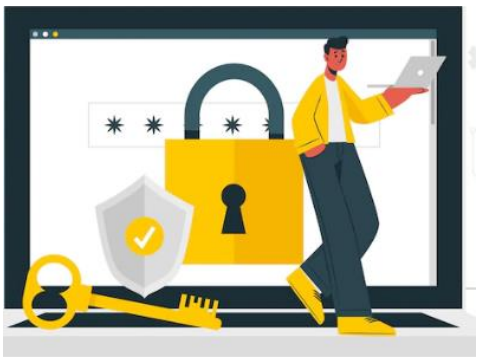


“PROPUESTA DE METODOLOGÍA DE GESTIÓN DE RIESGOS PARA EMPRESA MONOPÓLICA DE SERVICIOS PÚBLICOS”

Trabajo de aplicación de conceptos y técnicas de administración en situación laboral de revista o ambiente real

Venditti Galo Florencia
DNI: 42.500.073
fvendittigalo@gmail.com

Año 2023
Tutor: Marcelo Adrián García

Índice

Resumen

Como resultado de la pandemia la presencia online de la organización objeto de estudio se intensificó, a fin de resolver los requerimientos, consultas y reclamos de sus consumidores. En consecuencia, se percibió un mayor riesgo por exposición de información, de carácter sensible y se evidenció la necesidad de implementar mayores y mejores estrategias de seguridad, sobre todo las relacionadas con gestionar el riesgo asociado con la utilización de los activos de información.

El presente trabajo tiene como objetivo general proponer a una empresa monopólica de servicios públicos una metodología de gestión de riesgos adecuada a sus políticas de Seguridad de la Información (SI), basada en los estándares internacionales ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000 y NIST 800-30. Por cuestiones de confidencialidad, la misma será identificada bajo el nombre de fantasía “SyC”.

Se abordó esta investigación desde un enfoque cualitativo con un diseño investigación - acción. Se llevó a cabo un relevamiento de datos a través de distintos métodos entre ellos: sesión de profundidad, entrevistas, revisión de documentos y datos secundarios.

Finalmente, se elaboró una breve reflexión sobre la importancia de la participación del profesional de Ciencias Económicas en la gestión de riesgos de seguridad de la información.

Palabras claves: gestión – riesgos – seguridad de la información – metodologías

Introducción

El auge del conocimiento, comunicación y tecnología, que se ha presentado en los últimos años, deja en evidencia que la información es uno de los activos potenciales más valiosos que tiene una organización. A su vez, este crecimiento de la tecnología de la información y la comunicación impulsó en gran medida los delitos cibernéticos. Situaciones como el robo de datos, suplantación de identidad, espionaje industrial, sabotaje de sistemas, e incluso delitos internos como accesos no autorizados, errores humanos y mal manejo de recursos, representan un riesgo significativo para la integridad, confidencialidad y disponibilidad de la información. Estos ataques no solo pueden causar daños económicos y reputacionales, sino que también pueden perjudicar la continuidad de las instituciones y poner en peligro la confianza de los clientes y usuarios.

Como consecuencia, la gestión de riesgos tomó un papel fundamental en la Seguridad de la Información para mantener los activos protegidos de posibles amenazas. La misma no solo ayuda a identificar las vulnerabilidades, sino que permite evaluar el nivel de riesgo de estas, para la empresa y minimizar su impacto a un nivel aceptable en caso de concretarse algún incidente.

Invertir en actividades y herramientas que ayuden a gestionar estos riesgos debe ser un proceso iterativo en curso que debe repetirse de manera indefinida, ya que el entorno empresarial se encuentra en constante cambio y diariamente surgen nuevas amenazas y vulnerabilidades.

Contar con un plan de gestión de riesgos, que detalle las medidas correspondientes a aplicar ante cada situación, es de vital importancia. Al ser la información uno de los activos más valiosos de la organización, la gestión del riesgo debe considerarse esencial para mantenerla protegida, brindándole la atención que merece.

En la empresa objeto de estudio, existe un responsable de Seguridad de la Información encargado de investigar, desarrollar, proponer, y mantener las políticas y procedimientos del área. Para implementar las mismas, definió seis pilares básicos: capacitación, gestión de incidentes, gestión de activos, autenticación, necesidad de conocer y gestión de riesgos. Actualmente, los primeros 5 pilares se encuentran implementados y con buen funcionamiento. Sin embargo, la “Gestión de Riesgos” no se ha puesto en práctica. Hace unos años se lo intentó ejecutar de una manera muy precaria y sin éxito.

El propósito de este trabajo es proponer una metodología para la gestión del riesgo, con la finalidad de que la empresa objeto de estudio logre implementarla exitosamente. Para esto, se considera oportuno estudiar los distintos marcos de cumplimiento internacionales relacionados al tema, de tal forma que sirvan como guía para optar por lo que mejor se adapte a la organización. Estos documentos surgen a partir de mejores prácticas y son utilizados como herramientas estratégicas para intentar reducir costos, minimizar errores; así como aumentar la productividad dentro de las organizaciones. La selección de un estándar de carácter

internacional brinda beneficios adicionales, ya que permite posicionarse en un marco comparativo a nivel mundial.

Problema

La empresa “SyC” cuenta con un área de Seguridad de la Información en donde por muchos años se intentó llevar a cabo evaluaciones de riesgo. El inconveniente al que se enfrentaron es que al no existir un área específica que las ejecute, cada gerencia elaboraba una planilla de Excel donde la información quedaba dispersa y difícil de analizar. Además, estas planillas expresaban los riesgos de un momento dado, con planes de acción que muchas veces no se ejecutaban ni se gestionaban.

Si bien la alta dirección manifiesta activamente su apoyo a la gestión de riesgos, al no contar con un sector dedicado de forma exclusiva, se observa que no le otorga la prioridad que realmente requiere.

La empresa, al ser proveedora de servicios públicos, capta, procesa y almacena información sensible de sus clientes. Es por esto que resulta imprescindible implementar la gestión de riesgos en la organización para evitar cualquier incidente y estar preparado en el caso de que ocurra.

Preguntas de Investigación

- ¿Cuál es el estado actual de la empresa bajo estudio en cuanto a la gestión de riesgos de seguridad de la información?
- ¿Cuáles son las herramientas existentes para gestionar el riesgo?
- ¿Cuáles son los estándares internacionales de gestión de riesgo disponibles?
- ¿Cuál es la metodología que más se adecua a la situación de la empresa?

Objetivo General

Proponer una metodología de evaluación y gestión de riesgos adecuada, teniendo en cuenta las características particulares de la organización objeto de estudio y estándares internacionales relacionados.

Objetivos Específicos

- Conocer las características particulares y el estado actual de la gestión de riesgos de la organización objeto de estudio.
- Identificar las distintas herramientas existentes para gestionar el riesgo.
- Reconocer los distintos estándares internacionales de gestión de riesgo.

Marco Teórico

El estándar internacional ISO/IEC 27000:2018 define Seguridad de la Información como "la preservación de la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un enfoque de gestión de riesgos y el establecimiento de controles adecuados". Esta definición parte de la premisa de que la información es el nuevo gran valor y tesoro de la nueva realidad, ya que los malos manejos que se puedan hacer con ella, pueden ser catastróficos, para gobiernos, empresas e incluso para las personas que manejan información sensible en línea.

Según el INCIBE, un activo de información es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

Para poder definir “riesgo” es necesario comprender antes los siguientes conceptos: “probabilidad”, “amenaza”, “vulnerabilidad” e “impacto”. El Instituto Nacional de Ciberseguridad (INCIBE, s.f.) declara que:

- “Probabilidad” es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento. Las bases de cálculo pueden ser datos objetivos o históricos de la organización, estimaciones de expertos, entre otros;
- “Amenaza” es una circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad;
- “Vulnerabilidad” es una situación producida por la falta de controles que, de producirse, afectaría el entorno informático. Facilita la materialización de amenazas;

- “Impacto o consecuencia” es la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad.

Así, el INCIBE (s.f) define “riesgo” como la probabilidad de que una amenaza llegue a concretarse por la existencia de una vulnerabilidad; y “Gestión de Riesgos” como el proceso de toma de decisiones en un ambiente de incertidumbre sobre una acción que puede suceder y sobre las consecuencias que se presentarán, si ésta acción ocurre. Es el conjunto de actividades que tienen como objetivo mantener el riesgo por debajo de un umbral determinado.

A su vez, se puede diferenciar el riesgo operacional y el riesgo de tecnología de la información. Según la norma ISO 27001 el riesgo operacional se refiere a la posibilidad de pérdidas o daños resultantes de la inade-cuada o fallida aplicación de procesos internos, recursos humanos y sistemas o debido a eventos externos. Estos riesgos pueden incluir pérdidas financieras, pérdida de reputación, incumplimiento de regulaciones o leyes aplicables, y disrupción de las operaciones comerciales. Por otro lado, el estándar internacional NIST 800-30 define riesgo de tecnología de la información como la posibilidad de que se produzcan eventos adversos o impactos en la confidencialidad, integridad y disponibilidad de los sistemas de información y los datos, así como en los procesos y funciones comerciales que dependen de ellos.

Un “marco de trabajo” o “marco de cumplimiento”, en el ámbito de la seguridad de la información, se puede definir como "una estructura que establece los principios, políticas, estándares y mejores prácticas para gestionar la Seguridad de la Información en una organización. Proporciona una guía para desarrollar e implementar estrategias y controles de seguridad de la información de manera coherente y efectiva" (Serrano, 2018). Para este trabajo se estudiarán los siguientes:

- NIST 800-30: normas y estándares establecidos por la Agencia de Seguridad de la Información Nacional (NIST) en áreas como la seguridad de la información, la tecnología de la información y la ciberseguridad. Estas normas y estándares son desarrolladas y publicadas por el NIST para ayudar a las organizaciones a proteger la información confidencial y los sistemas contra amenazas externas y garantizar la confidencialidad, integridad y disponibilidad de la información. El cumplimiento del NIST es esencial para garantizar la seguridad de la información de una organización y protegerla contra posibles amenazas cibernéticas.

- ISO 27001: norma internacional emitida por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Esta norma proporciona un marco de referencia para que las organizaciones establezcan, implementen, operen, monitoreen, revisen, mantengan y mejoren de manera continua la seguridad de la información. Su objetivo es ayudar a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información. Se basa en

un enfoque de gestión de riesgos, que implica identificar y evaluar los riesgos de seguridad de la información y establecer controles adecuados para mitigarlos.

- ISO 27002: norma internacional emitida por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) que proporciona directrices y prácticas recomendadas para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI) dentro de una organización. Proporciona un marco de referencia detallado y completo que ayude a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información que manejan. Está diseñada para ser utilizada en conjunto con la norma ISO 27001.

- ISO 27005: norma internacional emitida por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) que establece un marco para la gestión de riesgos de seguridad de la información. Proporciona un enfoque sistemático y estructurado para la evaluación y gestión de los riesgos de seguridad de la información en una organización. Su objetivo es ayudar a las organizaciones a identificar y evaluar los riesgos de seguridad de la información, y a tomar medidas adecuadas para gestionarlos de manera efectiva.

- ISO 31000: norma internacional emitida por la Organización Internacional de Normalización (ISO) que establece los principios y directrices para la gestión del riesgo. Proporciona un marco de referencia para que las organizaciones identifiquen, evalúen y gestionen de manera efectiva los riesgos a los que se enfrentan. Su objetivo es promover una cultura de gestión del riesgo y facilitar la toma de decisiones informadas. La norma es aplicable a todo tipo de organizaciones, tanto del sector público como privado, y se puede adaptar a diferentes contextos y niveles de complejidad.

Marco Metodológico

Se abordará el trabajo desde un enfoque cualitativo con un diseño investigación - acción. Se busca relevar el proceso de Gestión de Riesgos de Seguridad de la Información en la empresa recopilando datos a través de los siguientes métodos:

- Sesión en profundidad: mediante la participación en un seminario, donde se recolectará información para comprender el accionar diario de la empresa.

- Entrevista a expertos: realizada al responsable de seguridad de la información de la empresa para conocer la situación actual de SyC con respecto a la gestión de riesgos.

- Revisión documental: se accederá a la política formal de la empresa y a material adicional sobre los sistemas.
- Datos secundarios: se investigarán posibles alternativas de herramientas para facilitar la gestión de riesgos de la empresa.

Etapas de investigación

1. Estudio bibliográfico;
2. Inmersión en la empresa de estudio;
3. Recolección de los datos a través de las diversas técnicas mencionadas;
4. Revisión y análisis de datos;
5. Relevamiento del proceso de gestión de riesgos;
6. Presentación de conclusiones y de herramientas adecuadas para la empresa.

Recolección y análisis de datos

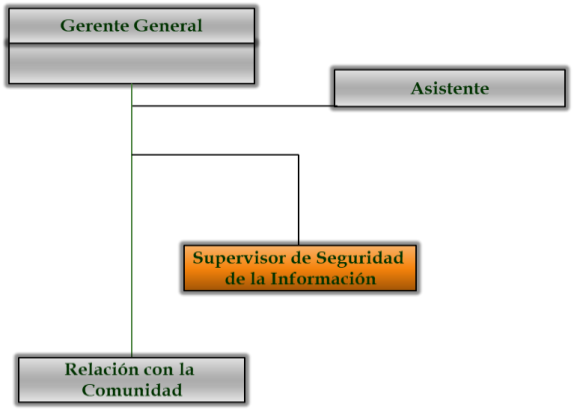
1. Seminario

El día martes 25 de Octubre del 2022, en el marco de la asignatura Seguridad y Control de Sistemas Informáticos, se participó en el seminario “El día a día de la seguridad de la información en una empresa tucumana” dictado por el responsable de la Seguridad de la Información de la empresa bajo estudio. Del mismo se pudo recabar la siguiente información:

Existe en la empresa un responsable de seguridad de la información que depende directamente de la gerencia general. El área sólo está integrada por el responsable de seguridad de la información, debido a que la empresa terceriza todos los servicios informáticos. Este responsable está encargado de investigar, desarrollar, proponer y mantener las políticas y procedimientos de Seguridad de la Información, como así también de participar activamente de la gestión de incidentes y gestión de cambios de los activos de información a fin de maximizar la generación de valor, aportando a la gestión de riesgos, control y gobierno corporativo.

A continuación, se presenta un organigrama que refleja dicha relación.

Imagen 1: Organigrama



Fuente: Presentación del disertante.

Se pudo identificar las políticas de seguridad de información que se implementaron en la empresa, basándose en el objeto principal de proteger y garantizar los aspectos de confidencialidad, integridad y disponibilidad de la información de acuerdo a los requerimientos del negocio.

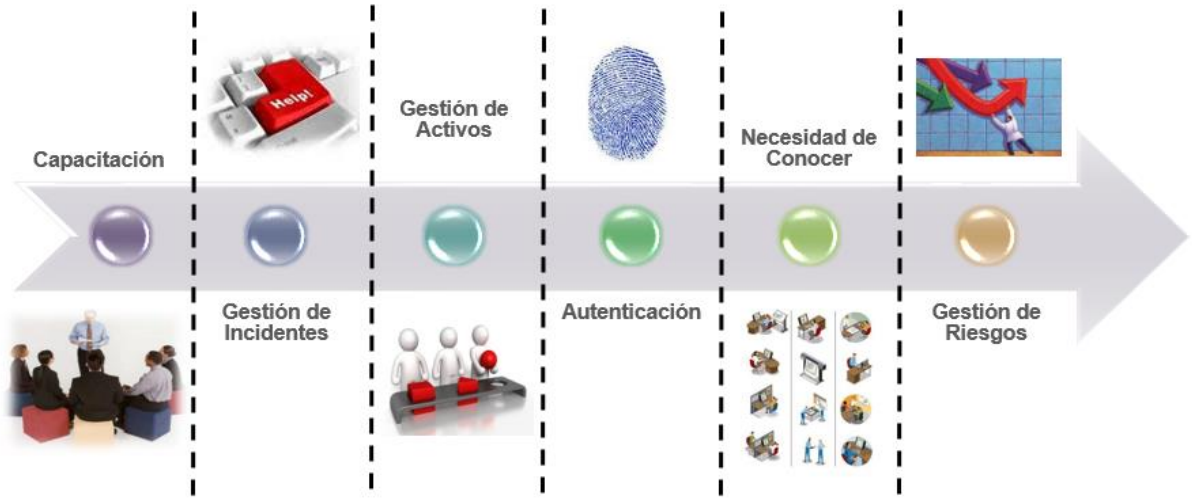
Para poder desarrollar estas políticas de seguridad es necesaria la formación de un equipo de trabajo con la participación activa de propietarios y custodios a fin de implementar los pilares básicos. Para ello, existe un comité de seguridad encargado de facilitar la toma de decisiones no incluidas dentro de la política de la empresa, conformado por la alta dirección de la empresa.

Los aspectos considerados para la política de seguridad son:

- El manejo consistente de la información
- Acceso a información en base a la necesidad
- Autenticación de usuarios
- Uso personal de los recursos de la empresa
- Actividades no permitidas
- Informes obligatorios
- Derechos sobre el material Desarrollado

Para la implementación se siguió un curso de acción basado en los siguientes pilares:

Imagen 2: pilares de la seguridad de la información de la empresa



Fuente: Presentación del disertante.

El primer pilar resulta crucial para sostener a los demás. La capacitación inicial debe ser hacia supervisores, jefes y gerentes. La misma se logra a través de campañas, que inician con la realización de Métricas para saber la situación actual en la que se encuentra la empresa. A partir de estas se ponen en marcha las capacitaciones necesarias que luego serán comparadas con las métricas para un posterior análisis de resultados. Con esto se puede implementar refuerzos de campaña sabiendo los puntos débiles que deben reforzar y así comenzar de nuevo el ciclo.

Con respecto a la gestión de incidentes, la empresa realiza reuniones mensuales para evaluar los posibles riesgos y buscar la mejor manera de abordarlos. Por cada incidente producido se realiza un informe detallando el impacto generado en el negocio.

Sobre el pilar de gestión de activos, se construye un inventario de activos que se va actualizando a medida que se aumentan o disminuyen estos activos de información. Esta base cumple con la Ley de Protección de Datos Personales (Ley 25326).

La empresa requiere que cada empleado y tercero que accede al sistema tenga un único identificador y sea responsable por el uso del mismo. Las contraseñas de los usuarios deben ser de uso personal e intransferible, por lo que la empresa cuenta con una política de autenticación de contraseñas fuertes y con un doble factor de autenticación.

El acceso a información de la empresa se proporciona de acuerdo al pilar Necesidad de Conocer. El mismo hace referencia a que la información debe ser divulgada únicamente a las personas que tengan una necesidad legítima sobre esta. Es por esto que la empresa se centró en redefinir los roles de acceso y formalizar una gestión corporativa de los permisos de acceso a información.

El pilar de la Gestión de Riesgos todavía no se encuentra implementado en la empresa. Se está buscando un sistema integrado a la gestión de cambios, gestión de incidentes y basándose en la gestión de activos.

El presente trabajo se enfocará en el estudio del sexto pilar de seguridad de la información en la empresa: la gestión de riesgos.

2. Entrevista

Se tuvo la oportunidad de entrevistar al responsable de seguridad de la información, a través de una entrevista no estructurada con preguntas abiertas, dando lugar al diálogo continuo e inmersión en nuevos temas relacionados. El principal objetivo de la misma fue profundizar en el proceso de gestión de riesgos de la empresa.

Se recolectó la siguiente información:

- La empresa no está obligada a cumplir con ninguna normativa referida a SI.
- Si bien se considera a la gestión de riesgos como uno de los pilares básicos de SI, al no contar con un área de gestión de riesgos en la empresa queda en evidencia que no se le está dando la importancia requerida. Sin embargo, el concepto de gestión de riesgos está en todas las áreas y se trabaja en eso, pero no existe un sistema o herramienta que lo acompañe.
- La información es el activo más importante de la empresa por lo que cualquier incidente puede causar daños tanto económicos como de imagen. Toda la información confidencial que se divulgue puede causar un perjuicio. Es por esto que se le da mucha importancia a su clasificación.
- Las nuevas iniciativas y proyectos involucran al área de SI desde hace un tiempo, desde el inicio de los mismos.
- Existe un inventario de los activos informáticos, dentro de estos están no solo los sistemas sino también las bases de datos.
- Existe un procedimiento donde están definidos los propietarios y custodios de la información.
- Se está evaluando una herramienta para la gestión de los activos informáticos.

- Constantemente se analizan vulnerabilidades y se actualizan los estándares de información con regularidad, de acuerdo con las nuevas vulnerabilidades que vayan apareciendo. Esto no lo realiza la empresa si no que es un servicio tercerizado.
- Se ejecutan herramientas de escaneo automatizado de vulnerabilidades una vez al año. Para esto se contrata una consultora que emite un informe con observaciones, las cuales se trabajan y resuelven hasta el próximo año cuando se vuelve a realizar el escaneo. Esta consultora no es siempre la misma, se va alternando todos los años para que no siempre vean lo mismo.
- Está definido quiénes son los propietarios de la información y toda la información en la nube se gestiona a través de permisos de accesos, los cuales son otorgados por el responsable de seguridad de la información.
- Todavía no se cuenta con un plan de recuperación ante desastres, pero se está trabajando en eso. Existen instructivos y procedimientos sobre recuperación de activos específicos, pero no uno general.
- Se realizan regularmente copias de respaldo de todos los datos del sistema de manera automatizada. Es un proceso maduro dentro de la organización. Se hacen *backups*, a disco y a cinta. Hay sistemas que tienen alta disponibilidad lo que significa que constantemente se están replicando los datos en tiempo real en otro espacio para que ante cualquier problema directamente se pase a este disco espejo y se continúe trabajando desde ahí.
- La frecuencia de estos respaldos ha sido acordada y definida para cada sistema con los propietarios de los procesos. De todas formas, se realiza diariamente el *backup* de todos los sistemas, el incremental todos los días y una vez a la semana el full backup.
- Se realizan pruebas de restauración con el objetivo de probar la integridad de los *backups*.
- Existen copias de resguardo *offsite,* que constan de cajas de seguridad ignífugas.
- El comité de seguridad de la información, definió una política de respuesta a incidentes de seguridad en el año 2012. La misma explicita que el análisis de los incidentes de seguridad debe realizarse con frecuencia mensual y debe existir un registro de todos los incidentes en un sistema.
- Existe un procedimiento de respuestas a incidentes por sistema. El mismo no solo está definido si no que se encuentra probado.
- Todavía no se han asignado cargos y responsabilidades para la respuesta a incidentes de ciberseguridad, pero en eso se está trabajando actualmente.

3. Revisión documental

Se accedió a los siguientes documentos de SyC:

a. Política General de Seguridad de la Información

El alcance de la política general de SI de “SyC” involucra la participación y soporte de todos los empleados y terceros que se vinculen o tengan acceso de algún modo a la información de la empresa.

En esta se especifica lo siguiente: “La empresa considera su información como un activo clave que debe proteger, evitando que la misma se vea afectada en su confidencialidad, integridad y/o disponibilidad. La empresa actualmente trabaja para preservarla, y tiene como objetivo organizar los esfuerzos en materia de seguridad de la información, de manera que se realicen acciones que lleven a los activos de información a un nivel aceptable de riesgo”.

b. Inventario y dependencia de activos

SyC posee un inventario de activos, en una hoja de cálculo, en el cual se detalla cada activo con sus características y la dependencia entre los mismos, indicando propietario y custodio.

c. Instructivo de trabajo: proceso de gestión de SI - especificación de propietarios de activos de información

Existe un instructivo cuya finalidad es definir e identificar a los propietarios de los activos de información de la empresa, encargados de autorizar los permisos de accesos a los mismos. En este se detalla la metodología de trabajo que se siguió para la determinación de los dueños de la información.

En el detalle de los propietarios de los activos de información se especifican los siguientes ítems: propietario general, propietario operativo, tipo de activo (de información, de servicio o de aplicación) y el activo analizado.

d. Proceso de gestión de incidentes de SI

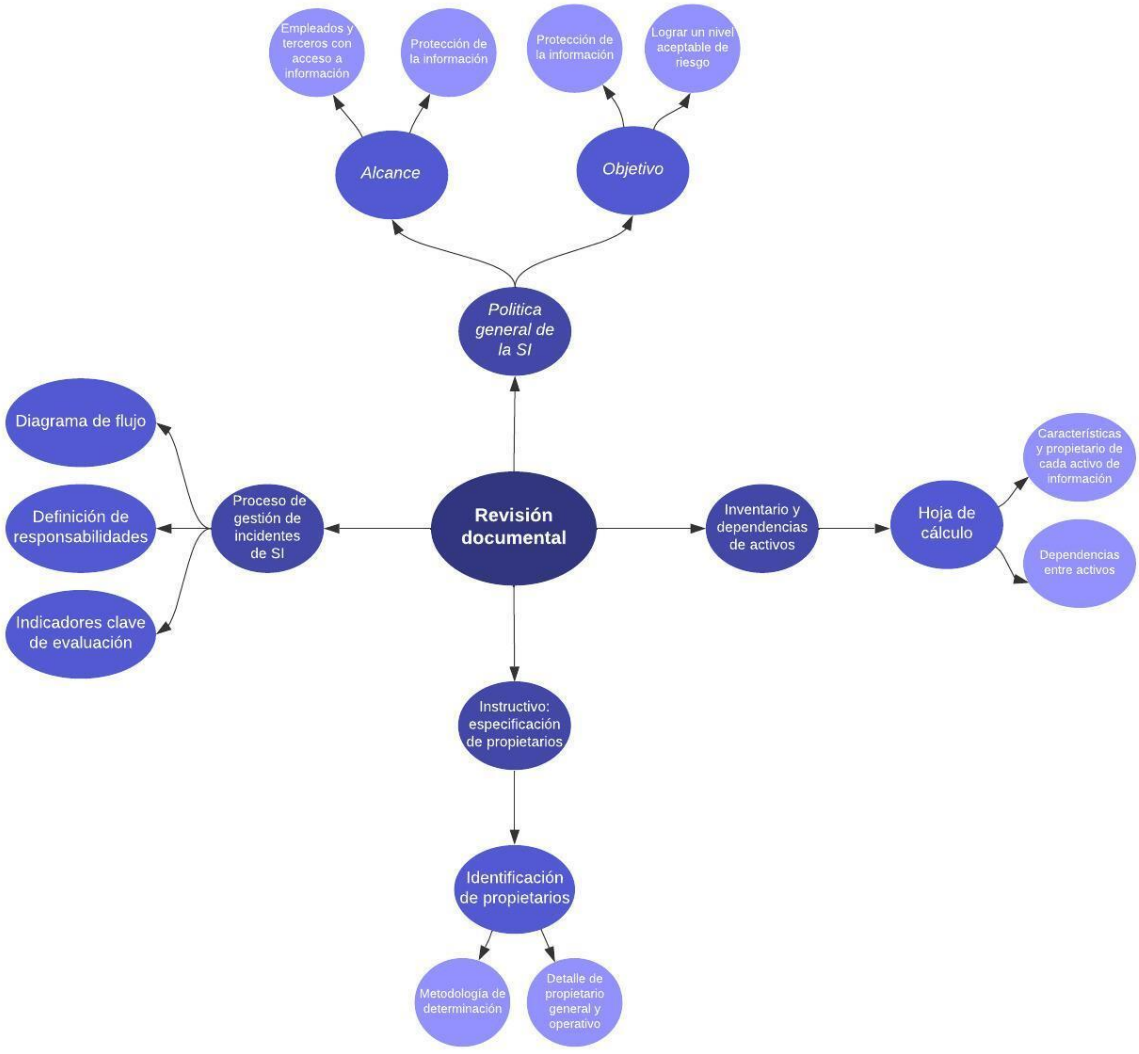
La empresa posee un documento formal con un diagrama de flujo y detalle del procedimiento a seguir para gestionar cualquier incidente de seguridad de la información que se originen, transcurran o impacten en la empresa. El mismo está basado en ISO 27035 y se enfoca en activos digitales.

Asimismo, se encuentran definidas las responsabilidades y los indicadores clave para evaluar el proceso.

4. Mapa conceptual

A partir de la revisión documental se elaboró el siguiente mapa conceptual para organizar y comprender mejor los documentos:

Imagen 3: mapa conceptual sobre documentos de la empresa



Fuente: elaboración propia a través de LucidChart

Propuesta metodológica

Habiendo realizado un análisis de los datos recolectados y estudiados los estándares internacionales ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000 y NIST 800-30 se propone a la empresa lo siguiente:

- Crear un sector específico para gestión de riesgos, dependiente del área Seguridad de la Información y articulado con “Auditoría Interna”, de forma que se logre promover una gestión más eficiente de la seguridad de la información, garantizando la identificación temprana de posibles vulnerabilidades y el cumplimiento de las políticas y estándares establecidos.

- Designar un especialista en el tema, encargado de llevar a cabo el proceso periódicamente.

- Asegurar el apoyo de la alta dirección, cumpliendo los ítems detallados en la sección 5.1 de la norma ISO 27001. Los mismos se basan en liderazgo y compromiso, buscan alinear las políticas de SI con la estrategia de la empresa y asegurar que el sistema de gestión de riesgos cumpla con sus objetivos y promueva la mejora continua.

- Implementar herramientas que faciliten el proceso. Un sistema automatizado proporcionará mayor eficiencia, precisión y consistencia en el proceso. La recopilación y análisis datos se hará de manera más rápida y precisa, permitiendo una mejor comprensión de los riesgos potenciales y una toma de decisiones más informada. Además, ayudará a establecer criterios y métricas claras, asegurando una evaluación uniforme y objetiva en toda la organización, logrando identificar y priorizar los riesgos más críticos y una asignación más eficiente de recursos para su mitigación. Algunas recomendaciones son:

    - ISO TOOLS: es un software diseñado para facilitar la implementación y gestión de los estándares y normas de la serie ISO, incluyendo ISO 27001 y ISO 31000 (Gestión de Riesgos). Ofrece diversas funcionalidades, entre ellas: documentación y plantillas de referencia para ayudar en la creación de políticas, procedimientos y otros documentos necesarios, seguimiento y cumplimiento de los requisitos establecidos por los estándares ISO y facilitación de la gestión de los controles de seguridad y riesgos, automatización de procesos relacionados con la gestión de riesgos y seguridad de la información, evaluación y auditoría, elaboración de informes y análisis para monitorear el desempeño de los sistemas de gestión.

    - Nosis Compliance: es una herramienta de gestión de riesgos y cumplimiento normativo. Ofrece diversas funcionalidades que incluyen: verificación de identidad a través de la validación de documentos de identificación, evaluación de riesgos mediante la realización de análisis de riesgos, reportes de cumplimiento que

documentan las medidas tomadas por la organización para mitigar los riesgos y cumplir con las regulaciones, alertas y notificaciones en tiempo real sobre cambios en la situación de clientes o proveedores permitiendo una respuesta rápida y oportuna ante posibles riesgos emergentes.

- Inteligencia Artificial (IA): la aplicación de la IA puede desempeñar un papel importante en el proceso de gestión de riesgos. Estas herramientas pueden ser de gran utilidad para: análisis de grandes cantidades de datos e identificación de patrones y tendencias, así como evaluación de la probabilidad e impacto de los riesgos; detección de amenazas en tiempo real, mediante un análisis de comportamientos y monitoreo continuo permitiendo una respuesta más rápida y precisa a las amenazas; automatización de tareas, como recopilación y análisis de datos; generación de informes y actualización de registros; análisis de vulnerabilidades y evaluación de impacto utilizando técnicas de escaneo y análisis automatizados, identificando áreas de riesgo y sugiriendo medidas de mitigación adecuadas; modelado y simulación de escenarios de riesgo, permitiendo evaluar los posibles impactos y resultados de diferentes decisiones de gestión de riesgos, lo que ayuda a tomar decisiones más informadas y prepararse para diferentes situaciones.

  Es importante tener en cuenta que, si bien la IA puede ser una herramienta poderosa en la gestión de riesgos de TI, no reemplaza la experiencia y el juicio humano. La colaboración entre profesionales de riesgos y expertos en IA es fundamental para aprovechar al máximo el potencial de esta herramienta y tomar decisiones basadas en un análisis combinado de datos y conocimientos.

  A continuación, se presentan algunas sugerencias de IA:

  1. Chat GPT: puede aportar en: generación de ideas y evaluación de riesgos; integración de gran cantidad de datos, convirtiéndolos en información para tomar buenas decisiones, investigación y conocimiento sobre las mejores prácticas, estándares de seguridad, marcos de trabajo y casos de estudio relevantes; análisis de grandes conjuntos de datos y detección de patrones; apoyo en la toma de decisiones, evaluando diferentes opciones y escenarios; generación de contenido educativo, explicando conceptos clave y ofreciendo consejos.

  2. Sense analytics: es una herramienta de detección de amenazas en tiempo real. Detecta riesgos y comportamientos anormales permitiendo dar respuesta inmediata a incidentes.

  3. Watson for Cybersecurity: ayuda en la detección y respuesta de amenazas cibernéticas. La herramienta utiliza técnicas de aprendizaje automático y análisis de datos para analizar

grandes volúmenes de información de seguridad, como registros de eventos, informes de incidentes y documentos de seguridad.

4. DarkTrace Enterprise Immune System: es una plataforma de ciberseguridad basada en tecnologías de IA y aprendizaje automático. Ayuda en la detección y prevención en tiempo real de amenazas cibernéticas, desde ataques internos y externos hasta amenazas emergentes y desconocidas. Detecta phishing, worms, robo de datos, entre otros. Analiza continuamente los patrones de tráfico y actividad en busca de desviaciones y señales de posibles amenazas. Además, proporciona información y análisis en tiempo real para ayudar a los equipos de seguridad a tomar medidas rápidas y efectivas ante posibles incidentes.

5. Cylance Protect: es una solución de seguridad cibernética que utiliza IA y aprendizaje automático para proteger los sistemas contra amenazas de malware y otras formas de ataques cibernéticos. Utiliza algoritmos avanzados para analizar el comportamiento y las características de los archivos y programas en tiempo real, identificando y bloqueando malware conocido y desconocido.

➢ Utilizar un enfoque cualitativo como metodología de gestión de riesgos: al ser una empresa grande con muchos procesos de negocios y activos de información, utilizar un enfoque cuantitativo podría ser un proceso muy lento, tedioso y costoso. El enfoque cualitativo nos ayudará a implementar el proceso en un plazo considerable. El mismo utiliza una escala de atributos calificadores para describir la magnitud de las posibles consecuencias (baja, media y alta) y la probabilidad de que esas consecuencias ocurran. Una gran ventaja es su facilidad de comprensión, sin embargo, está sujeto a la dependencia de la elección subjetiva de la escala.

➢ Elaborar una matriz RACI para definir y clarificar los roles y responsabilidades de las personas involucradas en el proceso. RACI es un acrónimo de los roles clave que se asignan en la matriz:

- Responsable: quien asume la responsabilidad de la tarea;
- *Accountable* (responsable último): quien aprueba la tarea realizada;
- *Consulted* (consultado): experto en el tema, encargado de asesorar.
- *Informed* (informado): involucra a todo aquel que deba ser informado sobre los avances y resultados del proyecto.

Sus principales beneficios son que minimiza la posibilidad de malentendidos y evita la falta de claridad en los roles, además de fomentar una mayor colaboración y comunicación efectiva.

Recomendaciones para su implementación:

- Identificar las tareas y actividades clave relacionadas al proceso;
- Identificar a las personas involucradas en cada tarea o actividad.
- Asignar los roles RACI correspondientes.
- Comunicar y compartir la matriz RACI con todas las partes interesadas.

Fases metodológicas a seguir

1. **Análisis del contexto:** tanto externo como interno. Implica establecer los criterios básicos necesarios para la gestión de riesgos de seguridad de la información, definiendo el alcance y los límites, y establecer una organización apropiada que opere la gestión de riesgos de seguridad de la información.

2. **Inventario de activos y dependencias**

   ➢ Identificar los procesos de negocio de la empresa y definir cuáles de estos son críticos para el funcionamiento de la empresa.

   ➢ Identificar los activos de información sujetos a cada proceso crítico del negocio.

   ➢ Identificar el propietario de cada activo de información encargado de proporcionar responsabilidad y rendición de cuentas por el mismo.

   ➢ Clasificar estos activos según su tipo (información, servicio, aplicación).

   ➢ Identificar la dependencia de los activos, es decir, la relación existente entre los mismos, donde el funcionamiento y disponibilidad de uno, o varios, depende de la disponibilidad y correcto funcionamiento de otros.

La empresa ya posee esta primera fase implementada en una hoja de cálculo. Sin embargo, se deben realizar actualizaciones de forma frecuente para incorporar nuevos activos y dar de baja aquellos obsoletos o dañados.

3. Valuación y clasificación

➢ Valuación estratégica de procesos:

Al ser una empresa grande, con muchos procesos de negocio, se recomienda realizar una valoración de los mismos para lograr identificar los procesos críticos y enfocar la gestión de riesgos en estos. La valoración estratégica nos ayudará también a mejorar la eficiencia, identificar cuellos de botella y mejorar la calidad de la gestión.

Se sugiere utilizar un enfoque cualitativo mediante el método de distribución de 100 puntos. El mismo permite a los evaluadores asignar una puntuación subjetiva a cada proceso de negocio en función de su importancia para la organización. La suma total de todas las puntuaciones asignadas a cada proceso debe ser igual a 100. Se recomienda este método por su sencillez y rapidez.

➢ Clasificación de los activos:

Una vez identificados los procesos críticos de la empresa, nos centraremos en clasificar los activos de información relacionados a los mismos.

Cada activo será clasificado según su dimensión en:

- confidencialidad: propiedad de la información que garantiza que está accesible únicamente a personal autorizado a acceder a ella.
- integridad: propiedad de la información que garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.
- disponibilidad: propiedad de la información que garantiza su accesibilidad y utilización por los usuarios o procesos autorizados cuando éstos lo requieran.

Se recomienda fijar los siguientes parámetros de clasificación de activos:

Tabla 1: parámetros para clasificación de activos según su dimensión

Nivel / Componente	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**
BAJO	La información es pública y no requiere protección especial.	La información no es crítica y no se requiere una alta integridad.	La información no es crítica y la disponibilidad no es una preocupación importante.
MEDIO	La información es sensible y debe ser protegida contra accesos no autorizados.	La información es crítica y requiere una alta integridad para asegurar su precisión y consistencia.	La información es crítica y requiere una alta disponibilidad para asegurar su accesibilidad y continuidad.
ALTO	La información es altamente sensible y confidencial, y su divulgación podría tener un impacto significativo en la organización.	La información es altamente crítica y requiere una integridad máxima para garantizar su validez y exactitud.	La información es altamente crítica y requiere una disponibilidad máxima para garantizar su accesibilidad y continuidad.

Fuente: inteligencia artificial.

Ya determinado el nivel de cada componente de los activos de información se debe calcular el nivel de criticidad de los mismos. Para esto se sugieren los siguientes parámetros:

- Si el activo está clasificado como "alto" en los tres aspectos su nivel de criticidad será "muy alto".
- Si el activo está clasificado como "alto" en al menos dos de los tres aspectos, su nivel de criticidad será "alto".
- Si el activo está clasificado como "medio" en al menos dos de los tres aspectos, su nivel de criticidad será "medio".
- Si el activo está clasificado como "bajo" en todos los aspectos, su nivel de criticidad será "bajo".

Para establecer los parámetros anteriores se utilizó la inteligencia artificial, obteniendo resultados muy prácticos y sencillos de aplicar por lo que se recomienda su uso.

4. Análisis de riesgos:

➢ Identificación de las amenazas:

Una vez identificados los activos críticos, el siguiente paso es identificar las amenazas que pueden afectarlos, tanto internas (ingeniería social, robo, sabotaje, fraude, entre otras) como externas (malware, spoofing y sniffing, botnet, inyección SQL, phishing, catástrofes, entre otras).

Se recomienda el uso de la tabla suministrada en el anexo C del estándar internacional ISO 27005. La misma clasifica las amenazas existentes según su fuente.

➢ Evaluación de vulnerabilidades:

Implica evaluar la capacidad de los controles existentes para mitigar las amenazas y determinar si se necesitan controles adicionales. La empresa implementa actualmente este paso, lo realiza una vez al año mediante la contratación de servicios de terceros.

Se recomienda el uso de la tabla suministrada en el anexo D del estándar internacional ISO 27005. La misma clasifica las vulnerabilidades existentes según su tipo y relación con las distintas amenazas.

➢ Determinación del impacto:

La materialización de un riesgo puede producir daños en la imagen de la empresa (como pérdida de prestigio o disminución de la confianza de los clientes), en el negocio (afectando la operatividad de la empresa, como la interrupción de procesos críticos o la pérdida de productividad y esto a su vez la rentabilidad), en los activos (afectando confidencialidad, integridad y disponibilidad) y en compliance (incumplimiento de normas de protección de datos personales o de seguridad de la información).

Se pueden establecer los siguientes parámetros para calcular el nivel de impacto de un riesgo materializado:

Tabla 2: parámetros para determinar impacto de un riesgo materializado

Nivel/ Impacto	IMAGEN	NEGOCIO	ACTIVOS	COMPLIANCE
BAJO	No afecta la imagen de la organización o solo tiene una repercusión a nivel local o interno.	No afecta significativamente la operatividad de la organización.	No afecta significativamente los activos de la empresa, los daños resultantes son menores, fácilmente manejables y/o reemplazables.	El incumplimiento de las normativas aplicables no tiene consecuencias graves para la organización.
MEDIO	Afecta la imagen de la organización a nivel regional o sectorial.	Afecta parcialmente la operatividad de la organización o tiene una repercusión a nivel local o interno.	Produce daños a los activos de la empresa, pero los mismos son manejables. Podrían requerir cierto esfuerzo de reparación o reemplazo pero no representan una amenaza existencial.	El incumplimiento de las normativas aplicables puede tener consecuencias legales y económicas para la organización.
ALTO	Afecta gravemente la imagen de la organización a nivel nacional o internacional.	Afecta gravemente la operatividad de la organización a nivel regional, nacional o internacional.	Afecta gravemente a los activos de la empresa, con un impacto financiero y operativo importante. Los daños podrían poner en peligro la continuidad de la empresa o su capacidad para cumplir con sus objetivos estratégicos.	El incumplimiento de las normativas aplicables puede tener graves consecuencias legales y económicas para la organización, incluyendo sanciones, multas o incluso la pérdida de licencias o permisos necesarios para operar.

Fuente: Inteligencia Artificial

➢ Estimación de la probabilidad:

La probabilidad de ocurrencia de un evento puede ser clasificada en:

- Baja: probabilidad de ocurrencia del evento muy baja o casi nula.
- Media: probabilidad de ocurrencia del evento moderada o solo ocurre ante ciertas circunstancias o condiciones.
- Alta: probabilidad de ocurrencia del evento alta y puede suceder en cualquier momento o en la mayoría de las circunstancias o condiciones.

➢ Cálculo del riesgo:

El nivel de riesgo es una estimación de lo que puede ocurrir y se calcula como el producto del impacto (la consecuencia en el negocio), asociado a una amenaza, por la probabilidad de la misma.

En la siguiente tabla se ilustra el cálculo:

Tabla 3: matriz de riesgo

		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD	BAJA	Muy bajo	Bajo	Medio
	MEDIA	Bajo	Medio	Alto
	ALTA	Medio	Alto	Muy alto

Fuente: elaboración propia

➢ Diagnóstico de la situación de la empresa:

Una vez calculado el riesgo, podemos realizar un informe para presentar a la alta dirección del diagnóstico de la situación de la empresa para determinar cuáles son los riesgos en los que debemos centrar nuestros mayores esfuerzos.

En este informe se recomienda incluir:

- Cálculo del riesgo general: valor promedio del riesgo general de mis activos.
- Cálculo del riesgo por dimensión: confidencialidad, integridad y disponibilidad.

- Ranking de activos: de más riesgoso a menos riesgoso. Esto ayudará a la alta dirección a definir el umbral de riesgos aceptables.
- Ranking de vulnerabilidades
- Ranking de amenazas

Es importante destacar que el proceso de análisis de riesgos debe ser continuo, ya que las vulnerabilidades y amenazas cambian con el tiempo. Por lo que se recomienda realizar evaluaciones periódicas y mantener un plan de gestión de riesgos actualizado.

5. Tratamiento de riesgos

En primer lugar, la alta dirección debe definir el apetito al riesgo de la empresa, es decir la medida en la cual la organización está dispuesta a aceptar la posibilidad de enfrentar pérdidas o incertidumbre en busca de alcanzar sus objetivos. El mismo debe definirse en función de sus objetivos estratégicos, tolerancia al riesgo y capacidad para manejarlo. Una vez definido se deben establecer las acciones que se pueden llevar a cabo para tratar los riesgos. Se recomiendan las siguientes:

- Evitar: Identificar riesgos potenciales y tomar medidas para evitar completamente su ocurrencia. Esto puede implicar evitar ciertas actividades o decisiones que presenten un riesgo inaceptable.
- Transferir: Transferir el riesgo a otra parte, generalmente mediante la contratación de seguros o acuerdos contractuales. Esto permite que otra entidad asuma la responsabilidad de manejar los riesgos y las consecuencias asociadas.
- Mitigar: Implementar medidas para reducir la probabilidad o el impacto de los riesgos. Esto puede incluir la implementación de controles de seguridad, mejores prácticas, sistemas de protección o protocolos de emergencia.
- Aceptar: Reconocer que un riesgo existe, pero decidir no tomar medidas adicionales para tratarlo. Esto puede ser adecuado cuando el costo de gestionar el riesgo es superior a los beneficios esperados o cuando el riesgo es considerado tolerable.
- Compartir: Compartir el riesgo con otras partes interesadas a través de alianzas estratégicas, colaboración o acuerdos de participación. Esto puede ayudar a distribuir la carga y los recursos necesarios para manejar los riesgos.

La selección de acciones específicas dependerá de la naturaleza del riesgo, los recursos disponibles, las políticas y la cultura organizativa.

Es importante destacar que el proceso de análisis de riesgos debe ser continuo, ya que los riesgos y amenazas pueden cambiar con el tiempo. Por lo tanto, es recomendable realizar evaluaciones periódicas y mantener un plan de gestión de riesgos actualizado.

➢ Desarrollo de medidas de control:

Finalmente, se deben desarrollar medidas de control para mitigar los riesgos identificados. Las mismas pueden clasificarse según su objetivo y función en:

- Preventivos: diseñadas para reducir la probabilidad de que ocurran eventos o incidentes no deseados. Algunos ejemplos son: políticas y procedimientos de SI, controles de acceso físico y lógico, capacitación y concientización al personal, implementación de medidas de seguridad de red (firewalls y sistemas de detección de intrusos).

- Correctivas: se implementan después de que ha ocurrido un incidente de seguridad para mitigar los daños y restaurar la seguridad de la información. Algunos ejemplos son: procedimientos de respuesta a incidentes, restauración de sistemas y datos desde copias de respaldo, investigación forense y análisis de incidentes.

- Detectivas: se utilizan para detectar eventos o incidentes de seguridad de la información en etapas tempranas, permitiendo una respuesta rápida y oportuna. Algunos ejemplos son: sistemas de monitoreo y detección de intrusiones, registros de eventos de seguridad, análisis de registros y monitoreo de actividad sospechosa, sistemas de alerta temprana y notificación de incidentes.

- Disuasivas: están destinadas a desalentar posibles amenazas o ataques de seguridad. Algunos ejemplos son: señalización de seguridad y advertencias, implementación de medidas de seguridad visibles (cámaras de vigilancia), sistemas de autenticación y acceso robustos.

- de Recuperación: se enfocan en la recuperación rápida y efectiva de los sistemas y datos después de un incidente de seguridad. Algunos son: planes de continuidad del negocio y de recuperación ante desastres, copias de respaldo regulares, procedimientos de restauración y recuperación de datos.

- Compensatorias: se utilizan para contrarrestar las deficiencias en otros controles o mitigar los riesgos que no pueden eliminarse por completo. Algunos ejemplos son: supervisión y revisión independiente de los controles existentes, auditorías internas y externas de SI.

Las opciones para el tratamiento del riesgo no son mutuamente excluyentes. La organización puede beneficiarse de una combinación de opciones, como reducir

la probabilidad de riesgos, reducir sus consecuencias y compartir o retener cualquier riesgo residual.

A partir de estas, se debe definir un plan de tratamiento que identifique el orden de prioridad en el que se deben implementar las distintas acciones y sus plazos. Las prioridades pueden establecerse según la clasificación de los riesgos y la relación costo-beneficio.

Es esencial comprender que la eficacia del tratamiento del riesgo dependerá de los resultados obtenidos del análisis.

Conclusiones

Poner en práctica el proceso de gestión de riesgos es fundamental para la empresa a fin de garantizar la continuidad operativa, dado el tipo de servicio que brinda y la información que maneja.

La implementación de una metodología adecuada a las políticas de seguridad de la información de SyC y basada en estándares internacionales, ayudará a tomar decisiones justificadas en términos del negocio y servirá como control sobre actividades de seguridad y riesgo operacionales y de TI. La misma proporciona un marco sólido y reconocido para abordar los diversos riesgos.

Implementar este proceso es un proyecto de gran visibilidad que involucra activamente a todo el negocio. Permite cumplir con los objetivos de seguridad de la información, contribuye a concientizar sobre la importancia de esta materia y proporciona informes y conclusiones ejecutivas que respaldan la toma de decisiones.

Es por esto que resulta crucial contar con el apoyo de la alta dirección para el éxito de la implementación de la metodología de gestión de riesgos. La participación activa y el compromiso de la alta dirección son fundamentales para establecer una cultura organizacional que valore y promueva la gestión de riesgos en todos los niveles de la empresa. Esto implica capacitar y concientizar a los empleados sobre la importancia y proporcionarles las herramientas necesarias para identificar, evaluar y mitigar los riesgos de seguridad de la información.

Se espera también, que los resultados obtenidos puedan ser utilizados como base para fortalecer los sistemas de gestión de riesgos en otras empresas del sector.

El rol del profesional de Ciencias Económicas en la Gestión de Riesgos de Información

La participación de profesionales de Ciencias Económicas en la gestión de riesgos de seguridad de la información se está volviendo cada vez más esencial. La formación de los mismos en áreas como contabilidad, finanzas y administración ayudan a analizar y comprender los diversos factores que surgen a una organización. Su experiencia en el manejo de datos financieros, la identificación de oportunidades y amenazas económicas, y la elaboración de estrategias financieras sólidas, lo posiciona como un agente clave en la gestión de riesgos.

Es importante destacar que la seguridad de la información es un tema que cada vez cobra mayor relevancia debido a la creciente digitalización de los negocios y la necesidad de proteger los datos de los clientes y la empresa misma. Por lo tanto, contar con profesionales de distintas áreas trabajando en conjunto para abordar este desafío puede ser la clave para lograr una gestión efectiva de los riesgos de seguridad de la información y proteger el valor de la organización.

La inclusión de esta temática en el plan de estudio de las carreras de Ciencias Económicas refuerza la formación integral, brindando una perspectiva más amplia y actualizada sobre los desafíos tecnológicos y la importancia de la protección de la información en el ámbito empresarial. Esta formación complementaria les permite, a los estudiantes, ser profesionales más preparados y competitivos en el mercado laboral, capaces de comprender y enfrentar los riesgos cibernéticos a los que se enfrentan las organizaciones en la actualidad.

Bibliografía

Banco Central de la República Argentina. (2023). *Circular A7724: Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información.* Buenos Aires, Argentina: Misto Macias, M. I. & Bossio M.D.

Equipo de contenido de Safety Culture. (2022). *¿Qué es la gestión de riesgos?* https://safetyculture.com/es/temas/gestion-de-riesgos/

Fiorito, D. (2020). *Gestión de riesgos: como cumplir objetivos en el ámbito personal y empresarial.* Dunken SRL.

Hernández- Sampieri, R. & Mendoza, C. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.* México. Editorial Mc Graw Hill Education.

INCIBE. (2015). *Gestión de Riesgos: Una guía de aproximación para el empresario*. España.

INCIBE. (2021). *Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario.* España.

Instituto Nacional de Estándares y Tecnología [NIST]. (2020). *Guide for Conducting Risk Assessments (NIST SP 800-30).*

Organización Internacional de Normalización [ISO]. (2015). *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos (IRAM-ISO/IEC 27001:2015* Segunda edición).*

Organización Internacional de Normalización [ISO]. (2022). *Tecnología de la información - Técnicas de seguridad - Código de práctica para la gestión de la seguridad de la información (IRAM-ISO/IEC 27002:2022* Tercera edición).*

Organización Internacional de Normalización [ISO]. (2018). *Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de la seguridad de la información (IRAM-ISO/IEC 27005:2018* Tercera edición).*

Organización Internacional de Normalización [ISO]. (2018). *Gestión de riesgos - Principios y directrices (IRAM-ISO/IEC 31000:2018* Segunda edición)*

Serrano, L. (2018). *Fundamentos de Seguridad de la Información*. Ediciones ENI.

Apéndice: preguntas de la entrevista realizada

¿Cómo está organizada el área de SI de la empresa?

¿Existe un comité de seguridad?

¿Cumple o debe cumplir con alguna normativa legal o marco regulatorio?

¿Qué importancia se le da a la gestión de riesgos dentro de la empresa?

Los riesgos inherentes a la información, en caso de materializarse, ¿podrían ocasionar daños o pérdidas económicas, de imagen, legales, u otros?

¿Las nuevas iniciativas y proyectos involucran al área de SI?

¿Se mantiene un inventario de toda la información sensible, almacenada, procesada o transmitida de los sistemas de tecnología de la organización?

¿Se actualizan los estándares de información con regularidad y de acuerdo con las nuevas vulnerabilidades que vayan apareciendo, evitando que estos queden obsoletos?

¿Se ejecutan herramientas de escaneo automatizado de vulnerabilidades?

¿Existen requerimientos de seguridad definidos, una valoración del riesgo y autorización explícita del dueño de la información cuando se utilizan los servicios en la nube?

¿Se cuenta con un plan de recuperación ante desastres?

¿Se realizan regularmente copias de respaldo de todos los datos del sistema de manera automatizada?

¿La frecuencia de estos respaldos ha sido acordada con los dueños de los procesos?

¿Se prueba la integridad de estos datos en forma periódica?

¿Existen copias de resguardo offsite?

¿Implementó la empresa un plan de seguridad y respuestas a incidentes de seguridad?

¿Implementó un procedimiento de respuestas a incidentes por sistema, hacking externo, interno, ransomware?

¿Se han asignado cargos y responsabilidades para la respuesta a incidentes de ciberseguridad?