GESTIÓN DE RIESGOS TECNOLÓGICOS Y SEGURIDAD DE LA INFORMACIÓN

2024

EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE

servicioalcliente@aquaterraesp.gov.co
www.aquaterraesp.gov.co
314 880 1262
604 358 86 13
Carrera 50 N° 42-100 local 209

GESTIÓN DE RIESGOS TECONOLÓGICOS Y SEGURIDAD DE LA INFORMACIÓN

Resumen

En este documento nos muestra una metodología para gestionar riesgos tecnológicos y de seguridad de la información, que como base tiene los estándares ISO (International Organization Standardization) 31000, 27001 y 27005, ya que son las normas que indican que se requiere para la gestión de dichos riesgos, más no el cómo se debe realizar esta gestión. También incluye buenas prácticas y recomendaciones de otros estándares y guías para el manejo de riesgos, seguridad de la información y gestión
La metodología es desarrollada para el riesgo tecnológico, ya que el aumento en el uso de tecnologías de la información genera mayor riesgo, vulnerabilidad y puntos de quiebre en aspectos de seguridad con respecto a la utilización de dichas herramientas, por tanto, es vital presentar una forma de aseguramiento y control sobre la infraestructura (Física), los sistemas de información (Lógico), y las políticas de seguridad (factor humano) desde una visión tecnológica. En segunda instancia se presenta una forma de integración de la metodología a las gestiones de continuidad del negocio, y el desarrollo de estrategias en lo que respecta a procesos de base tecnológica.

1. Introducción

El manejo de las tecnologías de la información (en adelante TI), se ha masificado he intensificado en las organizaciones independiente de la actividad que realice o servicio que preste, se encuentran en constante cambio y evolución adaptándose a las nuevas necesidades del mercado, del medio y de las organizaciones y así mismo dando cabida nuevos retos relacionados con su operación diaria. Debido al fuerte crecimiento las han convertido en blanco de ataques cibernéticos y demás; todos estos riesgos relacionados se intensifican y se transforman y hace necesario crear y adaptar constantemente los métodos y los medios implementados para mantener la seguridad de la información que la organización quiera proteger.

En este punto el uso de metodologías integradas ágiles y el constante desarrollo para gestionar riesgos y en este caso el tecnológico, es muy importante con el fin de minimizar el impacto que pueda llegar a causar un ataque informático de alguna de los pilares de la seguridad (correspondiente a la confidencialidad, Integridad, disponibilidad). En la actualidad el marco que existe para la gestión de riesgos lo conforman los estándares ISO 31000, 27001 e 27005. Dichos estándares nos brindan lineamentos generales, pero se hace necesario una guía mas precisa que pueda ofrecer pautas y una guía de lograr aspectos de seguridad necesarios y requeridos. Este documento adicionalmente hace referencia a la gestión sobre los riesgos globales tecnológicos.

El riesgo tecnológico puede afectar en gran medida las metas y objetivos organizacionales, y ser causa de otro tipo de riegos. Por esto el daño, suplantación, alteración o falla relacionada con el manejo de TI puede incurrir en grandes pérdidas para la empresa, pérdidas financieras, multas o incluso acciones de legales, afectación en el servicio, la imagen corporativa, incumplimiento y generar inconvenientes a nivel operativo y estratégico. Este tipo de incidentes son muy comunes y lo más importante es estar lo más preparados posibles para afrontar estas situaciones, un claro ejemplo donde se puede evidenciar todo lo anteriormente mencionado, es en la entidad bancaria Bancolombia que, en el año 2011, presentó una afectación y caída en la red del banco lo que ocasionó una suspensión en sus operaciones normales, ¿Qué trajo como consecuencia? Caos generalizado en sus usuarios por aproximadamente una hora; ¿Qué le implica? Pérdidas financieras y una afectación en la credibilidad de sus clientes (imagen corporativa).

Este tipo de eventos y antecedentes son los que motivan a generar y crear metodologías para el tratamiento de los riegos tecnológicos y que el origen y base son los estándares anteriormente mencionados ISO 31000, 27001 y 27005. Además, se adoptan y se suman recomendaciones y buenas prácticas de otras guías y metodologías como NIST SP, NTC e ITIL. Para ajustar así la metodología a la gestión de continuidad del negocio en lo que relaciona la definición de planes de gestión de incidentes tecnológicos.

2. Metodología para la gestión de riesgo Tecnológico

La metodología propuesta trabaja sobre procesos teniendo en cuenta que facilite el entendimiento sobre el funcionamiento de la organización y la definición e identificación de activos y riesgos asociados de TI. Además, el analizar procesos nos permite tener una visión global de la organización y con ello el apoyo requerido por parte de la gerencia, al evidenciar la necesidad de proteger y gestionar correctamente los procesos críticos de TI en la organización. El trabajo sobre procesos no se debe gestionar como un trabajo aislado puesto que esta visión cuenta con el talento humano quien será el encargado del desarrollo de toda la infraestructura y la ejecución que sea necesaria para su funcionamiento, todo lo anterior enmarcado dentro de los objetivos y estrategias de la empresa (ver Imagen 1). De igual manera dentro del análisis de proceso se tienen en cuenta procesos que son críticos, y que cuentan con un valor importante que permite ofrecer los servicios de la organización. La gestión de riesgos tecnológicos cuenta como base principal la ISO 31000.

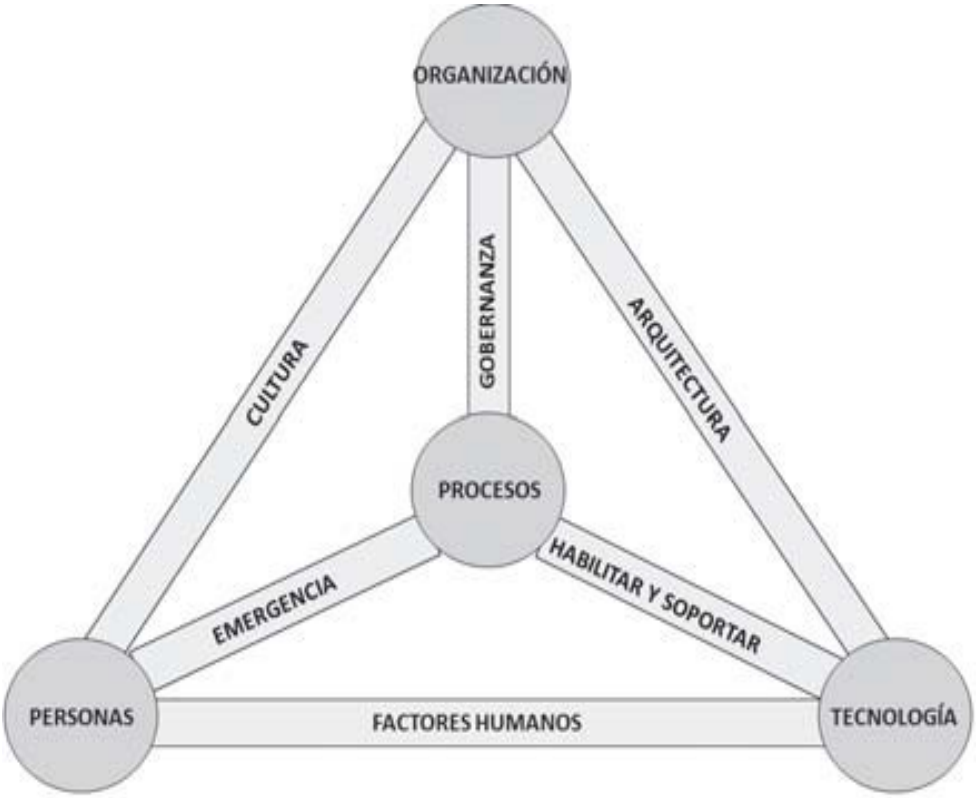

Imagen 1. Modelo de negocio para la seguridad de la información
Fuente: Institute for Critical Information Infrastructure Protection (ICIIP)

La metodología permite la inclusión en la gestión de continuidad de negocios como fase inicial de apoyo, lo que permite la identificación de dependencias críticas, activos y procesos clave, amenazas existentes y lo que pueda pasar en un futuro. Es común observar que la gestión de continuidad es clasificada como tratamiento de riesgos, pero es importante definir qué sirve nos sirve como soporte para la definición de impactos que pueda producir la no disponibilidad de servicios en la empresa.

Como siguiente paso de trabajo se relaciona con los activos de soporte a los procesos previamente analizados. Se debe analizar el Hardware, software, recursos humanos y físicos. Todo esto con la finalidad de clasificar y focalizar los recursos verdaderamente críticos y no clasificar en activos irrelevantes o poco importantes. (ver imagen2)

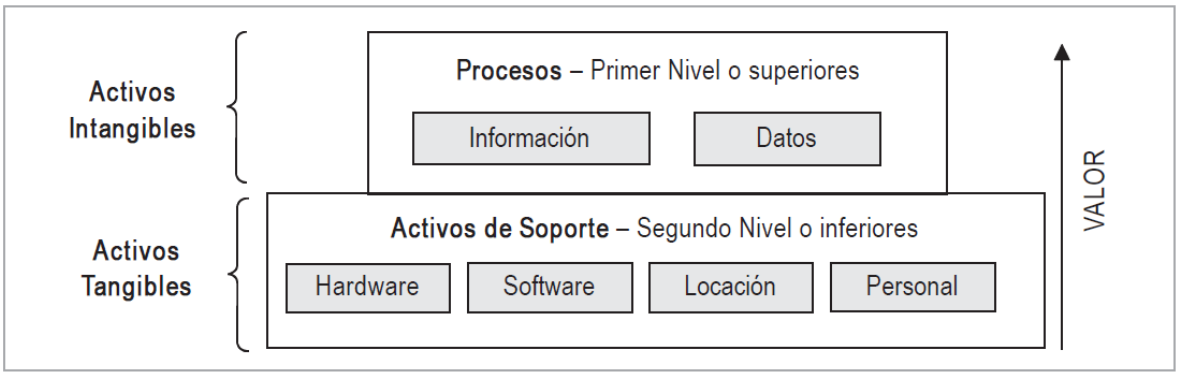

Imagen 2

Para el desarrollo de la metodología se toma como referencia el modelo PHVA (Planificar, Hacer Verificar y Actuar) para establecer así un proceso de gestión que se enfoque únicamente en la mejora continúa siguiendo bosquejo que a continuación se presenta:

PLANIFICAR: Establecer los procesos, objetivos y procedimientos para el proceso de gestión de riesgos tecnológicos. El objetivo principal de realizar esta planeación es la entrega de resultados que vayan con los lineamientos, políticas y objetivos de la empresa. De igual manera se establece una estrategia de comunicación y se analiza el contexto organizacional actual para poder definir el alcance de la gestión de riesgos tecnológicos.

HACER: Hace referencia a la implementación y puesta en marcha de los controles, procesos y procedimientos (implementación de las políticas definidas), y todo lo concerniente a la clasificación y tratamiento de los riegos.

VERIFICAR: Analizar y evaluar el rendimiento de los procesos contra la política y los objetivos de seguridad e informar oportunamente los resultados.

ACTUAR: Después de verificar los resultados, se debe establecer la política para la gestión de riesgos tecnológicos y realizar los cambios, implementaciones requeridas para la mejora de los procesos. Siendo parte de las fases verificar y actuar, son incluidos en una revisión constante y mejora continua, donde se validan constantemente los cambios y cumplimiento de los objetivos que fueron establecidos en la fase de planificación.

Como se indicó anteriormente, la metodología tiene como base los estándares internacionales y la norma técnica Colombiana 27001, ISO 31000, ISO 27005, debido a su enfoque en gestión de riesgos y al ser parte de la familia ISO, es posible ajustarlos a la metodología propuesta y linearla con el modelo PHVA (ver Imagen 3), es importante resaltar que fueron referenciadas mejoras de otras guías, que se mencionaran a continuación:

<table>
<tr><th>PHVA</th><th colspan="3">ISO 27005</th><th>ISO 31000</th></tr>
<tr><td rowspan="11">Planear</td><td colspan="3"></td><td>Mandato y compromiso de la dirección</td></tr>
<tr><td colspan="3">Definir plan de gestión de riesgos</td><td>Diseño del marco de trabajo para gestión riesgos</td></tr>
<tr><td colspan="2">Establecimiento del contexto</td><td rowspan="10">Proceso de gestión del riesgo</td><td>Entender la organización y su contexto</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Definir responsabilidades</td></tr>
<tr><td>Recursos</td></tr>
<tr><td>Integración con procesos</td></tr>
<tr><td>Establecer mecanismo de comunicación</td></tr>
<tr><td>Identificación del riesgo</td><td rowspan="3">Valoración Riesgo</td><td rowspan="4"></td></tr>
<tr><td>Estimación del riesgo</td></tr>
<tr><td>Evaluación del riesgo</td></tr>
<tr><td colspan="2">Desarrollar el plan de tratamiento del riesgo</td></tr>
<tr><td colspan="2">Aceptación del riesgo</td></tr>
<tr><td rowspan="3">Hacer</td><td colspan="2"></td><td>Establecer políticas para la gestión de riesgo</td></tr>
<tr><td colspan="2">Implementar el plan de tratamiento</td><td rowspan="2">Implementación del marco de trabajo para la gestión de riesgos</td><td rowspan="2">Implementar el proceso de gestión de riesgos</td></tr>
<tr><td colspan="2">Implementar plan de comunicación del riesgo</td></tr>
<tr><td>Verificar</td><td colspan="2">Monitoreo y revisión del riesgo</td><td colspan="2">Monitoreo y revisión del marco de trabajo</td></tr>
<tr><td>Actuar</td><td colspan="2">Mantener y mejorar el proceso de gestión</td><td colspan="2">Mejora continua del marco de trabajo</td></tr>
</table>

Imagen 3 Alineamiento de estándares ISO con modelo PHVA.

- **ISO 27001:** Norma técnica colombiana que especifica requerimientos para realizar la implementación de controles de seguridad acordes con el planteamiento del sistema de gestión de seguridad de la información (SGSI).

- **NTC/IEC 27002:** Estándar que establece pautas y principios generales para la implementación, mantenimiento y mejora de la seguridad. Tiene un amplio listado de objetivos y controles para el SGSI.

- **MAGERTIT:** Es una metodología española para el análisis y la gestión de riesgos de los sistemas de información, y se toma como base para la revisión y definiciones a la estimación de riegos.

- **NIST SP 800-30:** Guía creada por el instituto nacional de estándares y tecnología para la gestión de riesgos de sistemas de tecnología e información de estados Unidos. La guía nos brinda un apoyo en la valoración de procesos y mitigación de riesgos.

- **ITIL v3:** Librería de infraestructura de tecnologías de la información, estándar internacional que nos da indica y describe buenas prácticas para gestionar servicios de

TI. La metodología planteada aplica procesos que hacer referencia a gestión de incidentes, gestión de acceso (físico y lógico) y la mejora continua.

3. Pasos de la metodología

La metodología toma como referencia y base los pasos del proceso de gestión de riesgos de acuerdo a la ISO 27005 y que contempla las etapas siguientes (ver Imagen 4)

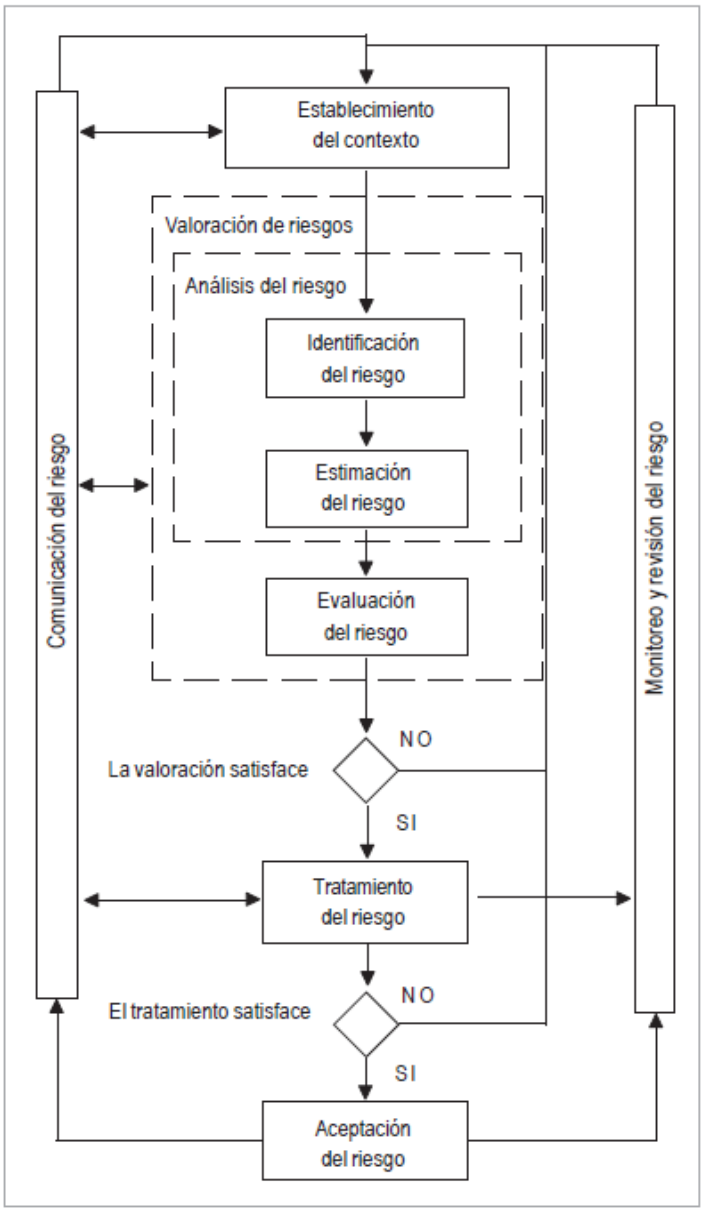

Imagen 4. Proceso para gestión de riesgos de acuerdo con ISO 27005

- Establecimiento de plan de comunicación interno y externo
- Definición del contexto organizacional interno y externo
- Valoración de riegos tecnológicos
- Tratamiento de los riesgos tecnológicos
- Monitoreo y mejora continua

3.1 Establecimiento de un plan de comunicación interno y externo

Un plan de comunicación debe realizarse a nivel interno donde sean activos (áreas de la empresa, empleados, socios, directivos) sea el caso, y si aplica a nivel externo (clientes, entes reguladores, proveedores o todos los anteriores si es necesario) teniendo como base las definiciones sobre la posible existencia del riesgo, los objetivos, los informes de los avances del proceso y de todo lo que se considere necesario. Los medios para comunicar el proceso dependen de las necesidades y disponibilidad del personal de la organización, pero se sugieren medios como capacitaciones, presentaciones, campañas de concienciación, circulares, correos electrónicos, contenido multimedia que permitan llegar al público objetivo.

El plan de comunicación deber ser diseñado y estructurado que permita crear cultura, conciencia en seguridad y se pueda dar a conocer el gran impacto de los riesgos tecnológicos. Si está bien diseñado nos permitirá alcanzar los objetivos de la gestión de seguridad, obtener información para su posterior análisis y poder prepararnos y planificar.
La propuesta para el plan de comunicación está dada por tres etapas

1. **Comunicación inicial:** descripción general sobre riesgos, ventajas e implicaciones

2. **Comunicación sobre el camino:** Se busca dar a conocer los avances del proceso de gestión de riegos e ir retroalimentando, y poder así conseguir el apoyo y participación de los miembros involucrados de la empresa

3. **Comunicación final:** En la última etapa de comunicación se busca dar a conocer y compartir los resultados obtenidos, dependiendo las políticas de la organización para alcanzar al público objetivo.

3.2 Definición del contexto organizacional interno y externo

Las organizaciones para este caso de ámbito público y gubernamental deben contar con un contexto que contiene, una misión, visión, políticas, objetivos, estrategias, normatividad y mucho más. De igual interactúa con un público y con esto podemos indicar que tiene un contexto externo por lo que debemos considerar aspectos como las regulaciones legales que apliquen, economía, tecnología, política. Es importante comprender estos aspectos para saber que debe ser protegido y que limitantes se pueden presentar para realizar dicha protección.
El principal objetivo de esta fase es conocer más a fondo la organización y así determinar que los puede afectar a nivel interno o externo, que deben proteger con base a la infraestructura tecnológica existente, como debe darse la protección, establecer el nivel de aceptación del riesgo (hasta donde puede ser negociable), determinar limitaciones actuales.

3.3 Valoración de riesgos tecnológicos

Es aquí en donde se identifican los activos que se quieren proteger, sus posibles debilidades y vulnerabilidades, amenazas a las cuales están expuestos. Se aconseja es recomendable adoptar controles para mitigación del riesgo.
Para la realización de la valoración de activos se deben tener en cuenta los activos tecnológicos que son más importantes y que son de vital necesidad para el funcionamiento correcto de la organización, como manejo de información, datos e infraestructura. La valoración se hace con base al costo de adquisición, renovación, mantenimiento, administración, licenciamiento si es el caso y es muy importante no olvidar el tema de depreciación. Después de culminar con el listado inicial de activos, validar si el alcance definido preliminarmente es correcto o si es necesario realizar ajuste para alcanzar los propósitos establecidos.
Es necesario considerar en esta etapa otros tipos de amenaza que pueden presentarse (lógicas, físicas, naturales, humanas, técnicas, intencionales), determinar los daños que pueden generar las amenazas, las pérdidas que pueden ocasionar. Con esta información es posible determinar los controles necesarios y establecer prioridades de riesgos.

La clasificación de los controles a usar es: los controles preventivos, controles predictivos y controles correctivos. Debemos tener en cuenta que, si hay uso o no de una base tecnológica, los controles pueden ser técnicos o no técnicos.

En el proceso de la identificación es importante tener presente las dependencias entre procesos y activos, el valor y el valor mismo por activo y proceso. Para esto los procesos deben ser priorizados con para poder así determinar los niveles de criticidad. Las vulnerabilidades pueden ser determinadas de varias maneras, como puede ser la ejecución de pruebas y listas de chequeo. Las amenazas deben clasificarse de acuerdo al análisis de criticidad y de impacto que pueda ocasionar y

relacionado con la frecuencia de ocurrencia para así determinar de mejor manera. La valoración se pueden utilizar técnicas cuantitativas como cualitativas para la valoración del riesgo y en cuanto a la presentación del informe final depende de los requerimientos, necesidades, recursos y habilidades de los colaboradores de la empresa u organización.

3.4 Tratamiento de riesgos tecnológicos

Es aquí en esta fase donde se establecen e implementan las acciones y correctivos a tomar para mitigar los riesgos encontrados y poder así disminuir en gran medida el riesgo y se convierta en un riesgo aceptable o residual aceptable para la organización, dentro de las acciones a tomar se determinan las siguientes: reducir, aceptar, eliminar y transferir.

Como parte del tratamiento, se definen las acciones o pautas a seguir y se establece un plan de tratamiento al riesgo según la priorización realizada previamente. El plan debe incluir recursos, responsabilidades ya actividades, teniendo como base principal las limitantes que se puedan presentar, nivel económico, legal, técnico y demás sean evidenciadas. Los controles que sean recomendados deben incluir análisis de costo-beneficio incluyendo costos de mantenimiento e implementación.

Es muy importante que el plan sea consistente con los objetivos y metas presupuestadas en la etapa de planificación del proceso de gestión de riesgos, de acuerdo con los tiempos definidos inicialmente y con base a los tiempos de vida útil del activo, además de ir de la mano con la siguiente fase de mejora continua.

3.5 Monitoreo y mejora continua del proceso de gestión

Es fundamental en esta etapa el control de cambios, por lo que se hace necesario el monitoreo sobre activos, procesos, vulnerabilidades, amenazas, controles, documentación de políticas para así establecer procedimientos y acciones a seguir ante los cambios presentados (riesgos o amenazas nuevas, ataques de día cero y muchos más) y asegurar así que la gestión este continuamente actualizada para poder evaluar los indicadores y cumplimiento de los planes.
El monitoreo principalmente busca asegurar la constate revisión sobre la gestión de riesgos y dar cumplimiento a los procesos de mitigación ya definidos. Permite también agregar y determinar nuevos riesgos.

4. Gestión del riesgo

La continuidad del negocio fundamentalmente cuenta con la gestión de incidentes que a su vez se relaciona con la gestión de riesgos. Una oportuna y

adecuada gestión de incidentes evita que sean activados los planes de continuidad del negocio y los planes de contingencia, debido a esto es tan importante que las respuestas a incidentes sean efectivas y se tenga muy claro y presente los riesgos que pueden estar relacionados y asociados.

La materialización de un riesgo (vulnerabilidad, amenaza) no es un secreto que puede ocasionar un gran impacto sobre la organización u empresa, que en muchos casos puede tener consecuencias legales, monetarias e indisponibilidad que para este caso puntual seria de servicios. Al realizar la valoración de gestión del riesgo tecnológico y su efecto sobre la infraestructura y activos de información. Con este análisis previo se puede proceder con la realización e identificación de los requerimientos mínimos para la continuidad de las operaciones, teniendo en cuenta posibles interrupciones y poder diseñar las alternativas o planes de contingencia para continuar así con la operación de la organización.

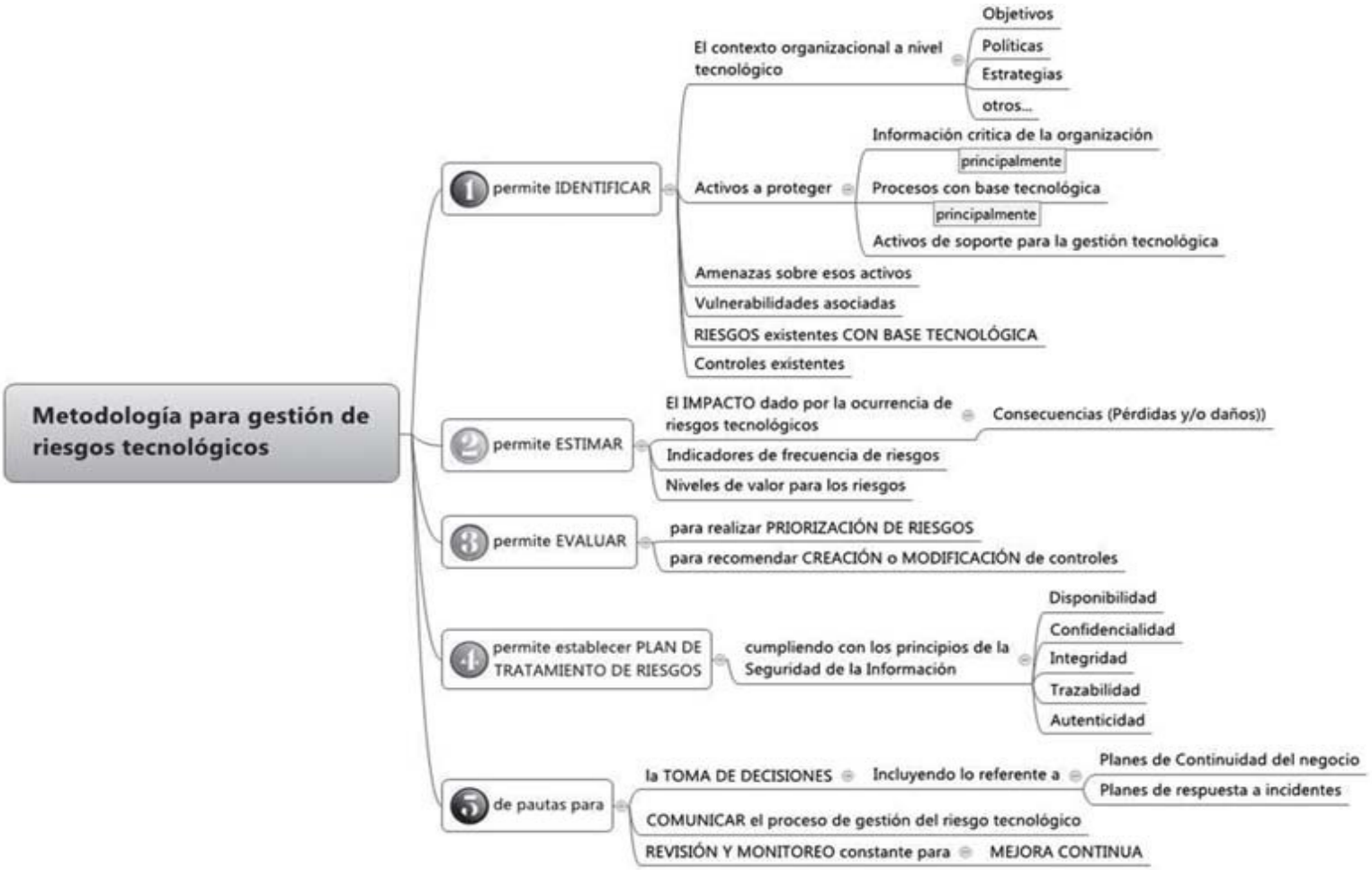

Imagen 5. Pasos de la metodología para la gestión

Parte de las estrategias de gestión de riesgos tecnológico y continuidad del negocio incluye la tarea u acción a tomar sobre los riesgos, y así saber el tratamiento que se le va a dar a dicho riesgo, aceptándolo, evitándolo, transfiriéndolo o mitigándolo.

Tenemos innumerables ejemplos y casos que nos sirven de apoyo que nos ilustran la necesidad de implementar planes de gestión de riesgos de tecnología y continuidad del negocio, en donde se pueda identificar los principales riesgos y amenazas a los cuales se ven expuestos diariamente la infraestructura tecnológica de la organización y poder contar con planes de respuesta eficaces en caso de alguna novedad o materialización de una amenaza. Hoy en día aún se encuentran muchas falencias en la gestión del riesgo tecnológico en muchas organizaciones, incluso de gran tamaño. Se realizó un estudio recientemente donde se encontró que solo una tercera parte de las organizaciones cuentan con estrategia de control del riesgo, lo cual es muy alarmante y preocupante debido a que no se le está dando la importancia necesaria a las medidas de prevención y mitigación de los riesgos.

Conclusiones

La metodología detallada en este documento ofrece una perspectiva amplia y profunda para la comprensión y aplicación de los conceptos establecidos en los estándares ISO para la gestión de riesgos tecnológicos. Proporciona un marco coherente y estructurado para identificar, clasificar y tomar acciones adecuadas frente a los riesgos tecnológicos. Esta metodología no solo enfatiza la importancia de la identificación de riesgos, sino que también guía en cómo clasificarlos y en la elección de las medidas de mitigación más efectivas.

En la era actual, donde la tecnología es un pilar fundamental en los procesos de negocio de las organizaciones, la gestión de riesgos tecnológicos se vuelve crítica. Las empresas, al depender en gran medida de las soluciones tecnológicas, se encuentran inherentemente expuestas a una variedad de riesgos tecnológicos. Estos riesgos pueden afectar significativamente las operaciones, la reputación y las actividades cotidianas de una organización, resultando en pérdidas y daños considerables. Por lo tanto, es imperativo fomentar una cultura de conciencia y seguridad de la información, enfocándose en la prevención y mitigación de estos riesgos. La búsqueda constante de estrategias efectivas y el apoyo decisivo de la alta gerencia son fundamentales para garantizar el aseguramiento y el buen uso de los recursos tecnológicos.

Finalmente, es esencial que las organizaciones fortalezcan su protección en tres niveles críticos: físico, lógico y humano. Esto incluye la implementación de controles de acceso, cámaras, seguridad perimetral y sensores a nivel físico; la gestión eficaz de los sistemas de información y software a nivel lógico; y una toma de decisiones informada y consciente de los riesgos a nivel humano. Dado que la tecnología impregna estos tres aspectos, la exposición a riesgos tecnológicos es una constante que requiere atención y gestión continua.