentra relacionado con el enfoque utilizado a la hora de implementar controles de seguridad de la información. Ha sido

posible advertir que, en tanto algunas organizaciones efectivamente realizan una gestión de riesgos a partir del cual se identifica la necesidad de disponer de ciertos controles de seguridad, existen otras organizaciones que han avanzado en la implementación de controles de seguridad sin contar con dicha información, esto es, sin disponer de una clara visión integral de los riesgos que a través de la implementación de dichos controles de seguridad se mitigan.

Resulta sencillo establecer a simple vista que aquellas entidades que han decidido avanzar en la implementación de controles de seguridad sin realizar una adecuada gestión de riesgos no lo encuentran necesario o bien, aun considerándolo necesario, se enfrentan con dificultades para llevar adelante esta actividad, aspecto sobre el que se profundizará en las próximas secciones. Aun así, no resulta posible establecer que el concepto de riesgo se encuentre ausente en estos casos, como se podrá observar a continuación.

Fue posible notar que en las mencionadas organizaciones se reconocen riesgos que afectan a determinados activos de IT que son identificados como críticos, esto es: sistemas de gestión críticos para el negocio, *firewalls* perimetrales, y otros elementos específicos de la infraestructura de IT. Sobre la noción de los riesgos que podrían afectar a estos activos seleccionados, se implementan controles de seguridad, pero siempre con un enfoque acotado al componente de IT que se desea proteger. Siendo así, se advierte que el concepto de riesgo se encuentra presente, aun cuando el tratamiento que se le da a estos sea insuficiente.

En una primer observación, es posible notar que no existe en estas

organizaciones una clara distinción entre la información y los sistemas en los que dicha información se procesa o almacena, confundiendo así la necesidad de proteger un determinado sistema con aquella de resguardar la información en ellos contenida. En estos casos, de realizarse un análisis más profundo de la información a proteger como parte de un proceso de evaluación de riesgos, se podría observar que en la actualidad la información muchas veces traspasa la frontera de los sistemas que la almacenan, ya sea porque los usuarios imprimen la información, hacen sus propias copias de seguridad, o realizan reportes que pueden ser distribuidos a otras personas y/u organizaciones. A partir de esto, resulta evidente que desarrollar controles de seguridad para proteger un determinado sistema de información no garantiza la seguridad de la información.

Un segundo aspecto, tal vez de mayor relevancia que el anteriormente expresado, se encuentra relacionado con la visibilidad que de los riesgos se posee. Siendo que estas organizaciones no han realizado una evaluación de riesgos, la cual permite obtener una visión completa e integral de los riesgos a los que la entidad se encuentra expuesto, se dispone en cambio de una percepción de los riesgos a partir de ciertos activos que se desea proteger que resulta ser una visión parcializada, segmentada del riesgo, y acotada únicamente a aquellos elementos bajo análisis. En tal caso, este enfoque omite importantes aspecto del contexto organizacional, tanto interno como externo, y por lo tanto impide identificar riesgos que surjan directamente de aquellos elementos del contexto omitidos, así como también otros riesgos que podrían darse a partir del desarrollo de escenarios más complejos donde múltiples amenazas puedan

desarrollarse al mismo momento.

Acerca de la cultura organizacional en relación a la gestión de riesgos

Así como fue posible observar el rol preponderante que cumple la postura general de la organización en relación a la seguridad de la información, del mismo modo se ha observado a través de la teoría consultada y también de la investigación realizada cuán desafiante resulta desarrollar una administración de la seguridad de la información basada en una gestión de riesgos cuando no existe el marco organizacional adecuado.

Este aspecto ha sido mencionado por distintos autores que fueron citados en el Marco Teórico, en donde se advirtió la necesidad de disponer del apoyo y la participación activa de la dirección. Asimismo, este factor también fue observado uniformemente en la investigación, siendo que la necesidad de apoyo de la dirección fue un tópico que se presentó tanto en todas las herramientas de investigación utilizadas.

Es posible entonces mencionar dos factores que influyen en la cultura de la organización en este sentido: la visión propia de la dirección, y, específicamente en lo que respecta a la gestión de riesgos de la información, la demanda del mercado, ya sea debido a requerimientos de clientes o bien de la legislación y/o regulación vigente.

En relación al primero de los puntos mencionados, es preciso recordar que la gestión de riesgos es preponderantemente una actividad que tiene por finalidad la toma de

decisión. Todo el proceso tiene por objetivo generar la información necesaria para que la dirección pueda tomar una decisión acerca de los riesgos que está dispuesta a asumir para la consecución de los objetivos de la entidad sobre la base de resultados obtenidos a través de un proceso analítico. Siendo así, si la dirección no considera que los resultados de un análisis de riesgos puedan contribuir en manera alguna a la toma de mejores y más informadas decisiones, difícilmente apoye esfuerzo alguno en este sentido y apruebe que se destinen recursos para la gestión de riesgos.

Esta visión de la dirección se ve influenciada, en muchos casos, por el segundo de los puntos mencionados, en relación a las demandas del mercado. Desde el punto de vista del marco legal o regulatorio, son pocas las industrias en Latinoamérica a las cuales el Estado Nacional exige cuidados especiales en relación a la seguridad de la información. Los mayores controles se observan en el sector financiero, y también en términos generales relacionados con la protección de datos de personas de existencia física, pero no existen en la región requerimientos de mayor alcance y más detallados como por ejemplo se pueden observar en Estados Unidos con las regulaciones PCI DSS (*Payment Card Industry Data Security Standard*) y HIPAA (*Health Insurance Portability and Accountability Act*), o los estándares de Protección de la Información de la Unión Europea. Concordantemente, tampoco se observan mayores requerimientos de los distintos segmentos de clientes que motiven a las empresas a implementar ciertos controles de seguridad, y que permitan, adicionalmente, observar un beneficio directo resultante de la implementación de controles de seguridad.

En cualquier circunstancia, resulta de gran importancia para los profesionales

especializados en la gestión de riesgos en general y aquellos profesionales de la seguridad de la información en particular hacer notar a la dirección la importancia del proceso de gestión de riesgos.

Acerca del proceso de evaluación de riesgos

A partir de los conceptos teóricos explorados en la presente tesis, y considerando también las opiniones y experiencias obtenidas a través del Marco Investigativo, resulta evidente que la evaluación de riesgos es un proceso complejo. Sin embargo, es posible advertir que el proceso en sí no resulta ajeno a la naturaleza humana, siendo que las personas realizan en su vida cotidiana y en forma completamente intuitiva varias evaluaciones de riesgo por día. Decisiones tales como la contratación de un seguro automotor, de vida o para la vivienda, la selección de un *portfolio* de inversiones, o inclusive decisiones triviales como tomar un taxi por sobre caminar en un barrio peligroso representan claro ejemplos de evaluaciones de riesgos, en donde las amenazas, la probabilidad de ocurrencia, el impacto y el costo de mitigar esos riesgos son considerados sin siquiera tener conciencia de este hecho.

Sin embargo, a la hora de realizar un análisis de riesgos en el contexto de una organización, se puede apreciar la existencia de dos grandes dificultades: en primer lugar, la complejidad y extensión del contexto que se desea analizar, y adicionalmente, la dificultad para establecer y acordar criterios objetivos de evaluación.

Sobre el primero de los puntos mencionados, es posible identificar varios aspectos que hacen a la complejidad del proceso, tales como:

- Dificultad para identificar amenazas en un contexto de globalización e interconexión mundial;
- Dificultad para asignar una probabilidad de ocurrencia a eventos, ya sea por no disponer de estadísticas confiables o bien por tratarse de eventos discretos;
- Dificultad para asignar un valor monetario a activos intangibles (entre ellos la información);
- Dificultad para correlacionar distintos eventos y amenazas que podrían desencadenar en escenarios específicos.

En este sentido, resulta imprescindible disponer de una metodología de gestión de riesgos que permita administrar toda esta complejidad y obtener resultados válidos. No obstante, pareciera que, a pesar de las muchas metodologías que se encuentran disponibles en el mercado, resulta muy difícil para las organizaciones adoptar dichas metodologías sin antes adecuarlas a la realidad y contexto de la organización en cuestión. Este aspecto queda evidenciado a partir del hecho que más de la mitad de las organizaciones que participaron en la encuesta, y también aquella que fuera objeto de estudio para el análisis del caso, ha utilizado una metodología de evaluación de riesgos propia o al menos ajustada a las necesidades de la organización.

En lo que respecta al segundo de los puntos mencionados –establecer y acordar criterios objetivos de evaluación–, es posible establecer que el desafío radica, en

primer lugar, en describir con precisión los elementos que intervienen en la evaluación de una determinada situación, y en segundo lugar, consensuar la valoración que de dicho elementos se realizará en la organización. Se podrá observar que la complejidad surge a partir del hecho que estos procesos racionales se desarrollan intuitivamente y, más aún, son completamente subjetivos según la personalidad de cada individuo. En cualquier caso, este factor también influye en gran medida en la metodología de gestión de riesgos que se adopte y, consecuentemente, en la ejecución del proceso de evaluación de riesgos.

A partir de los argumentos expuestos, es dable establecer como una importante barrera hacia la gestión de riesgos de la información la necesidad de desarrollar una metodología de gestión de riesgos que se ajuste a las necesidades, cultura y nivel de madurez de la organización.

Acerca de los recursos requeridos para la evaluación de riesgos

Un último aspecto a señalar, no por ello menos importante, se encuentra relacionado con los recursos humanos asignados a la ejecución de la evaluación de riesgos. En el apartado anterior fueron mencionados los desafíos que plantea disponer de una metodología de gestión de riesgos adecuada. Ya sea que se trate de desarrollar la mencionada metodología, adaptar una ya existente a las necesidades de la organización o bien ejecutar la evaluación de riesgos sobre la base de una metodología ya establecida, en cualquier caso existe un importante componente

humano en el proceso, que sin duda afectará los resultados finales obtenidos.

Desafortunadamente no existe una profesión que tenga por objetivo la gestión de riesgos, por lo que las personas que se desarrollan en este campo provienen de distintas profesiones, cada una de las cuales aporta, desde su visión, diversas perspectivas que contribuyen al resultado final pero que también pueden sesgar el análisis si el profesional en cuestión no dispone de una visión suficientemente amplia sobre el proceso y el giro del negocio. A modo de ejemplo, profesionales de carreras de tecnología podrían enfocarse demasiado en riesgos tecnológicos, o bien no llegar a comprender los procesos de negocio más allá de las herramientas informáticas que los soportan, en tanto que profesionales de carreras de administración de empresas podrían por el contrario no alcanzar a comprender la complejidad técnica de las organizaciones modernas en lo que a sistemas de información concierne.

En cualquier caso, los especialistas asignados a la tarea deberán también asimilar aquellos criterios establecidos por la dirección para el desarrollo de la evaluación de riesgos, estableciendo de este modo un marco metodológico universalmente aceptado dentro de la organización, evitando así caer en criterios subjetivos.

A partir de lo anteriormente expuesto, es posible advertir la importancia que posee disponer de recursos humanos capacitados y con experiencia en este complejo proceso, elemento indispensable para lograr obtener una visión clara y precisa de los riesgos a los que la organización debe hacer frente.

3.3. Propuestas

A partir de las observaciones y conclusiones desarrolladas en el presente capítulo, es posible identificar diversas consideraciones que permitirán una mejora en el proceso de evaluación de riesgos de la información, entendiéndose por esto una ejecución más eficiente de dicho proceso y la obtención de mejores, más completos y precisos resultados –entiéndase, riesgos–. Estas consideraciones se encuentran detalladas a continuación.

Apoyo de la dirección

Se ha realizado mucho hincapié sobre este aspecto a lo largo de las páginas de la presente tesis, y aun así se considera este un factor a mejorar. El apoyo de la dirección no se limita únicamente a facilitar la ejecución de la evaluación de riesgos y disponer de los recursos necesarios para ello, sino que también implica comprometerse con los resultados que de dicho estudio deriven y el tratamiento que se le dará a los riesgos. De poco sirve realizar una evaluación de riesgos si no es para advertir a la dirección sobre una determinada condición y que se tomen decisiones concretas sobre cómo administrar dicha situación. En este sentido, es preciso que los profesionales a cargo de la actividad puedan exponer con claridad los objetivos del proceso, cuáles son sus resultados y qué tipo de decisiones se esperar por parte de la dirección en relación a los resultados (es preciso recordar que la omisión de los resultados implica la aceptación pasiva de los riesgos informados).

Evitar la simplificación de los resultados obtenidos

Los ejecutivos de las organizaciones modernas se encuentran a menudo sobrepasados en sus actividades diarias, con largas jornadas laborales en donde se dispone de poco tiempo para el tratamiento de los múltiples asuntos que hacen al giro normal de la organización. Esto podría llevar a los profesionales a cargo de la evaluación de riesgos a seleccionar y presentar sólo algunos de los riesgos identificados –aquellos de mayor criticidad–, en pos de facilitar la atención de la dirección sobre estos temas. Sin embargo, aun cuando resulte necesario llamar la atención sobre los riesgos más relevantes identificados, que son aquellos que requieren más urgente tratamiento, es importante informar adecuadamente a la dirección sobre la totalidad de los riesgos observados para que exista una consciencia sobre la magnitud y complejidad del contexto en el que la organización se desarrolla y, aun cuando la dirección tome acción directa sobre aquellos riesgos de mayor relevancia, debe hacer un seguimiento completo e integral de todos los riesgos con los que la organización debe lidiar.

Equipo de trabajo multidisciplinario

Se ha hecho mención en páginas anteriores acerca de la necesidad de disponer de personal calificado para la realización de las evaluaciones de riesgo. Sin embargo, resulta más importante aún la constitución de equipos de trabajo multidisciplinarios que permitan realizar un análisis completo de la situación de la institución. La gestión de riesgos es un proceso que atraviesa a las organizaciones horizontalmente, y por

consiguiente múltiples aspectos deben ser observados y analizados tanto para identificar y valorar los activos de información, como también para identificar y ponderar amenazas, vulnerabilidades, probabilidades de ocurrencia e impacto. La posibilidad de establecer un grupo interdisciplinario que incorpore profesionales de la seguridad de la información, informática, del derecho y también responsables del negocio permitirá nutrir el análisis de distintas perspectivas que sin duda resultarán en una evaluación de riesgos más completa y precisa.

Herramienta informática de soporte al proceso

Se ha podido observar a lo largo del estudio cuan compleja y extensa puede resultar una evaluación de riesgos que cubra distintos activos de información en un contexto globalizado e interconectado como el presente. A partir de esto, no resulta sencillo modelar toda esta complejidad sin disponer de una herramienta informática específicamente diseñada para tal fin. Se ha podido observar que muchas organizaciones que se embarcan en el desarrollo de una gestión de riesgos se encuentran obstaculizadas para avanzar en este sentido al no poder documentar la realidad que observan de una forma tal que facilite su análisis. Disponer de dicha herramienta permitirá organizar la información adecuadamente, soportar los distintos pasos del proceso y presentar los hallazgos y resultados en forma clara y precisa.

Validación de los criterios de evaluación adoptados con la realidad

A partir del material teórico consultado, se ha observado que, al momento de definir la metodología de gestión de riesgos a utilizar, es preciso establecer los criterios de ponderación y/o valoración que serán utilizados a lo largo del proceso de evaluación de riesgos. En relación a esto, es preciso realizar una regular validación de los resultados que siguiendo los mencionados criterios se obtienen para garantizar que estos se encuentren en concordancia con la realidad. De otro modo, se corre el riesgo de realizar un análisis completo de los riesgos que podría arrojar resultados inconsistentes o bien incongruentes con el escenario actual de la organización.

Apoyarse en casos de uso

Los casos de uso son esquematizaciones que permiten detallar escenarios y que, por lo tanto, facilitan la creación de una descripción, en mayor o menor medida gráfica según la técnica utilizada, de determinados procesos o interacciones. Siendo que ha sido señalado en múltiples oportunidades a lo largo del presente estudio la extensión y complejidad del contexto en el que las organizaciones modernas se desarrollan, la utilización de casos de uso facilitará la segmentación y consecuente análisis del entorno, lo cual permitirá analizar con mayor rigor, detalle y profundidad las amenazas y vulnerabilidades sobre los que se construye el análisis de riesgos. Se evita de este modo encontrarse perdido en la descripción de un contexto tan basto y extenso que resulte muy difícil de observar y considerar.

3.4. Aportes para futuras investigaciones

A partir de la presente tesis, distintos aspectos de la temática bajo estudio podrían ser utilizados para desarrollar nuevas líneas de investigación. A continuación se detallarán algunos de ellos:

- Métodos para medir la efectividad de la gestión de riesgos: siendo que la ausencia de incidentes no es prueba suficiente para garantizar una correcta gestión de riesgos, ¿de qué forma es posible obtener una evidencias concretas sobre la efectividad del proceso de gestión de riesgos?
- La utilidad de los métodos cuantitativos por sobre aquellos cualitativos: fue posible observar que los métodos cualitativos realizan ponderaciones y evaluaciones subjetivas de los distintos elementos que conforman el análisis de riesgos. A partir de esto, ¿en qué medida un análisis con rigor matemático podría ofrecer resultados más precisos y confiables, y en qué medida es esto factible de ejecutar?
- Automatización del proceso de evaluación de riesgos: ¿en qué medida es posible automatizar la captura de aquellos datos sobre los cuales se constituye la evaluación de riesgo de forma tal de permitir una ejecución menos costosa, en términos de esfuerzos, del proceso de evaluación de riesgos?
- Educación superior en materia de gestión de riesgos: se ha señalado con anterioridad en el presente estudio la ausencia de una profesión que tenga por objetivo la gestión de riesgos. En este sentido, ¿existe oportunidad para desarrollar un plan de estudios que aborde la problemática de la gestión de

riesgos?

La posibilidad de profundizar sobre los conceptos anteriormente mencionados permitirá aportar nuevas perspectivas al proceso de gestión de riesgos en lo que respecta a su eficiencia y precisión, resultando así en una considerable mejora de la calidad de la información para la toma de decisiones.

3.5. Consideraciones finales

A lo largo de las páginas del presente estudio se ha profundizado sobre las características de la gestión de riesgos, el marco conceptual y metodológico bajo el cual esta actividad se desarrolla, cuán extendida se encuentra esta práctica en la actualidad y también los desafíos que representa para aquellas organizaciones que desean llevarla a cabo. Más allá de estos aspectos, una última palabra merece ser mencionada en relación a la gestión de riesgos en cuanto a su importancia, relevancia y necesidad en el contexto actual de la economía mundial y de la evolución tecnológica.

El estado actual de la tecnología lleva a las empresas a contratar servicios informáticos en lo que se conoce en español como “la nube”, donde, dependiendo del servicio, no es posible determinar en ocasiones siquiera en qué país los datos son almacenados. El acceso a los datos ya no se efectúa únicamente desde computadoras instaladas físicamente en las oficinas de las distintas organizaciones, sino que se desarrolla desde *notebooks* conectadas remotamente, aplicaciones web, y hasta aplicaciones en teléfonos celulares. Adicionalmente, la tecnología permitió el

desarrollo de una economía globalizada como nunca se había observado en la historia de la humanidad. Diferentes servicios son provistos por centros de servicios compartidos establecidos en ciudades a los que muchas personas les resultaría difícil siquiera identificar en qué país estos se encuentran. En los últimos años se ha visto desaparecer las fronteras tecnológicas de distintos organismos ya sean privados o gubernamentales, donde prima la ubicuidad del acceso a la información.

Particularmente en el campo de la seguridad de la información, en los últimos años han salido a la luz incidentes de seguridad que han afectado seriamente a empresas e individuos por igual, y que sorprenden no solo por la magnitud del impacto, sino también por las razones que motivaron a los atacantes a llevar a cabo estas actividades. El ataque al sitio de citas Ashley Madison fue perpetrado por activistas informáticos en contra de la promoción de un estilo de vida libertino. El ataque a la empresa Sony fue supuestamente ejecutado por Corea del Norte, en principio, motivado por la película *The Interview* que ponía en ridículo al gobierno de ese país.La fuga de información que se dio a conocer bajo el nombre de *Panama Papers*[1]fue producto de un empleado que no deseaba "contribuir" a la "optimización – evasión– fiscal" y se sentía moralmente afectado por este hecho.

Lo anteriormente expuesto establece la imperiosa necesidad de dar un salto evolutivo en la gestión de la seguridad de la información hacia la gestión de riesgos, que

[1]Nombre por el que se conoció la fuga de información de la firma panameña Mossac Fonseca.

permita a las organizaciones analizar un contexto tan complejo como extenso, en constante evolución y cambio, y que requiere una atención y gestión activa por parte de los profesionales de la seguridad en pos de proteger el activo más importante de las organizaciones del siglo XXI, la información.

BIBLIOGRAFÍA

Libros:

- Harris, Shon (2013). *CISSP Exam Guide (6th Edition).* McGraw-Hill
- Hubbard, Douglas W. (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It.* New Jersey: John Wiley & Sons, Inc.
- ISACA (2014). *CRISC Review Manual 2014.*
- Haag, Stephen; Cummings, Maeve(2004). *Management Information Systems for the Information Age (8th Edition).* McGraw-Hill
- Castells, Manuel (2010). The Rise of the Network Society: The Information Age: Economy, Society, and Culture Volume I (2nd Edition). Wiley-Blackwell.

Publicaciones:

- COSO, Committee of Sponsoring Organizations of the Treadway Commission (2004). *Gestión de riesgos corporativos – Marco integrado.*
- ISO, International Organization for Standardization (2009) *31000 – Risk*M*anagement – Principles and guidelines.*
- NIST, National Institute of Standards and Technology (2011)*Special Publication 800-39 Managing Information Security Risk.* Gaithersburg.
- NIST, National Institute of Standards and Technology (2012) *Special Publication*

800-30 – Revision 1: Guide for Conducting Risk Assessments. Gaithersburg.

- SEI, Software Engineering Institute (2010). *Risk Management Framework.* Hanscom AFB.

ANEXO I

Formulario de encuesta a profesionales de la seguridad de la información

GESTIÓN DE RIESGOS DE LA INFORMACIÓN

ENCUESTA

Ing. Guillermo Frick *guillermofrick@outlook.com*

*(No se requerirán más de 15 minutos para completar esta encuesta. Desde ya agradecemos su tiempo)***.**

Objetivos y marco en el que se realiza esta encuesta

Esta encuesta se realiza dentro del marco de una tesis de MBA a ser presentada en la Facultad de Ciencias Económicas de la Universidad de Palermo, Argentina. No cuenta con otro fin que el de estudiar y profundizar el estado del tema bajo revisión.

Aclaraciones

La información contenida en esta encuesta será tratada bajo la mayor confidencialidad y su utilización será solamente académica.

En caso de no poder contestar alguna de las preguntas, se agradece que sea completado el resto del formulario para permitir continuar con la investigación.

Gestión de riesgos de la información – Definición y alcances

A los fines del presente trabajo, se entiende como riesgo la posibilidad de ocurrencia de un evento que afecte negativamente a una determinada organización. Puntualmente, los riesgos de la información son aquellos que se encuentran relacionados con los activos de información de la organización.

El concepto de gestión de riesgos es posible visualizarlo como el proceso organizacional que tiene por objetivo la detección y administración de los riesgos de forma tal de obtener un determinado nivel de certeza en relación al logro de los objetivos de la organización.

En último lugar, es posible decir que la evaluación de riesgos es la actividad que tiene por objetivo producir una lista de riesgos que luego será priorizada y utilizada para determinar los planes de acción necesarios que –eventualmente- serian requeridos para darle tratamiento a cada uno de ellos.

CUESTIONARIO

- Nombre del participante y posición:
- Nombre de la empresa:
- Rubro de la empresa en la que se desempeña:
- Origen del capital

a. Internacional _____

b. b. Nacional _____

- Cantidad de empleados

- ✓ Argentina: _____
- ✓ Región (indicar países) _____
- ✓ Total Corporación _____

- Fecha en que se completa esta encuesta:

1. ¿Existe en su organización un sector cuya misión consista en gestionar la seguridad de la información?: a. Si. b. No.
[Si se responde afirmativamente la pregunta 1] 2. El mencionado sector reporta a: a. Gerente/Director de Sistemas o CIO. b. Gerente/Director de Finanzas o CFO. c. Gerente/Director de Riesgos o CRO. d. Director General o CEO. e. Otro (por favor detallar):_____
3. ¿Cuál es su rol en dichos ector? a. Gerente/Director b. Jefe/Supervisor c. Colaborador d. No aplica

4. Considera Usted que los controles de seguridad que la organización pone en funcionamiento tienen por objetivo:
   a. Cumplir con requerimientos legales y/o regulatorios.
   b. Cumplir con políticas internas de su organización, ya sean locales, globales o regionales.
   c. Satisfacer las expectativas de los clientes de la organización.
   d. Mitigar riesgos que puedan afectar la seguridad de la información.
   e. Otro (por favor detallar):_____

[Si no se seleccionó el punto d. de la pregunta 4]	**[Si afirmativamente se seleccionó el punto d. de la pregunta 4]**
5. Siendo que no ha seleccionado el punto d. de la pregunta anterior relacionado con la mitigación de riesgos, considera que: a. No se posee conocimiento de la existencia de riesgos que afecten la seguridad de la información	5. En cuanto a la mitigación de los riesgos indicada en el punto d. de la pregunta anterior, ¿se ha conducido en su organización un proceso formal de evaluación de riesgos para identificar los mencionados riesgos? a. Si b. No c. No poseo conocimiento de ello.

	[Si se responde afirmativamente la pregunta 5, esto es, se ha conducido una evaluación de riesgos formal] 6. Se ha seguido alguna metodología reconocida en el mercado para desarrollar el análisis de riesgo, como por ejemplo MAGERIT, ISO 31.000, ISO/IEC 27.005 o NIST SP800-39? *Respuesta:* a. Si. Se utilizó (indicar la metodología utilizada):_____ b. No. Se utilizó una metodología propia. c. Se utilizó una metodología propia, aunque basada en una metodología de mercado. Para este fin, se utilizó (indicar la metodología utilizada):_____	**[Si se responde negativamente la pregunta 5, esto es, <u>no</u> se ha conducido una evaluación de riesgos formal]** 6. Siendo que no se ha conducido un proceso de evaluación de riesgos formal, pero sin embargo uno de los objetivos de la implementación de los controles de seguridad es mitigar riesgos, ¿cómo se identifican los riesgos que deben ser mitigados? *Respuesta:* _____ _____ _____

	7. ¿Son revisados regularmente los riegos identificados, con el objetivo de determinar la existencia de nuevos riesgos y/o cambios en los riesgos ya detectados? *Respuesta:* a. Si b. No c. No poseo conocimiento de ello	7. ¿Por qué motivo considera que no se ha realizado una evaluación de riesgos? *Respuesta:* _____ _____ _____
	8. ¿Se posee un conocimiento acerca de la medida en que los controles de seguridad implementados mitigan los riesgos detectados? *Respuesta:* a. Si b. No c. No poseo conocimiento de ello	

9. ¿Cuál es la posición general de la organización a la que pertenece en relación a la gestión de riesgos?
   a. La organización dispone de una cultura de gestión de riesgos desarrollada y, consecuentemente, asigna recursos a la gestión de los riesgos corporativos.
   b. La organización posee una cultura de gestión de riesgos incipiente. Se desarrollan actividades con escasa coordinación para gestionar los riesgos corporativos.
   c. La organización no posee una cultura de gestión de riesgos desarrollada. No se desarrollan actividades en forma coordinada y sistemática que tengan por objetivo gestionar riesgos.
   d. Otro (por favor detallar): _____

10. ¿Cuál es su opinión personal en lo que respecta a la gestión de riesgos de la información en lo que respecta a utilidad, necesidad y dificultad de ejecución?

    Respuesta:

    _____

    _____

11. Por favor, ingrese a continuación cualquier comentario adicional que desee agregar en relación a las preguntas anteriores.

    Respuesta:

    _____

ANEXO II

Guía de entrevista a informantes-clave

Detalle de los entrevistados

Los profesionales y especialistas entrevistados se muestran en el cuadro expuesto a continuación:

Cuadro 11. Detalle de informantes-clave

Nombre	Antecedentes	Fecha de entrevista	Modo de realización	Duración
Pablo Correnti	• Profesional con 20 años de experiencia en el campo de la seguridad de la información, con experiencia en sector privado, gobierno y docencia.	12 de agosto del 2015	Personal	1 hora
Diego Taich	• Profesional con amplia en el campo de la seguridad de la información, con especialización en consultoría y servicios forenses.	4 de septiembre del 2015	Personal	1 hora y 15 minutos

Fuente: Elaboración Propia (2016)

Diseño de las entrevistas

Las entrevistas, semi-estructuradas, contaron con las siguientes preguntas básicas:

4. ¿Cuán extendida considera que se encuentra la práctica de evaluaciones de riesgo en el campo de la seguridad de la información?
5. ¿Cuáles considera que son los factores que influyen en dicha situación?
6. ¿Cuáles son las ventajas y desventajas que ofrece este escenario para las organizaciones?
7. ¿Cuáles son las principales dificultades a la hora de llevar adelante una evaluación de los riesgos que comprometen la seguridad de la información?
8. ¿En qué medida influyen sobre dicha actividad la cultura organizacional y visión de la gerencia en relación a la gestión de riesgos en general y a la seguridad de la información en particular?
9. ¿Cuál considera Usted que será la evolución del mercado en relación a este tema?
10. ¿Existen mejores prácticas que pueda mencionar?
11. ¿Desea Usted realizar algún otro comentario al respecto relacionado a este tema?

CURRíCULUM VITAE

Trayectoria laboral

PwC (Agosto 2005 – presente)

PwC ofrece servicios de Auditoría, Consultoría y Asesoramiento Impositivo y Legal. Más de 169.000 personas en 158 países trabajan en equipo brindando servicios profesionales.

- CISO – Chief Information Security Officer para Sudamérica (Julio 2010– presente)

Reportando al CIO Regional, a cargo de un equipo de trabajo de 8 colaboradores. Responsable por: Programa de Seguridad de la Información; Planeamiento estratégico regional de Seguridad de la Información; Representación de la región en los distintos grupos de trabajo globales; Elaboración y control del presupuesto del área; Gestión de riesgos y cumplimientos de normas de seguridad; Respuesta ante incidentes de seguridad; Programa de *cybersecurity*.

- Gerente Regional de IT & Seguridad de la Información para Sudamérica (Julio 2008–Junio 2010)

Reportando al Director Regional de Tecnología y al CISO, responsable por: Gestión de proyectos de infraestructura de Tecnología Informática (TI) y Seguridad de la Información (SI); Coordinación de equipos de trabajo regionales y con proveedores; Definición de políticas, procedimientos y estándares de IT y Seguridad de la Información; Representación de la región en los

distintos grupos de trabajo globales; Elaboración de RFP (*Request For Proposal*) y selección de proveedores; Gestión de contratos con proveedores; Auditorías de seguridad; Análisis de riesgos.

- Líder de Proyectos Regional para Sudamérica (Agosto 2005 –Junio 2008)

Reportando al Director Regional de Tecnología y al CISO, responsable por: Gestión de proyectos de TI, Comunicaciones y Seguridad de la Información; Realización de auditorías de seguridad; Implementación de herramientas de TI y Seguridad de la Información; Análisis de riesgos.

Telecom Argentina (Julio 1998 – Julio 2005)

El Grupo Telecom ofrece a sus clientes una variedad amplia de servicios de comunicaciones, entre ellos comunicaciones urbanas, interurbanas e internacionales, transmisión de datos y servicios de Internet.

- Supervisor de Implementaciones (Octubre 2003 – Julio 2005)

Reportando al Gerente de Aseguramiento de Datos, a cargo de un equipo de trabajo de 10 colaboradores.Responsable por: Coordinación y conducción del sector de implementación de servicios de datos para el segmento Operadores y Prestadores; Participación en la definición de SLA con clientes internos; Participación en la definición de procesos de provisión de servicios; Implementación de servicios de datos sobre tecnología IP, FR y ATM.

- Implementador de Servicios de Datos (Julio 2002 – Septiembre 2003)

Reportando al Supervisor de Implementaciones, responsable por: Administración de servidores Sun Solaris; Administración de servidores de aplicaciones Radius, Tacacs y DNS; Implementación de servicios de datos sobre tecnología IP, FR y ATM; Implementación de servicios de VOIP; Análisis de capacidad y reingeniería de redes WAN y LAN.

- Líder de Proyecto (Julio 2000 – Junio 2002)

Reportando al Gerente de Sistemas de la Unidad de Negocios, a cargo de un equipo de trabajo de 2 colaboradores. Responsable por: Relevamiento de requerimientos de las áreas de negocio; Especificación funcional y técnica de aplicaciones; Gestión de proyectos de implementación de sistemas; Capacitación de usuarios; Atención de reclamos (nivel 3).

- Analista de sistemas (Julio 1998 – Junio 2000)

Reportando al Líder de Proyecto, responsable por: Soporte a usuarios de las aplicaciones de negocio; Prueba de nuevas funcionalidades previas a la implementación; Capacitación de usuarios; Mantenimiento preventivo de base de datos; Atención de reclamos (nivel 2).

Estudios universitarios

- Ingeniero en Sistemas de Información – Universidad Tecnológica Nacional

(finalizado año 2006).

Certificaciones profesionales

- Certified Information Systems Security Professional (CISSP) – ISC2 – Certification Number: 103617.
- Certified ISO/IEC 27001 Auditor - Certificate Number: PECB-ISMSA-100012.

Conocimientos complementarios y cursos de capacitación

- Administración de proyectos: metodología PMI.
- Mejores prácticas y estándares de seguridad informática: ISO/IEC 27001 e ISO/IEC 27002.
- Mejores prácticas y estándares de TI: Information Technology Infrastructure Library (ITIL).
- ISO 27001 ISMS Lead Auditor – CTE Solutions
- Information Security Management System (ISMS) – PwC
- Especialista en Administración de Proyectos (Project Management) – UTN
- Coaching – Telecom Argentina
- Liderazgo – Telecom Argentina
- Negociación y Resolución de conflictos – Telecom Argentina

Idiomas

- Español: Nativo.
- Inglés: Fluido (oral y escrito – First Certificate in English).
- Portugués: Nivel elemental.

Datos personales

- Fecha de nacimiento: 21 de marzo de 1979
- Edad: 37 años
- Nacionalidad: Argentina – Española
- Domicilio particular: Laguna 739 – Ciudad de Buenos Aires
- Estado civil: Soltero
- DNI: 27.225.522