UNIVERSIDAD GABRIELA MISTRAL
FACULTAD DE INGENIERIA

Implementando una iniciativa de Resiliencia Operacional en una Compañía de Seguros.

Memoria para optar al título de Ingeniero de Ejecución en Informática

Autor : Hernán Valdés Torres
Profesor Guía : Roberto Carú Cisternas
Profesor Integrante : Jorge Tapia Castillo

Santiago – Chile
Octubre, 2012

INDICE

1. INTRODUCCION

En la actualidad las empresas orientadas a los servicios deben enfrentar una cantidad innumerable de desafíos propios de un mercado cada vez más competitivo. Esto se ve reflejado en la constante lucha por desarrollar nuevos y mejores productos que mantengan fieles a sus clientes y también permitan acrecentar su cartera actual, con el objetivo implícito de no sólo cubrir y rentabilizar su inversión, sino además garantizar una proyección en el tiempo.

Por otra parte están los requerimientos de las entidades reguladoras, las cuales fruto de la apertura económica y de la aparición de un gran número de transnacionales y compañías extranjeras en el escenario local, han tenido que afinar sus exigencias en virtud de que las empresas deban tener una gestión efectiva de su riesgo operacional. Este fenómeno ya se ha visto desde hace algún tiempo en el sector financiero, donde las entidades reguladoras que lo rigen (la Superintendencia de Bancos e Instituciones Financieras y la Asociación de Bancos e Instituciones Financieras de Chile A.G) han tenido que alinearse con el estándar internacional BASILEA I y II, el cual regula el mercado de capitales en virtud de los riesgos, tanto financieros como operacionales.

Es por lo indicado anteriormente que la gestión eficiente del riesgo operacional se está convirtiendo, poco a poco, en un tema relevante dentro de las empresas. Esto conlleva el evidente impacto en las áreas responsables de administrar las tecnologías de la información, piedra angular en la operación de muchas organizaciones orientadas a los servicios. Las mismas han tenido que destinar importantes esfuerzos para mantener una plataforma tecnológica administrada adecuadamente con el fin de ofrecer un nivel aceptable de control sobre los riesgos. Tal es el caso de las empresas de Contact Center, que dan servicios a bancos y financieras, debiendo cumplir los mismos requerimientos de seguridad y continuidad operativa que tienen sus clientes.

También la apertura económica es un factor importante que ha marcado este cambio en el mercado. Donde muchas empresas que se han fusionado con transnacionales, están volviéndose más exigentes para la evaluación de sus proveedores tomando la gestión de riesgo operacional como un elemento crítico en la selección de estos.

Así es como algunos marcos de gestión como COBIT y estándares internacionales como las ISO/IEC27001y BS7799, las cuales entregan los pasos para implementar un programa de seguridad alineado con los objetivos del negocio junto con las buenas prácticas asociadas, están empezando a convertirse en una guía obligada que las empresas deben seguir para cumplir satisfactoriamente los requerimientos del mercado y de las entidades reguladoras.

El mercado evoluciona y, para sobrevivir, las empresas de servicios deben adaptarse rápidamente a esta realidad.

No basta con el cumplimiento con estándares o requerimientos de las entidades reguladores, las organizaciones deben evaluar como ellas pueden manejar adversidades y seguir cumpliendo con sus metas, ya que siempre están expuestas a una serie de eventos: la tecnología puede fallar, la gente puede cometer errores, los ataques de competidores y/o adversarios y los eventuales desastres ya sean naturales o provocados por el hombre. La organización debe ser capaz de operar bajo condiciones adversas y tener la capacidad de volver a su operación normal, de manera rápida y al menor costo posible. En otras palabras, la organización debe hacerse suficientemente *"resiliente"* [1] a las interrupciones, si esta se propone seguir siendo viable.

Una organización que quiera hacerse *resiliente* para mejorar su competitividad, debe tener presente que la gestión efectiva de los riesgos a los que está expuesta depende de dos factores fundamentales:

[1] La resiliencia será explicada en detalle en el capítulo 2 de este trabajo: Marco Teórico.

- La capacidad de prever y anticipar potenciales situaciones de riesgo que puedan poner en peligro la continuidad de sus operaciones, a través de medidas protección.
- La capacidad de reaccionar a tiempo en caso que las medidas de protección no hayan sido suficientes y el riesgo se haya hecho efectivo. Esto último a través de medidas represivas y/o correctivas que permitan reducir ó corregir los daños ocasionados por el incidente en el menor tiempo posible.

De lo anterior se puede deducir que un modelo de negocios tolerante a riesgos requiere del trabajo conjunto de dos iniciativas: Seguridad de la Información y Continuidad del Negocio.

El resultado del trabajo alineado y complementado de estas dos iniciativas permite generar una “coraza” en aquellos elementos que se desea hacer más resilientes. Por un lado la Seguridad de la Información establece medidas de protección (preventivas), mientras que Continuidad del Negocio garantiza la sostenibilidad de los elementos con medidas represivas y correctivas.

Lo que más importa a las organizaciones es que todos sus servicios y procesos esenciales sean siempre capaces de llevar adelante su misión en forma consistente, dentro de los presupuestos establecidos, y dentro de las tolerancias operacionales normales. Desde el punto de vista de la resiliencia operacional todos los activos que soporten estos servicios ó procesos de negocio deberán ser cubiertos en el alcance de las iniciativas de Seguridad y Continuidad de Negocios. Fundamentalmente son 4 los activos que deben ser considerados:

- Las personas, que son quienes ejecutan y monitorean los procesos de negocio.
- La información, que ingresa y además es producida por los procesos de negocio.
- La tecnología, que soporta y automatiza los procesos de negocio.

- Las instalaciones (oficinas, edificios, etc.), en donde se llevan a cabo estos procesos.

De existir en la compañía un Plan de Continuidad de Negocios actualizado, será sencillo poder identificar aquellos procesos de negocio que conforman el núcleo del negocio de la compañía. A partir de allí será factible establecer cuáles son las personas asignadas a éstos, cuál es la información producida como parte de su ejecución, qué infraestructura tecnológica los soporta, y cuáles son las instalaciones en donde se llevan a cabo.

1.1. Motivación.

En el mercado de seguros existe como entidad reguladora la Superintendencia de Valores y Seguros (SVS) la cual tiene estatutos, en formato de circulares, con variadas exigencias que deben ser cumplidas por las aseguradoras. Los requerimientos que podemos encontrar en estas circulares van desde garantizar la continuidad de los servicios a los clientes, hasta de proteger la información sensible de los mismos.

Por otra parte dada la naturaleza de este negocio, donde no existe la manufactura o producción de bienes, el activo más importante es la información, tornándose crítica la plataforma tecnológica y los sistemas informáticos que la sustentan. Debido a lo explicado anteriormente, es necesario implementar una gestión de riesgos de TI acorde con los objetivos estratégicos de la organización, con el fin de implementar controles que garanticen la calidad y continuidad de las operaciones y cumplir los compromisos establecidos con socios y clientes, creando un aporte que permita aumentar la tolerancia de la compañía a los riesgos y consecuentemente aumentar la confiabilidad de la misma, lo que redundará en contratos a más largo plazo con sus clientes y/o socios, aumento de capital de inversión de parte de los inversionistas y menores reservas patrimoniales exigidas por la entidad reguladora.

1.2. Hipótesis.

La hipótesis planteada para este trabajo es la implementación de una iniciativa de resiliencia operacional en una organización, a través de un modelo de gestión de riesgos con orientación de procesos, que integre los fundamentos de la Gestión de la Continuidad de Negocios (BCM con sus siglas en inglés) junto con la gestión de los riesgos de seguridad y de TI, para disminuir y controlar permanentemente el nivel del riesgo sobre los activos y garantizar la continuidad operativa y comercial. El propósito final es mejorar la rentabilidad de la organización a través de la eficiencia de los procesos críticos de negocio y la inversión segregada e inteligente de controles de seguridad en función de la importancia de la información a proteger.

Es importante destacar que la aplicación de este modelo puede ser hecha en cualquier empresa cuya gestión dependa fuertemente de la tecnología, sin importar su tamaño, dado que su fin último es la gestión eficiente del riesgo operacional y garantizar a los interesados una continuidad operativa que satisfaga las expectativas de sus clientes y sus requerimientos de negocio.

1.3. Objetivo general.

Integrar la gestión de continuidad de negocios con la gestión de riesgos de seguridad de TI para mejorar la resiliencia operacional en una organización. El principal objetivo será disminuir el nivel del riesgo operacional y garantizar la continuidad ante desastres, controlando los riesgos sobre los activos que soportan los procesos críticos de una organización: personas, información, tecnología e instalaciones, con especial énfasis en los activos de información y la plataforma tecnológica que los soporta.

1.4. Objetivos Específicos.

- Definir las premisas de análisis las cuales determinarán el alcance de la iniciativa.
  - Evaluación de escenarios de desastres y su respectivo impacto.
  - Definir los procesos críticos que serán cubiertos por la iniciativa.
  - Áreas de la empresa que serán incluidas por defecto.
  - Generación del alcance en virtud de lo definido por la dirección de la empresa.

- Confección del Business Impact Analisys (BIA) para los procesos cubiertos por el alcance de la iniciativa, junto con un inventario de activos de información donde los mismos serán clasificados en virtud de sus requerimientos de confidencialidad, integridad y disponibilidad.

- Generar una evaluación de riesgos de seguridad a través de un análisis sobre los activos críticos de información.

- Definir con la dirección de la empresa las estrategias de mitigación de los riesgos identificados.

- Implementar los controles sugeridos por el análisis en virtud de la estrategia de mitigación definida.

- Medir el resultado de la iniciativa generando un plan de auditoría para evaluar la implementación de los controles y un plan de pruebas para evaluar la efectividad de los planes de continuidad de negocios.

1.5. Alcance.

Desarrollar una iniciativa de gestión de continuidad de negocios, que mantenga identificados los procesos críticos de la organización, y que permita desarrollar un dispositivo de seguridad que identifique y controle los riesgos operacionales que puedan impactar a los activos que soportan los procesos críticos del negocio.

2. MARCO TEORICO

2.1. Resiliencia operacional

2.1.1. ¿Qué es Resiliencia?

En la comunidad científica este fenómeno es entendido como la capacidad de los materiales físicos como el acero y el cuero, para volver a su forma original después que han sido deformados de alguna manera. También este término ha sido empleado en otras disciplinas, tal es el caso de la sicología educacional, donde la resiliencia se refiere a la capacidad de las personas para recuperarse ante la adversidad y/o hechos traumáticos de los cuales han sido víctima.

2.1.2. ¿Cómo definimos la Resiliencia Operacional?

La Resiliencia Operacional se puede describir como la capacidad de una organización para adaptarse y gestionar los riesgos que emanan de su operación diaria, haciendo frente de una manera sistemática y transparente a los eventos perturbadores que puedan impactar en la capacidad global de cumplir su misión. Desde un punto de vista práctico, implementar la resiliencia operacional significa diseñar y gestionar los procesos del negocio junto con los activos críticos relacionados (personas, información, tecnología e instalaciones) con un enfoque de riesgo, de una manera que asegure que la misión de los procesos sea factible y sustentable. Así podemos decir que la resiliencia operacional en un proceso de negocio, es fruto de la gestión efectiva de la resiliencia en cada uno de los activos críticos que lo soportan.

Funcionalmente la resiliencia operacional es un punto de equilibrio que la organización debe ser muy hábil de gestionar. En este punto de equilibrio, está la convergencia de muchas demandas organizacionales que deben ser consideradas. Por un lado, la organización está balanceando los recursos y activos que utiliza para alcanzar sus objetivos tomando en consideración su deseo de mantener los costos contenidos y

maximizar el retorno sobre la inversión. Al mismo tiempo, debe tomar en cuenta el nivel de recursos que pretende gastar para que aquellos eventos que atenten contra el cumplimiento de sus objetivos sean contenidos, o limitar el nivel de daño que podrían provocar a la organización.

Para enfocar la resiliencia operacional desde un punto de vista estratégico, las organizaciones deben intentar responder dos preguntas:

- ¿Cual es el estado normal de funcionamiento de la organización?
- ¿Que nivel de resiliencia operacional es adecuado para la organización?

El grado en que una interrupción se convierta en un tema crítico para la organización depende del nivel de tolerancia que esta tiene para operar fuera de su funcionamiento normal. Al ser capaz de definir el concepto de *operación normal* proporciona un punto de referencia contra el cual la organización puede decidir su nivel de resiliencia tomando en cuenta una serie de impactos.

2.2. Equilibrio Operacional.

Todas las empresas operan diariamente en lo que se denomina su Equilibrio Operacional ó Zona de Confort. Es decir, el punto en donde existe un balance entre los productos generados, los recursos utilizados, los costos incurridos y las ganancias obtenidas. La ocurrencia de un incidente que desplace a la empresa de su Zona de Confort hace que sea necesario "gastar" más recursos de lo habitual, como resultado de ello se incurre en costos adicionales, se pone en riesgo el cumplimiento de los objetivos y compromisos, disminuyen los retornos de inversión y la reputación de la empresa se ve afectada.

Las Figuras 1 y 2 muestran el efecto producido por un incidente que desequilibra la Zona de Confort en una organización vulnerable y otra resiliente. La pendiente de la

curva que se produce luego del incidente y la amplitud de la misma indican el grado de vulnerabilidad de la empresa frente al incidente, mientras que el comportamiento de la función marca la capacidad de la misma de recuperar el nuevo estado de equilibrio.

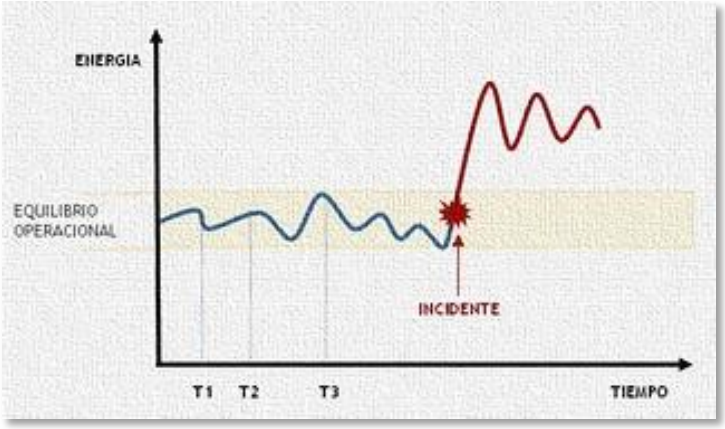

Figura 1. Impacto de un incidente en el Equilibrio Operacional de una organización vulnerable.

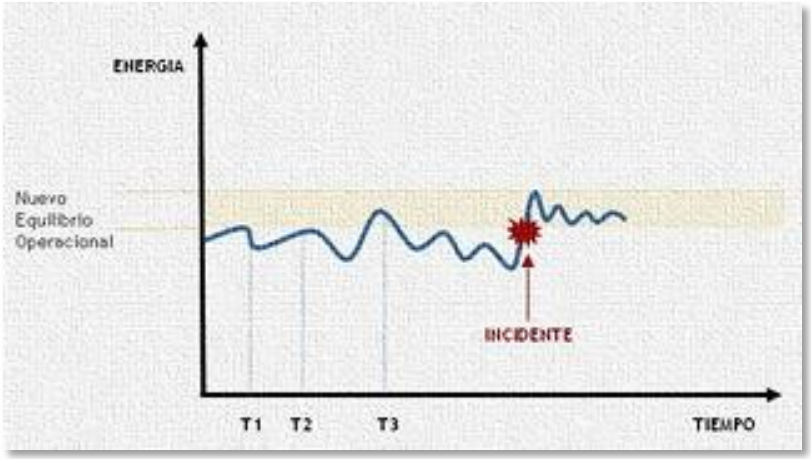

Figura 2. Impacto de un incidente en el Equilibrio Operacional en una organización “resiliente”.

Una organización que frente a un incidente obtiene un leve desplazamiento hacia arriba de la función de equilibrio, consecuencia de la inversión de más energía para la aplicación de las medidas y los controles de respuesta, obtiene un aumento en su resiliencia lo que la coloca en una posición más favorable para enfrentar nuevas situaciones de riesgo.

Una organización debe decidir en base a muchos factores, incluyendo sus conductores organizacionales y la tolerancia al riesgo, cuanto movimiento del umbral de equilibrio puede aceptar. Ligeras variaciones diarias pueden ser tolerables, pero los movimientos extremos pueden sofocar la organización e incluso provocar el cese de las operaciones. En el día de hoy, existen muchas organizaciones que son sensibles a fuerzas del mercado y a los riesgos ambientales, tal es el caso de las aerolíneas donde el aumento del precio del combustible por un tiempo prolongado puede provocar que las compañías quiebren, y por otra parte están los negocios basados en internet, donde los ataques del tipo DoS (denegación de servicios) pueden afectar su capacidad de conectarse con los clientes con catastróficas consecuencias.

El punto de equilibrio operacional es importante porque es la base para describir el rango de tolerancia que una organización tiene en caso de alteraciones. A su vez, este rango describe esencialmente los límites de la capacidad de recuperación operativa de la organización. Una organización que puede operar dentro de un amplio rango de desviación de lo normal puede tener un funcionamiento más resistente que aquella organización que tiene unos límites más estrictos

2.3. El nivel de resiliencia operacional adecuado.

El nivel adecuado de resiliencia es único para cada organización, dado que depende de muchos factores que se vuelven particulares hacia las mismas, tales como la misión, la ubicación geográfica, posición competitiva, el nivel de dependencia de la tecnología, las leyes y los requerimientos de las entidades reguladoras, etc. Ejemplificando un poco tenemos el caso de una empresa que provee el servicio de data center cuyos clientes corresponden a entidades financieras, dadas las exigencias del nivel de servicio de de sus clientes necesita fortalecer su resiliencia operacional para cumplir con sus obligaciones. Otro caso es una empresa con una considerable reserva de capital, la cual podría ser capaz de tolerar largos períodos de bajos ingresos o aumento temporal de los costos debido a eventos disruptivos o riesgos. El nivel adecuado de resiliencia

también es dinámico, lo que nos permite cumplir con nuestra misión hoy puede cambiar drásticamente mañana.
En resumen una organización operacionalmente resiliente debe tener la capacidad de lograr tres cosas:

I. En la medida de lo posible, aplicar controles y procesos que prevengan o limiten el movimiento de la organización fuera del rango normal.
II. Ser capaz de sobrevivir durante un movimiento prolongado o significativo fuera del rango normal hasta que la perturbación se controle o se elimine.
III. Lo más importante, tener la capacidad de volver al funcionamiento normal.

En otras palabras la organización debe ser capaz de invertir los recursos necesarios de manera efectiva y eficiente, para prevenir la interrupción, operar durante la interrupción, y restaurar sus operaciones al estado normal. La inhabilidad de la organización para llevar a cabo alguna o todas estas tareas, disminuye su resiliencia operacional.

2.4. Riesgo operacional.

El riesgo operacional es la potencial pérdida que surge a raíz de la operación diaria en una organización. De acuerdo al Comité de Basilea[2], el riesgo operacional puede ser definido como el riesgo de pérdida resultante de:

- Procesos internos inadecuados o fallidos.
- Acciones deliberadas o accidentales de la gente.
- Problemas con sistemas y tecnología.
- Eventos externos.

En un intento de delimitar el concepto de riesgo operacional, el Comité de Basilea define siete categorías estándar de eventos que podrían resultar en este tipo de riesgo:

[2] El Comité de Basilea se describe en detalle en el glosario de este trabajo.

1) Fraude interno.
2) Fraude externo.
3) Prácticas laborales y de seguridad en el trabajo.
4) Clientes, productos y prácticas de negocio.
5) Daño de activos físicos.
6) Interrupción del negocio y fallas en los sistemas.
7) Ejecución, entrega y gestión de procesos.

En una organización se puede identificar y controlar el riesgo operacional a través de la gestión de seguridad, la continuidad de negocios y la operación de TI. A su vez podemos indicar que en la medida en que se logra administrar y equilibrar la ecuación del riesgo operacional (condición y consecuencia) podremos alcanzar un nivel satisfactorio de resiliencia operacional.

2.5. Implementando resiliencia operacional en la organización.

2.5.1. El rol de seguridad.

El objetivo de toda gestión de seguridad es mantener los activos críticos bajo un nivel deseable de resguardo, alineando todas sus actividades bajo un enfoque de gestión del riesgo, de hecho podríamos decir que las actividades de seguridad son muchas veces una extensión de esta disciplina: identificación, análisis y mitigación del riesgo que puede afectar a los activos críticos de la organización. Una adecuada gestión de seguridad requiere un enfoque integral de los dos elementos de la ecuación de riesgo: causa (vulnerabilidades y amenazas) y consecuencia (impacto para el negocio). Cuando una organización realiza esto de manera efectiva, en alineamiento con los conductores organizacionales y al menor costo posible, está dando un apoyo directo a su resiliencia operacional.

Elementos de riesgo	Actividad de seguridad
Condición	Identificar vulnerabilidades y posibles amenazas a los activos críticos a través de actividades de identificación y análisis de riesgos.
Condición	Limitar la exposición de los activos críticos a través del desarrollo e implementación de controles técnicos, administrativos y físicos.
Consecuencia	Desarrollo e implementación de planes para prevenir, reducir o limitar el impacto de los riesgos a un nivel aceptable.

Tabla 1: Relación entre los elementos de riesgo y las actividades de seguridad.

2.5.2. El rol de la Continuidad de Negocios.

El fundamento de la continuidad de negocios es satisfacer el requerimiento de toda organización de limitar los efectos no deseados de un riesgo cuando se concreta. El reciente surgimiento de la continuidad del negocio como una parte esencial de la planificación de la organización se basa en el aumento de eventos catastróficos, junto con el impacto mediático que traen consigo, tales como los ataques terroristas y los fenómenos naturales como huracanes, terremotos y tsunamis. Pero la importancia de la continuidad del negocio es también una consecuencia del reconocimiento de esta actividad como un factor central de gestión de riesgos y, como tal, tiene por necesidad evolucionar y madurar hasta convertirse en una competencia en toda la empresa.

Existe una relación significativa entre la continuidad del negocio y la gestión de la seguridad debido a que ambos se refieren a aspectos del riesgo operacional. Aunque la gestión de la seguridad tiende a centrarse más en las condiciones de riesgo, la continuidad del negocio ha sido tradicionalmente una actividad orientada hacia las consecuencias del mismo. Cuando estas iniciativas convergen, se vuelve posible la gestión integral del riesgo operacional lo que va en favor de mejorar el nivel de resiliencia operacional.

2.5.3. Importancia de las Operaciones de TI.

La tecnología es parte fundamental en la operación de las organizaciones hoy en día. Soporta la productividad de los procesos y los activos críticos del negocio. Pero también introduce mayor complejidad que a menudo resulta en nuevos escenarios de riesgo. De hecho, es una de las más ricas fuentes de riesgo operativo, tomando en consideración que la mayoría de las organizaciones cuando definen su programa de seguridad y de continuidad de negocio lo realizan en torno a las actividades soportadas por la tecnología. No es una casualidad que las organizaciones que mejoran su capacidad en la operación de TI a menudo obtienen también mejoras en seguridad y continuidad, esto es producto de que la adecuada gestión de las operaciones de TI involucra tecnología de alta disponibilidad. El destacado papel de la tecnología, para llevar a cabo los procesos de negocio, significa que una mayor disponibilidad se traduce en una mejora directa de la resiliencia operacional.

2.5.4. Enfoque de proceso.

Un proceso es un conjunto estructurado de actividades relacionadas entre sí con el fin de llegar a un resultado deseado. Hay muchos procesos en la organización, algunos son definidos y conocidos por la misma, y otros son informales, mal definidos, y no pueden ser comunicados. Cuando un proceso está bien definido, es más probable lograr los resultados deseados ya que la hoja de ruta para alcanzar los objetivos está desarrollada y comunicada.

Un enfoque de proceso para la resiliencia operacional se describe como el medio que define, comunica, y controla el proceso utilizado para sostener la misma de manera adecuada en la organización. De esta manera se logran establecer metas compartidas para la gestión del riesgo operacional, alineando las actividades necesarias para el cumplimiento de los objetivos de la gestión de seguridad, de la continuidad del negocio y de las operaciones de TI. Algunos beneficios del enfoque de proceso son:

- Enfoque en metas y requerimientos comunes.
- La eliminación de las barreras organizativas para el logro de metas.
- Definir y comunicar los procesos de seguridad y de continuidad de negocio.
- Medición de la efectividad.
- Proporcionar una estructura para las mejores prácticas.
- Definir un lenguaje común.
- Facilitar el cumplimiento de los compromisos regulatorios.

2.5.5. Activos que deben ser cubiertos por la iniciativa.

Al implementar una iniciativa de resiliencia operacional, se debe tener presente que las actividades deben ir en dirección de soportar los cinco activos que permiten que la organización cumpla su misión: gente, información, tecnología, instalaciones y procesos de negocio. Por lo tanto las actividades de seguridad tienen el propósito de prevenir la interrupción de la capacidad productiva de estos objetos, mientras que las actividades de continuidad del negocio se enfocan en que los procesos de negocio que son soportados por estos, puedan seguir operando en el evento de que algún activo sea interrumpido. En resumen, para soportar la resiliencia operativa de la organización es necesario soportar la resiliencia operativa de cada uno de estos activos, los cuales son indicados en la Figura 3.

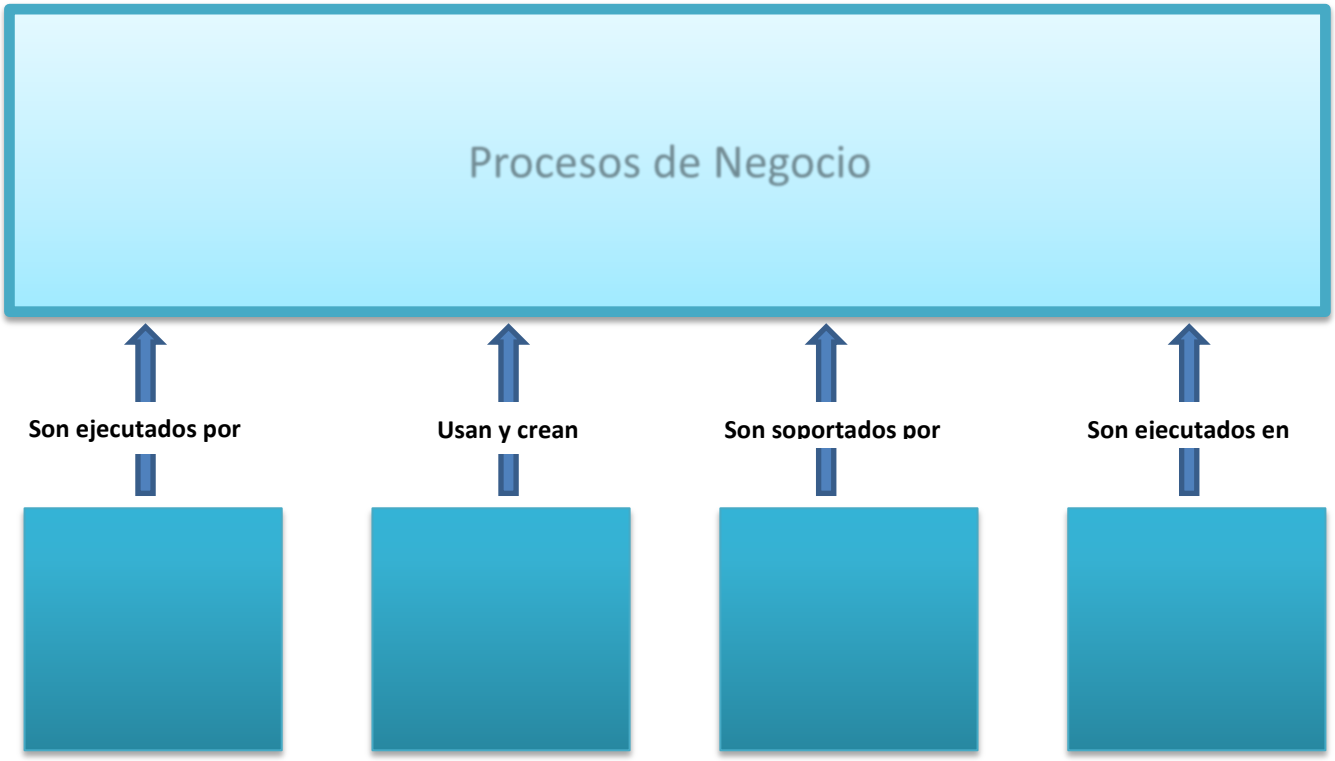

Figura 3. Los activos que deben ser cubiertos por la Resiliencia Operacional.

- ***Proceso de Negocio:*** conforma el motor fundamental que hace que la organización funcione.
- ***Personas:*** Operan y monitorean el proceso.
- ***Información y data:*** Es usada y producida por el proceso.
- ***Tecnología:*** Soporta y automatiza el proceso.

- ***Instalaciones:*** Lugar donde el proceso es realizado.

2.5.6. Buenas prácticas de la industria.

En la siguiente tabla podemos encontrar algunas fuentes de buenas prácticas, con reconocido prestigio en el mercado, que pueden ser herramientas útiles para establecer el marco de trabajo que nos permita desarrollar una iniciativa de resiliencia operacional.

Fuente	Audiencia	Enfoque	Relevancia para la organización
ISO17799	Internacional	Gestión de la seguridad de la información	Gestión de las practicas vinculadas a la seguridad de la información
COBIT	Internacional	Seguridad y controles de IT	Objetivos de control para la seguridad de TI y para el control de procesos.
ITIL	Internacional	Gestión de los servicios de TI.	Practicas para la gestión de operaciones y los servicios de TI que contribuyen a la seguridad
NIST 800-40/800-53	USA	Seguridad en los sistemas de información	Practicas de la seguridad de la información que son enfocadas a sistemas.
CMMI	Internacional	Mejora de procesos	Estructura para la mejora de procesos y niveles de madurez
DRII	Internacional	Continuidad de negocios y recuperación	Practicas de BCP y DRP respaldadas por el Disaster Recovery Institute International.

Tabla 2. Buenas prácticas y estándares de la industria.

2.6. El proceso de seguridad de la información.

El proceso de seguridad de la información es un círculo que comienza con la evaluación de riesgos y la determinación de requerimientos de seguridad, seguido por el monitoreo y evaluación de los sistemas y prácticas involucradas, el entrenamiento y sensibilización a los empleados, finalizando con la implementación de controles y políticas de acuerdo

a los requerimientos determinados en la primera etapa. Un ejemplo de la aplicación de la seguridad como proceso es el ***sistema de gestión de seguridad de la información*** (SGSI) desarrollado por el estándar ISO 27001, el cual implementa un programa de seguridad a través del modelo de calidad PDCA (Plan, Do, Check, Act):

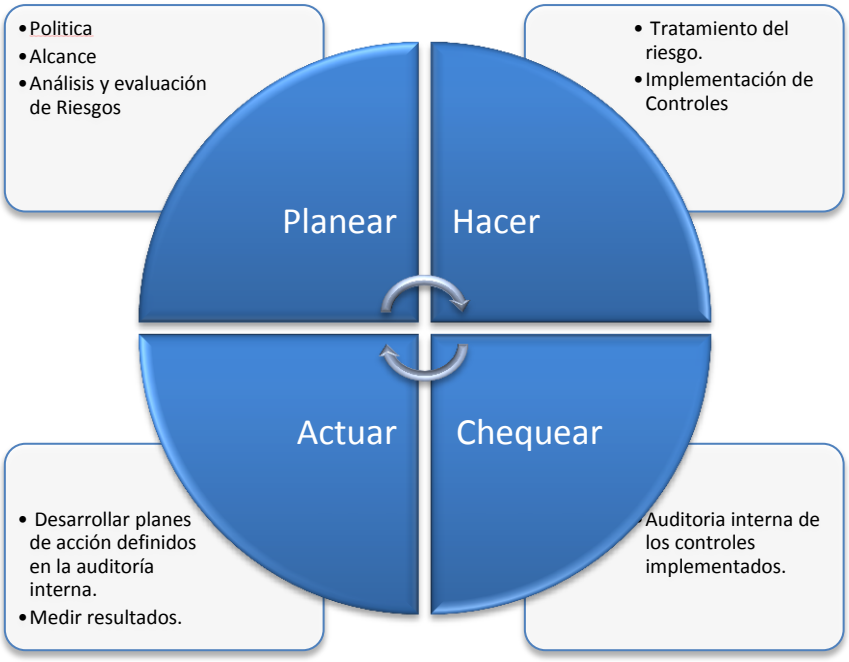

Figura 4. Sistema de Gestión de Seguridad de la Información (SGSI) del estándard ISO 27001.

Los componentes centrales de un programa de seguridad son gestión del riesgo, políticas de seguridad, procedimientos, estándares, líneas bases, clasificación de la información y sensibilización, teniendo como principal objetivo la protección de los activos de la organización. Donde el análisis del riesgo identifica Los activos, las amenazas que podrían afectarle, junto con el impacto o pérdidas que podrían tener. Los resultados del análisis de riesgos ayudan a la gerencia a construir presupuestos con fundamentos sólidos para invertir en controles que protejan los activos y desarrollar políticas que direccionen las actividades de seguridad. Los planes de sensibilización informan a cada empleado con los lineamientos de seguridad adoptados para mantenerlos informados y alineados con las metas de seguridad adoptadas.

Es fundamental que una iniciativa de seguridad tenga un enfoque *top-down*, es decir, que su iniciación, soporte y dirección venga de la alta gerencia de la empresa, pasando por los mandos medios hasta llegar a los miembros del personal. Por el contrario el enfoque *bottom-up*, que es cuando el área de TI toma las riendas de la iniciativa sin el debido respaldo de la gerencia, tiene pocas posibilidades de éxito producto que tendrá un alcance limitado en la organización, siendo un programa dirigido sin aquellas personas que tienen como primera responsabilidad la protección de los activos de la organización (la dirección de la empresa).

En un modelo de seguridad a nivel organizacional, la planificación de la seguridad puede separarse en tres áreas: estratégica, táctica y operacional. La planificación estratégica está alineada con los objetivos del negocio y de TI. Las metas del plan estratégico tienen una mirada de largo plazo y se proyecta de tres a cinco años. Algunos ejemplos de metas del plan estratégico de seguridad son:

- Asegurarse que el riesgo sea entendido y direccionado.
- Asegurar cumplimiento con entidades reguladoras y las leyes.
- Integrar responsabilidades de seguridad a través de la organización.
- Crear un modelo de madurez que permita una mejora continua.

- Usar seguridad como una ventaja competitiva que atraiga más clientes.

La planificación táctica corresponde a las iniciativas y otros apoyos que deben ser implementados para alcanzar las metas más amplias que han sido definidas por la planificación estratégica. Su alcance es de mediano plazo (uno a dos años).

Finalmente la planificación operativa tiene que ver con planes más específicos, con plazos y metas a corto plazo. Algunos ejemplos de planes operativos son:

- Realizar evaluaciones de riesgos de seguridad.
- No permitir que los cambios de seguridad impacten en la productividad.
- Implementar y mantener los controles.
- Buscar continuamente vulnerabilidades y parchar los sistemas.
- Evaluar cumplimiento de políticas.

Una organización nunca implementa todos los cambios a la vez, y algunos cambios toman más tiempo que otros, y muchas veces algunos cambios no pueden pasar hasta que otros no hayan sucedido.

2.6.1. Fundamentos de la seguridad.

La seguridad de la información la podemos definir como la preservación de las propiedades de Confidencialidad, Integridad y Disponibilidad de la información, lo que se le llama la triada CIA (Confidentiality, Integrity, Availability), aunque existen organizaciones donde se suma una nueva propiedad, auditabilidad. Estos elementos fundamentales para la seguridad se explican a continuación:

- ***Confidencialidad:*** Es la propiedad de la información que garantiza que la información sea entregada sólo a personal autorizado, donde se debe asegurar que el nivel apropiado de secreto sea reforzado en cada etapa del proceso de datos. La confidencialidad puede ser controlada a través del cifrado en el almacenamiento y

transmisión de datos, estricto control de acceso, clasificación de activos, entrenamiento del personal y procedimientos de seguridad. Algunas amenazas que vulneran la confidencialidad son la ingeniería social, monitoreo de la red, troyanos, spyware y los ataques del tipo shoulder surfing, este último se refiere a espiar, por sobre el hombro de una persona lo que está haciendo en su computador

- ***Integridad:*** Propiedad de la información y de los sistemas que la soportan de mantenerse precisa y confiable, protegida de cualquier modificación no autorizada. Los sistemas deberían ser protegidos de cualquier interferencia y contaminación externa. Cuando un atacante inserta virus, bombas lógicas o back doors en un sistema, la integridad es comprometida trayendo como impacto corrupción de la data y proceso erróneo de datos. Aunque la mayoría de las veces el motivo de los riesgos de integridad es accidental por errores de los usuarios, también se da el caso de acciones intencionales ligadas a fraudes.
- ***Disponibilidad:*** Es el aseguramiento del acceso oportuno y confiable de los individuos a los activos. Los sistemas y redes deberían tener controles adecuados para funcionar de manera previsible con un nivel aceptable de rendimiento, con la capacidad de recuperarse en caso de interrupciones de manera segura y rápida. Las principales amenazas de disponibilidad se relacionan con fallas de software, ataque de denegación de servicio, virus o malware, cortes de energía, riesgos ambientales, fallas de hardware, etc.
- ***Auditabilidad:*** Propiedad que define la capacidad de hacer seguimiento de las acciones realizadas en el activo (quién hizo, qué, cuándo y el origen). Muchas entidades reguladores establecen esta propiedad como requisito fundamental para ser evaluado en la gestión de activos de información de las empresas, ya que permite detectar errores, no cumplimiento de políticas, modificaciones no autorizadas, y mal uso de privilegios de los usuarios con acceso al activo. Esta propiedad depende directamente de la responsabilidad de los individuos sobre sus acciones en los activos.

2.6.2. Administración de seguridad y controles.

La organización debe designar quienes son los dueños de la información, los cuales tienen la responsabilidad de validar que usuarios pueden acceder a sus activos, y que privilegios pueden tener una vez que el acceso haya sido otorgado. El responsable designado de la seguridad en la organización debe velar por que esos objetivos sean cumplidos implementando los controles necesarios. Los controles de acceso se definen en tres categorías que corresponden a tres capas de protección:

Controles Administrativos: Son aquellos que implican desarrollo y publicación de políticas, implementación de procedimientos de control de cambio, gestión de riesgo, conducir el entrenamiento de sensibilización al personal, etc.

Controles técnicos: Estos consisten en implementar y mantener mecanismos de control de acceso, gestión de claves, métodos de identificación y autenticación, configuración de la infraestructura.

Controles físicos: Estos conllevan el control de acceso de personas a las instalaciones, la protección del perímetro de estas, el monitoreo de intrusiones y controles ambientales.

Estos controles y su relación con los activos de la empresa se ilustran en la Figura 5.

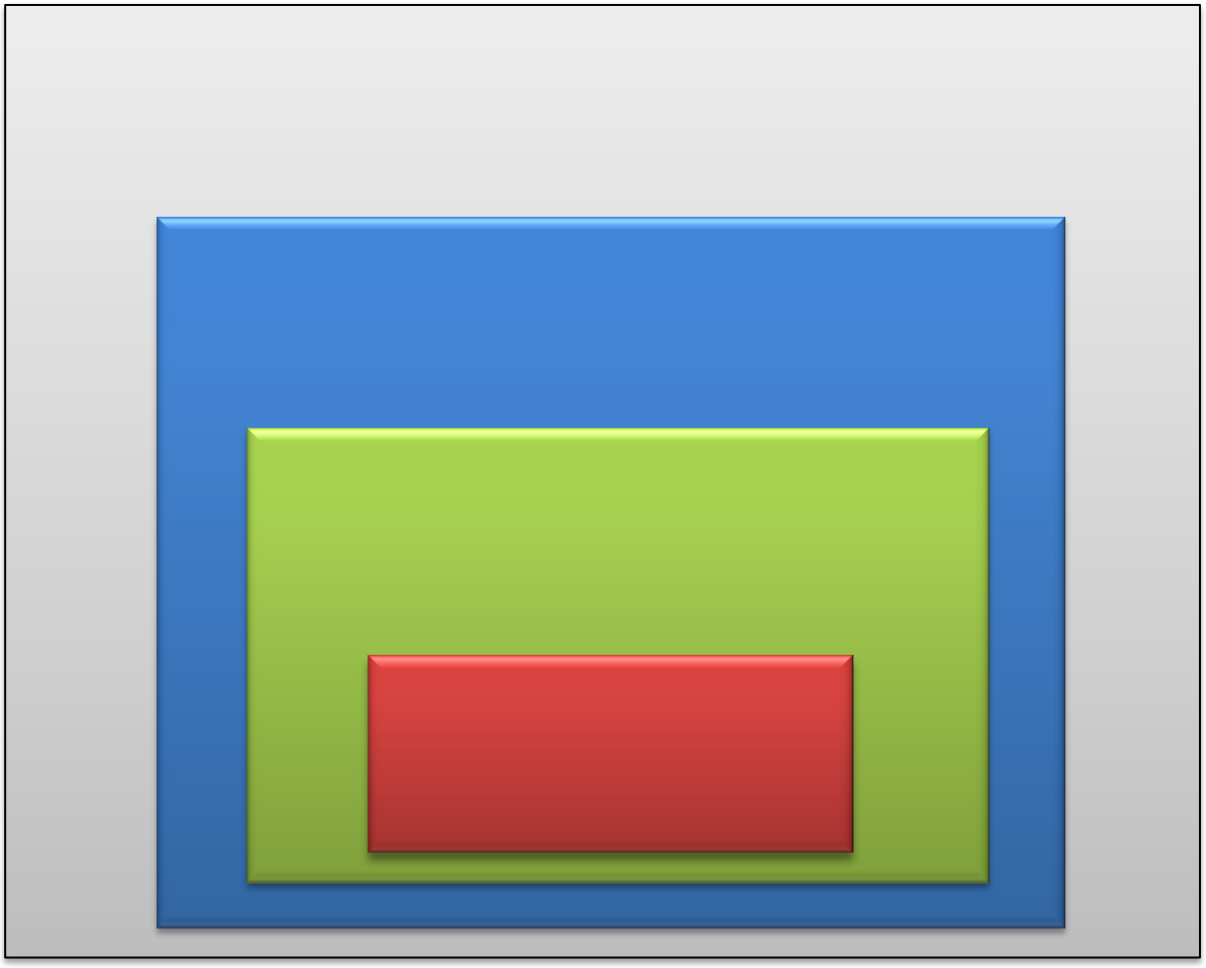

Figura 5. Tipos de controles para proteger los activos de la empresa.

A su vez también cada control trabaja a diferentes niveles de granularidad, como también realizar distintas funcionalidades. Las diferentes funcionalidades de los controles son:

- ***Disuasivo:*** Destinado para desalentar a un potencial atacante
- ***Preventivo:*** Destinado para evitar que ocurra un incidente.
- ***Correctivo:*** Correcciones de los componentes o sistema después que un incidente ha ocurrido.
- ***Recuperación:*** Destinado para traer de vuelta a la operación normal.
- ***Detectivo:*** Ayuda a identificar una actividad relacionada con un incidente.

- ***Compensatorio:*** Controles que proveen una medida alternativa de control.
- ***Directivo:*** Controles mandatorios que han sido implementados debido a requerimientos regulatorios o ambientales.

Para administrar adecuadamente la seguridad es necesario definir los roles y las responsabilidades correspondientes en la organización, algunos roles principales son:

- ***Dueño de la información:*** Es usualmente miembro de la gerencia que está a cargo de una unidad de negocio, quien es el último responsable de la protección y uso de la información. Esta persona también es responsable de que los controles necesarios de seguridad estén en su lugar, definiendo los requerimientos para la clasificación y respaldo de información, asegurando que los privilegios sean correctos y definiendo los criterios de acceso de los usuarios. El dueño de la información aprueba requerimientos de acceso y puede escoger delegar esta función a los jefes de las distintas unidades bajo su cargo. El dueño de la información siempre es quien debe enfrentar las violaciones de seguridad a los activos que debe proteger.
- ***Custodio de la información:*** Es el responsable de mantener y proteger la data. Este rol es generalmente entregado al departamento de TI o al de seguridad, y debe llevar a cabo los respaldos, validar periódicamente la integridad de la data, restaurar información de los respaldos, y satisfacer los requerimientos definidos por los dueños de la información y en las políticas y/o estándares de seguridad establecidos.
- ***Dueño de sistema:*** Este es responsable por uno o más sistemas, los cuales pueden sostener y procesar información de varios dueños de información. También es responsable de integrar las consideraciones de seguridad en aplicaciones y proyectos de desarrollo. El dueño de sistema es responsable que se apliquen los controles de seguridad necesarios, gestión de claves, acceso remoto, configuraciones del sistema operativo, etc. Este rol debe asegurarse que el sistema

tenga sus vulnerabilidades adecuadamente evaluadas y debe reportar cualquier incidente al dueño de la información.

- ***Dueño de proceso:*** Es aquel que es responsable de definir, monitorear y evaluar mejoras en un proceso de negocio. Un dueño de proceso no necesariamente pertenece a una unidad específica de negocio o es el dueño de una aplicación, ya que muchas veces los procesos complejos de negocio son transversales en la organización en términos de personas, tecnología e información.
- ***Oficial de seguridad:*** Es el responsable de entender los riesgos que la compañía encara y de mitigar los mismos a un nivel aceptable. Este rol es responsable de entender los conductores del negocio y de crear y mantener un programa de seguridad que soporte y facilite esos conductores, entregando seguridad, cumplimiento con los requerimientos legales y regulatorios, los requerimientos de los clientes y las obligaciones contractuales. Su labor va más allá de los limites de TI, reportando a la alta gerencia con un enfoque holístico del negocio y la seguridad.
- ***Administrador de seguridad:*** Este rol es quien tiene privilegios de administrador en los sistemas. Este rol debe asegurar que los usuarios tengan privilegios de acceso que cumplan con las políticas de seguridad y las directivas de acceso entregadas por el *dueño de la información*.
- ***Analista de seguridad:*** Este rol trabaja a un nivel estratégico del programa de seguridad ya que es el que ayuda a desarrollar las políticas, las líneas guía, y líneas base. Esta persona trabaja más a un nivel de diseño que de implementación.
- ***Usuario:*** El usuario es aquel que trabaja día a día con el sistema o activo de información. Este debe tener un nivel apropiado de acceso para realizar sus tareas, siendo responsable de seguir los procedimientos operacionales de seguridad establecidos.

2.6.3. Estándares de seguridad.

El desarrollo y despliegue de un programa de seguridad no es tan complejo como muchas organizaciones pueden creer, pero representa nuevos desafíos que muchas

veces traen consigo un cambio de enfoque en la estructura y elementos culturales de las empresas. Es por esto que se hace necesario emplear como referencia los estándares y buenas prácticas de la industria, muchos de los cuales traen la guía y la receta para implementar y mantener un programa de seguridad en la organización, a continuación revisaremos las más importantes.

Cobit (Control Objetives for Information and related Technology) es un marco de trabajo desarrollado por ISACA (Information Systems Audit and Control Association) y el ITGI (IT Gobernance Institute), el cual posee una cantidad de objetivos y metas para administrar apropiadamente las TI y asegurar que su gestión se encuentre alineada con siete objetivos de negocio: Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento y Confiabilidad. El modelo entregado por Cobit se divide en cuatro dominios:

- Planificar y Organizar.
- Adquirir e Implementar.
- Entrega y Soporte.
- Monitoreo y Evaluación.

Por ejemplo Adquirir e Implementar posee las siguientes subcategorias:

- Adquirir e Implementar Software de Aplicaciones.
- Adquirir e Implementar Infraestructura Tecnológica.
- Desarrollar y Mantener Procedimientos.
- Instalar y Acreditar Sistemas.
- Gestión de Cambios.

Así este dominio trae metas y objetivos para cuando la organización compre, instale, pruebe y certifique productos de TI. Esto es relevante para la mayoría de las empresas, producto que muchas usan un enfoque ad-hoc e informal cuando realizan actividades de esta naturaleza.

El modelo de Cobit es la fuente empleada por muchos auditores de sistemas, para establecer los criterios con los cuales evalúan la eficiencia de los controles implementados, es importante estar familiarizado con su contenido si la organización está próxima a una auditoria de esta naturaleza. La figura 6 nos muestra los componentes de Cobit y como conecta los objetivos del negocio junto con los recursos y procesos de TI:

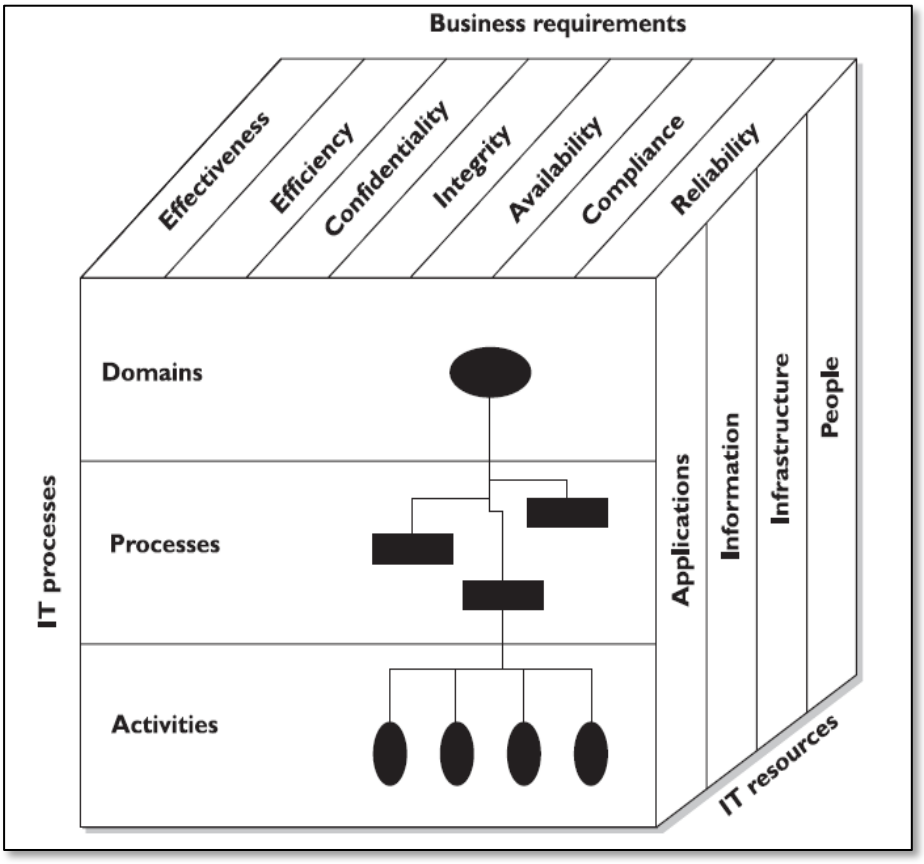

Figura 6. Marco de Cobit.

Cobit fue derivado de COSO[3] (Comitte of Sponsoring Organizations of the Treadway Comission), el cual es una iniciativa de organizaciones del sector privado

[3] Coso fue creado en 1985 en Estados Unidos como sponsor de la Comisión Nacional en el Reporte del Fraude Financiero, para estudiar los factores que pueden llevar a este tipo de fraude.

norteamericano para liderar el desarrollo de marcos de trabajo aplicables a la gestión del riesgo corporativo, el control interno y la disuasión de fraudes.

Los componentes de COSO son:

- ***Controles ambientales.***
    - Filosofía de la gerencia y estilo operativo.
    - Cultura de la compañía con respecto a la ética y el fraude.
- ***Evaluación de riesgos.***
    - Establecimiento de objetivos de riesgo.
    - Habilidad para manejar los cambios internos y externos.
- ***Actividades de Control.***
    - Políticas, procedimientos y las prácticas empleadas para mitigar riesgos.
- ***Información y comunicación.***
    - Estructura que asegure que la información correcta le llegue a la gente correcta, en un tiempo adecuado.
- ***Monitoreo.***
    - Responder y detectar deficiencias en los controles.

La diferencia entre COSO y Cobit es que el primero tiene una orientación mas estratégica del negocio estableciendo los principios del Control Interno en la organización, mientras que el segundo tiene una orientación operativa, COSO es gobierno corporativo mientras que Cobit es gobierno de TI.

La ISO 17799 es el estándar más usado por la industria, el cual fue derivado del estándar británico BS7799. Es un estándar de reconocimiento internacional para la gestión de seguridad de la información. Una organización debería certificarse contra la ISO 17799 para entregar confianza a sus clientes y socios, sirviendo también como una

herramienta de posicionamiento en el mercado. Los dominios cubiertos por el estándar ISO 17799 son los siguientes:

- ***Política de seguridad de la información en la organización*:** Mapa de objetivos para la seguridad, soporte de la gerencia, metas de seguridad, y responsabilidades.
- ***Creación de una infraestructura de la seguridad de la información:*** Crear y mantener una estructura organizacional para la seguridad, con comités de seguridad, proceso de autorizaciones, tercerización, y revisiones independientes.
- ***Clasificación y control de activos:*** Desarrollar una infraestructura de seguridad para proteger los activos organizacionales a través inventario de activos, clasificación y procedimientos de manejo.
- ***Seguridad del personal:*** Reduce riesgos inherentes a las personas a través del proceso de selección del personal, definición de responsabilidades de seguridad en los cargos y entrenamiento adecuado de seguridad para los empleados.
- ***Seguridad física y ambiental:*** Protege los activos de la organización escogiendo las instalaciones adecuadas, implementando perímetros de seguridad, con controles de acceso y protección del equipamiento.
- ***Gestión de la operación y comunicaciones:*** Llevar a cabo operaciones seguras a través de procedimientos operacionales, un apropiado control de cambios, manejo de incidentes, separación de responsabilidades, plan de la capacidad, administración de la red y manejo de medios.
- ***Control de Acceso:*** Controlar el acceso a los activos en virtud de los requerimientos de negocio, gestión de usuarios, métodos de autenticación y monitoreo.
- ***Mantención y Desarrollo de sistemas:*** Implementar seguridad en todas las fases del ciclo de vida de los sistemas a través del desarrollo de requerimientos de seguridad, procedimientos criptográficos, de integridad y para el desarrollo de software.
- ***Gestión de la continuidad de negocios:*** Contrarrestar interrupciones de la operación normal a través de planes y procedimientos de recuperación.

- ***Cumplimiento:*** Cumplir con los requerimientos regulatorios, contractuales, y de estatutos internos a través de controles técnicos, auditorias de los sistemas y entrenamiento del personal en temas relacionados.

La ISO 17799:2005 es la versión nueva de la BS7799 Part I, mientras que la ISO/IEC 27001:2005 es la actualización de la BS7799 Part II. El estándar ISO 27001:2005 provee los pasos para implementar y mantener un programa de seguridad, también conocido como SGSI o Sistema de Gestión de Seguridad de la Información.

ITIL o Information Technology Infraestructure Libraby es el estándar que entrega las mejoras practicas relacionadas con la gestión de los servicios de TI, siendo un marco de trabajo personalizable que es entregado en un set de libros en línea. Se complementa con Cobit, dando los pasos a nivel de proceso para alcanzar los objetivos delineados por este ultimo. Aunque ITIL tiene un componente de seguridad, su enfoque es para establecer acuerdos internos de nivel de servicio entre el departamento de TI y las otras áreas de la organización. La Figura 8 nos muestra los dominios cubiertos por ITIL y la relación que establece entre el negocio y la tecnología que lo soporta.

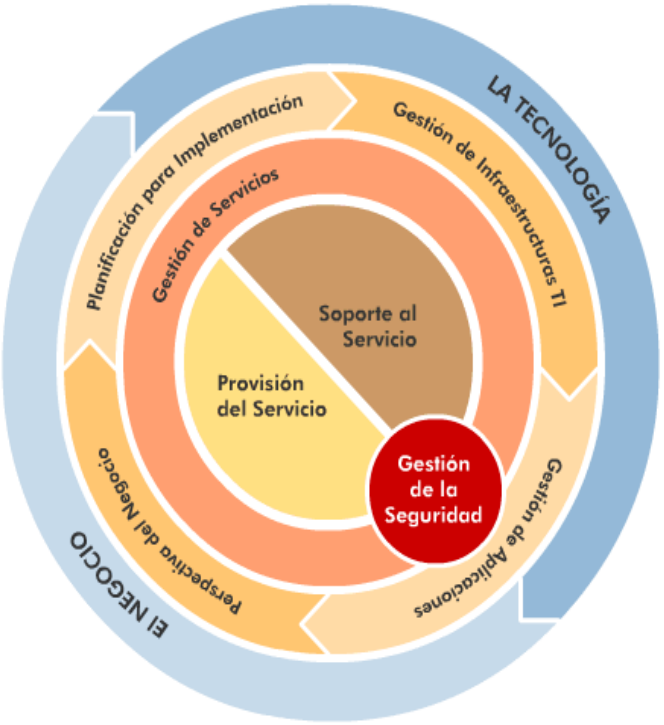

Figura 8. La librería de ITIL en virtud del Negocio y la Tecnología.

2.6.4. Desarrollo de un programa de seguridad.

Es importante entender que un programa de seguridad tiene un ciclo de vida que es siempre continuo, por lo que debería ser constantemente evaluado y mejorado. Si no se toma este enfoque para abordar una iniciativa de seguridad, solo seria tratada como otro proyecto con fecha de inicio y fecha de término, perdiendo su efectividad para proteger los activos de la organización. En líneas generales un programa de seguridad está compuesto por las siguientes fases y componentes, aunque la aplicación de estas últimas depende de los requerimientos y riesgos de cada organización:

- ***Planificar y Organizar.***
    - Establecer compromiso de la Gerencia
    - Establecer un comité con la supervisión de la dirección de la empresa.
    - Evaluar los conductores del negocio.
    - Llevar a cabo una evaluación de amenazas de la organización.
    - Llevar a cabo una evaluación de riesgos.
    - Identificar controles.
    - Obtener aprobación de la gerencia para seguir adelante.
- ***Implementar.***
    - Asignar roles y responsabilidades.
    - Desarrollar políticas, líneas bases, procedimientos y estándares.
    - Identificar la información sensible en tránsito y almacenada.
    - Implementar los siguientes procesos:
        - Identificación y gestión de activos.
        - Gestión de Riesgos.
        - Gestión de Vulnerabilidades.
        - Cumplimiento.

        - Gestión de identidad y control de acceso.
        - Control de cambio.
        - Ciclo de vida de desarrollo.
        - Plan de continuidad de negocios.
        - Entrenamiento y sensiblización.
        - Seguridad física.
        - Respuesta de incidentes.
    - Implementar las soluciones por cada proceso.
    - Desarrollar planes de auditoría y monitoreo para cada proceso.
    - Establecer metas, SLA y métricas para cada proceso.
- ***Operar y Mantener.***
    - Medir que todas las líneas bases se cumplan en los procesos implementados.
    - Llevar a cabo auditorías internas.
    - Administrar las actividades de cada proceso.
    - Administrar los SLA definidos en cada proceso.
- ***Monitorear y Evaluar.***
    - Revisión de logs, resultados de auditoría interna, de los valores de las métricas y de los SLA.
    - Evaluar el cumplimiento de cada proceso.
    - Llevar a cabo reuniones trimestrales con los comités ejecutivos.
    - Desarrollar objetivos de mejoras e integrarlos en la fase *Planificar y Organizar.*

Para implementar los procesos necesarios dentro del programa se debería tomar en cuenta las mejores prácticas de la industria, como las contenidas en la ISO 17799 y la ISO 27001.

2.7. Proceso de gestión de riesgos.

La gestión de riesgos es una parte esencial de la gestión estratégica de cualquier empresa. Es el proceso por el que las empresas tratan los riesgos relacionados con sus actividades, con el fin de obtener un beneficio sostenido en cada una de ellas y en el conjunto de todas las actividades.

La gestión de riesgos de la información es el proceso que identifica y evalúa los riesgos relacionados con los activos de información, reduciéndolos a un nivel aceptable de acuerdo a la tolerancia y apetito de riesgos de la organización, junto con la implementación de los mecanismos adecuados para mitigarlos. Cada ambiente tiene factores de riesgos internos y externos que potencian la aparición de amenazas que deben ser identificadas y cubiertas permanentemente por la gestión de riesgos de una organización. La Figura 9 muestra las etapas del proceso:

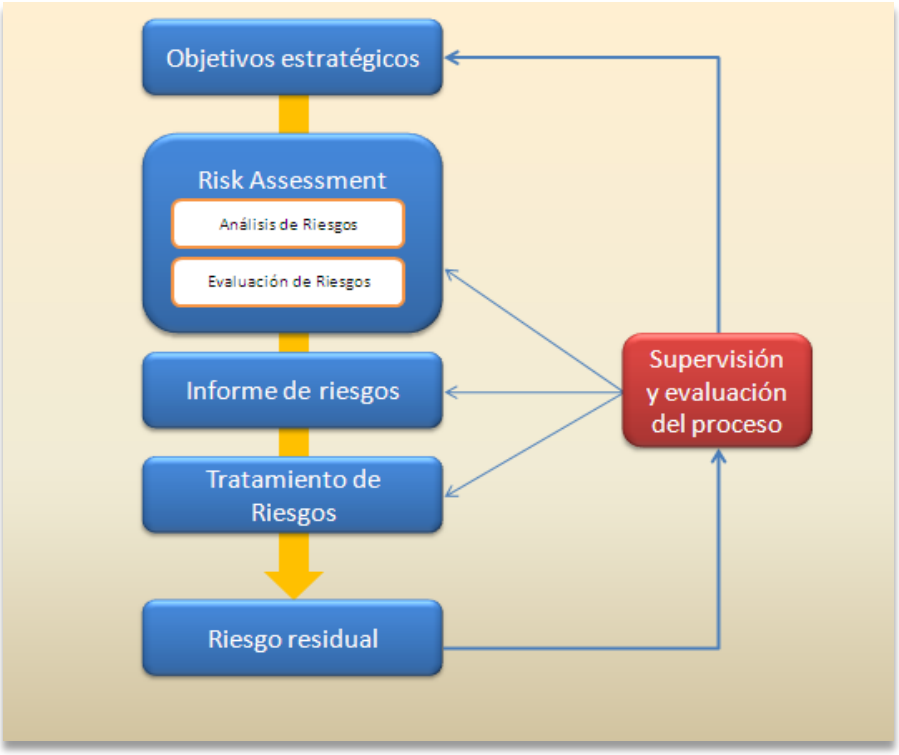

Figura 9. Visión macro del proceso de Gestión de Riesgos.

2.7.1. Análisis y Evaluación de riesgos.

Esta etapa del proceso de gestión de riesgos es crítica, siendo necesario adoptar una metodología adecuada para llevarlo a cabo. Una metodología de evaluación de riesgos establece las reglas para realizar la evaluación, definir quién necesita involucrarse, establece el criterio para cuantificar y cualificar el riesgo, y la información que necesita ser recolectada para el análisis. El objetivo de esta metodología es entregar una medición objetiva de los riesgos sobre los activos críticos de información, dando las herramientas necesarias para tomar las decisiones de negocio relacionadas con la inversión en términos de personas, procesos y tecnología para llevar los riesgos a un nivel aceptable. Algunas de las metodologías que nos ofrece la industria son:

- OCTAVE (Operattionaly Critical Threat Asset and Vulnerability Evaluation) en su versión completa y Allegro, desarrollada por la universidad Carnegie Mellon.
- La metodología del NIST (US National Institute of Standard and Technology) difundida en su publicación NIST 800-03.
- La metodología RisK IT de ISACA, la cual se basa en Cobit.
- El estándar ISO 27001:2008 basado en los estándares ISO 27001 y 27002.

Cualquiera sea la metodología escogida los pasos del análisis y evaluación de riesgos son:

1. ***Identificar los activos y los interesados (Stakeholders):*** Con los activos se delinea el alcance del análisis y los interesados serán los dueños del proceso de negocio quienes conocen los activos críticos y su valor para la organización.
2. **Analizar Impacto:** Medir el impacto, asumiendo que el activo sea comprometido en virtud de su confidencialidad, integridad y disponibilidad. Describiendo la magnitud como Alta, Media o Baja.
3. ***Identificar Amenazas:*** Identificar las maneras por las cuales un activo seria comprometido en el negocio. La herramienta empleada es el escenario de riesgo, donde se indican los actores, la motivación y las rutas por las cuales podría comprometerse el activo.

4. ***Investigar Vulnerabilidades:*** A través de las amenazas encontradas se analizan los controles implementados y las debilidades que podrían facilitar el que se concreten los riesgos.
5. ***Analizar controles:*** Identificar los controles implementados en torno al activo para evaluar su nivel de protección.
6. ***Calcular la probabilidad:*** De acuerdo a la información recabada se analiza la probabilidad de que la amenaza se concrete, considerando el actor, la motivación, las vulnerabilidades y la efectividad de los controles implementados para proteger el activo. La probabilidad se entrega como Alta, Media o Baja.
7. ***Calcular la Magnitud del Riesgo:*** El cálculo de la magnitud del riesgo combina el impacto de negocio si el activo es comprometido, con el efecto sobre los requerimientos de Confidencialidad-Integridad-Disponibilidad del activo, y la probabilidad de que la amenaza se concrete.

2.7.2. Midiendo la magnitud el riesgo

Existen dos maneras de medir el riesgo: con el análisis cuantitativo y con el análisis cualitativo, el primero usa cálculo de riesgo para predecir el nivel de pérdida monetaria y el porcentaje de probabilidad para cada tipo de amenaza, mientras que el segundo no usa cálculos empleando opinión y análisis basados en escenarios. Ambas tienen sus pros y sus contras y se aplicarán mejor en algunas situaciones que en otras.

Análisis Cuantitativo: Este análisis intenta asignar números reales y significativos a todos los elementos del análisis de riesgos. Estos elementos pueden incluir costos de los controles, valor de los activos, impacto financiero, probabilidades de ocurrencia, etc. Como resultado de un análisis cuantitativo deberíamos obtener:

- Valor monetario asignado a los activos.
- Lista exhaustiva de todas las amenazas significativas.
- Una medición matemática para la probabilidad de cada amenaza.

- Perdida potencial que la empresa puede soportar por amenaza considerando períodos de 12 meses.
- Controles recomendados.

Algunos parámetros del análisis cuantitativo son:

- ***ARO (Annualized rate of ocurrence):*** Es el valor que representa la frecuencia estimada de ocurrencia de una amenaza específica en el período de un año, la fórmula matemática sería *frecuencia estimada / años*, por ejemplo: la probabilidad de un tsunami en la zona de Lampa es de 1 vez en 1000 años, por lo tanto su ARO tiene un valor de 0.001 (1 / 1000).
- ***SLE (Single loss expectancy):*** Es un monto en dinero que es asignado a un solo evento que representa una pérdida potencial para la compañía si una amenaza específica se concreta. Se calcula con la siguiente fórmula:

Valor del activo x Factor de exposición (FE) = SLE

- ***FE (Factor de exposición):*** Representa el porcentaje de pérdida que una amenaza provocaría en un activo.
- ***ALE (Annualized loss expectancy):*** Es la pérdida monetaria esperada de un evento en un período de 12 meses:

SLE x Annualized rate of occurrence (ARO) = ALE

Análisis Cualitativo: Este análisis no incorpora números ni valor monetario a las pérdidas. En lugar de eso se examinan diferentes escenarios de riesgos, se categorizan las amenazas según su seriedad y se validan diferentes propuestas de controles en virtud de opiniones de expertos. Los parámetros y el riesgo se miden en términos de Bajo, Medio, Alto y Muy Alto o Extremo según puntuaciones asignadas.

El resultado del análisis debería entregar un mapa de riesgos, como el indicado en la Figura 10, que muestre gráficamente la magnitud de los mismos en virtud de la probabilidad y el impacto. El mapa de riesgos es una herramienta útil para la toma de decisiones con respecto a la respuesta al riesgo, producto que señala de manera gráfica y directa cuales son los riesgos que deberían tener acción inmediata.

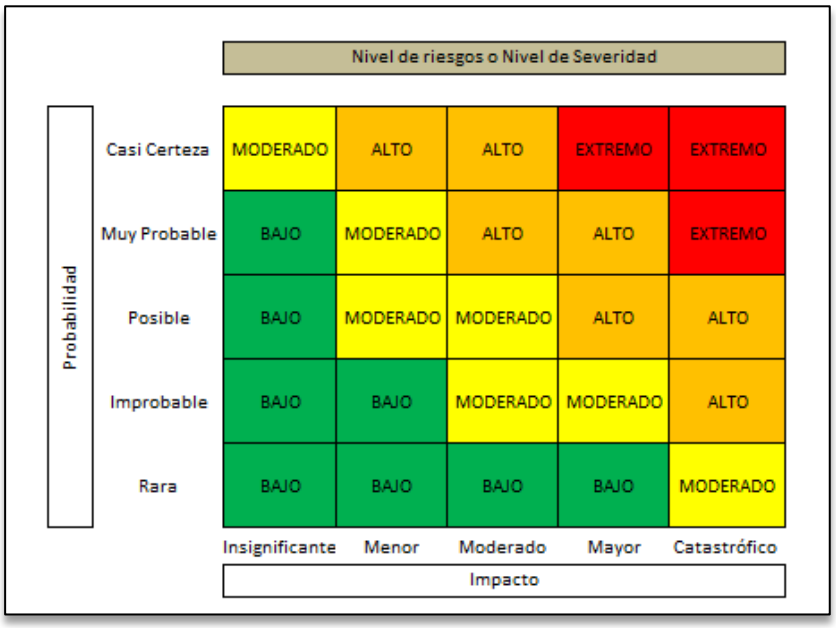

Figura 10. Ejemplo de un mapa de riesgos

2.7.3. Tratamiento de los riesgos.

El tratamiento de los riesgos consiste en la respuesta que la dirección de la empresa decidirá tomar ante los riesgos evaluados por el proceso de Análisis y Evaluación de Riesgos. Esta respuesta al riesgo se genera muchas veces cuando un riesgo supera los umbrales de tolerancia al riesgo de la organización.[4]

La priorización de la respuesta al riesgo y del desarrollo de un plan de tratamiento de riesgo es influenciada por varios elementos:

[4] La tolerancia al riesgo se explica en el glosario de este trabajo.

- Costo de la respuesta para reducir el riesgo a un nivel aceptable.
- Importancia del riesgo.
- Capacidad de implementar la respuesta.
- Efectividad de la respuesta.
- Eficiencia de la respuesta.

No todos los riesgos pueden ser direccionados al mismo tiempo y puede tomar una inversión considerable contenerlos. Los riesgos con una probabilidad y un impacto mayor serán priorizados en vez de los riesgos que son considerados menos probables o de menor impacto. Las alternativas para responder al riesgo son:

- ***Evitar el riesgo:*** Evitar el riesgo significa que las actividades o condiciones que dan lugar al riesgo son descontinuadas. Esta respuesta aplica cuando el nivel de riesgo, incluso después de seleccionar los controles, sería más grande que el nivel de tolerancia de la organización.
- ***Mitigar el Riesgo:*** Mitigación del riesgo significa que se toman acciones para reducir la probabilidad y/o impacto del riesgo. Para mitigar un riesgo se deben integrar adecuadamente todos los tipos de controles (administrativos, técnicos y físicos).
- ***Aceptar el Riesgo:*** Aceptación del riesgo significa que no se tomaran acciones relativas a un riesgo particular, es decir que se aceptan las pérdidas si el riesgo se concreta.
- ***Transferir el Riesgo:*** La transferencia del riesgo significa que el impacto es reducido transfiriendo o compartiendo una parte del riesgo con una organización externa o con otra entidad interna. Ejemplo: tomar un seguro para cubrir desastres o incidentes, externalizar la operación de un proceso de negocio.

La Figura 11 ilustra las diferentes opciones para responder a los riesgos y los elementos que influirán en la selección de las mismas.

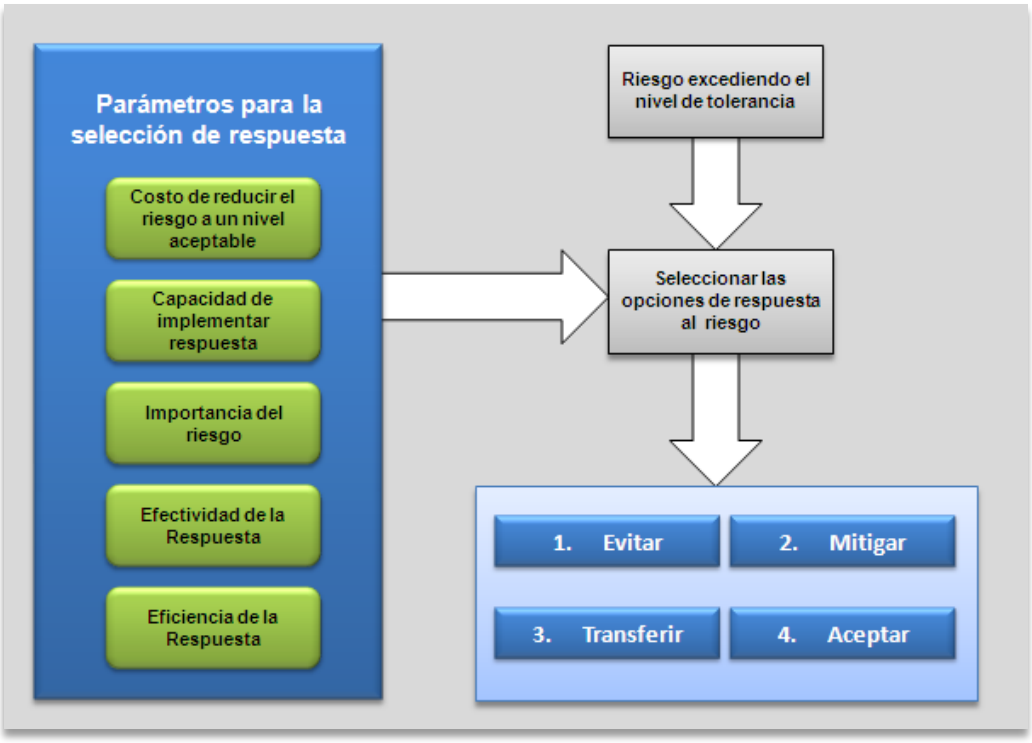

Figura 11. Tratamiento del riesgo

2.8. Metodología OCTAVE Allegro.

OCTAVE (Operattionaly Critical Threat Asset and Vulnerability Evaluation) es una metodología para identificar y evaluar riesgos de seguridad de la información. OCTAVE Allegro es la última actualización esta metodología, desarrollada al igual que sus predecesoras por el Instituto de Ingeniería de Software de la Universidad Carneggie Mellon[5]. Su propósito es entregar una herramienta a las organizaciones que ayude al alineamiento de las actividades de seguridad de la información con las metas del negocio. Su enfoque se orienta hacia los activos de información y al contexto de como ellos son usados, donde son almacenados, transportados, procesados y como ellos son expuestos a las amenazas, vulnerabilidades, y los posibles impactos resultantes.

[5] La Universidad Carneggie Mellon es la institución que también desarrolló el modelo de gestión CMMI.

La metodología consiste en 8 pasos que son explicados en la Figura 12 que se muestra a continuación:

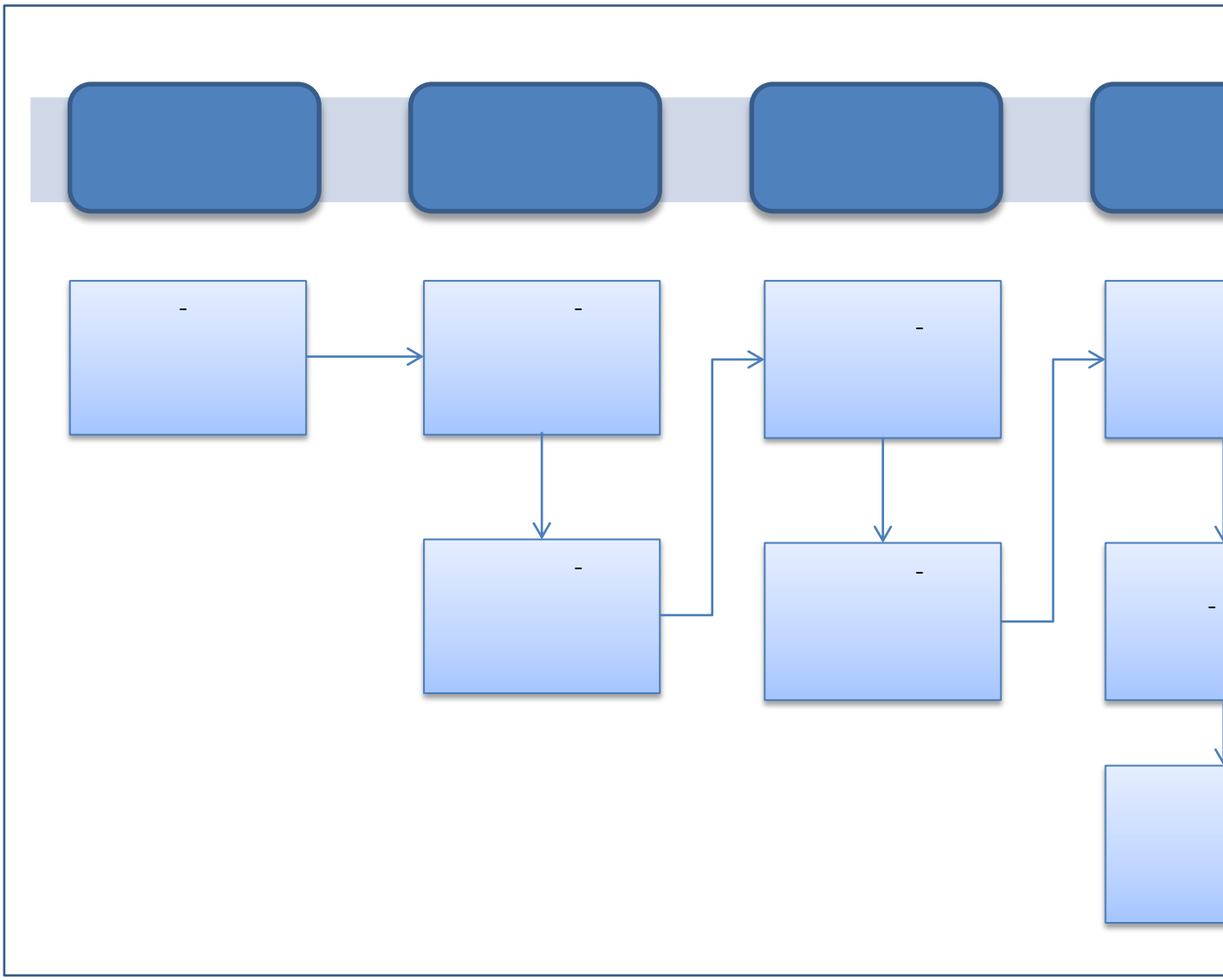

Figura 12. Etapas de la metodología OCTAVE Allegro.

Paso 1: Establecer criterio para la medición de Riesgos.

El primer paso en el proceso de OCTAVE Allegro es establecer los conductores de negocio que nos permitirán evaluar los efectos de un riesgo sobre la misión de una organización y sus objetivos. Estos conductores se reflejan en un conjunto de criterios de medición de riesgo que se crean y se registran como resultado de este

primer paso. Los criterios de medición de riesgos son un conjunto de medidas cualitativas en virtud de las cuales los efectos de un riesgo dado pueden ser medidos y formar la base de una evaluación de riesgo sobre los activos de información. Establecer criterios de medición de riesgos que reflejen la visión de la organización, asegura que las decisiones sobre cómo mitigar el riesgo sean consistentes para los múltiples activos de información y las distintas áreas y departamentos de la organización.

Paso 2: Desarrollar el Perfil de los activos de información.

Un perfil es una representación de un activo de información que describe sus características únicas, cualidades, características y valor. La metodología de proceso de perfilado se asegura de que la descripción de un activo es clara y consistente, al igual que sus límites, y que los requisitos de seguridad estén adecuadamente definidos. El perfil de cada activo se captura en una sola hoja de trabajo que constituye la base para la identificación de amenazas y riesgos en las etapas subsiguientes.

Paso 3: Identificar los contenedores de los activos de información.

Los Contenedores son los lugares en que los activos de información son almacenados, transportados y procesados. Los activos de información residen no sólo en contenedores dentro de los límites de una organización, sino que también a menudo en lugares que no están bajo el control directo de la misma. Cualquier riesgo identificado en los contenedores donde están los activos de información, es heredado hacia estos.

Paso 4: Identificar Áreas de Cuidado.

En este paso comienza el proceso de identificación de riesgos por brainstorming acerca de las condiciones o situaciones que pueden poner en peligro los activos de una organización. Estos escenarios del mundo real se refieren como áreas de cuidado y pueden representar amenazas y sus correspondientes resultados no deseados. Estas Áreas de cuidado pueden caracterizar una amenaza que es único en una organización y sus condiciones de funcionamiento. El propósito de este paso no es la captura de una lista completa de todos los escenarios posibles amenazas para la

un activo de información, sino que la idea es captar rápidamente las situaciones o condiciones que vienen inmediatamente a la mente del equipo de análisis.

Paso 5: Identificar escenarios de Amenazas.

En la primera mitad de la etapa 5, las áreas de cuidado capturadas en el paso anterior se expanden en escenarios de amenaza. Pero la información obtenida no necesariamente tiene una consideración fuerte de todas las posibles amenazas de los activos de información de una organización. Por lo tanto, en la segunda mitad de la etapa 5, se amplía el rango de amenazas profundizando en su análisis a través del desarrollo de arboles de amenaza. La Tabla 3 indica una descripción detallada de esta herramienta.

Tipo de Amenaza	Definición
Actores humanos usando medios técnicos.	Las amenazas en esta categoría representan amenazas a los activos de información a través de la infraestructura técnica de la organización o por el acceso directo a un contenedor (activos técnicos) que aloja un activo de información. Es necesaria la intervención directa de una persona y puede ser de naturaleza deliberada o accidental.
Actores Humanos usando acceso físico.	Las amenazas en esta categoría representan amenazas a los activos de información que resultan desde el acceso físico al activo o un contenedor que aloja un sistema de información de los activos. Que requieren la acción directa de una persona y puede ser deliberada o accidental.
Problemas técnicos	Las amenazas en esta categoría son los problemas relacionados con la tecnología y los sistemas. Algunos ejemplos son los defectos de hardware, defectos de software, código malicioso (por ejemplo, virus), y otros problemas relacionados con el sistema.
Otros problemas	Las amenazas en esta categoría son los problemas o situaciones que están fuera del control de una organización. Esta categoría incluye las amenazas de desastres naturales (por ejemplo, inundaciones, terremotos) y riesgos por la falta de infraestructuras críticas (por ejemplo, la fuente de alimentación).

Tabla 3.Clasificación de los tipos de amenazas y su definición.

Paso 6: Identificar Riesgos.

Mientras en el paso 5 se identifican las amenazas, en el paso 6 se identifican las consecuencias para una organización si una de estas se concreta, completando el cuadro de riesgo. Una amenaza puede tener múltiples impactos potenciales sobre una organización. Por ejemplo, la interrupción del sistema de comercio electrónico de una organización puede afectar a la reputación de la organización con sus clientes, así como su posición financiera. Las actividades involucradas en esta etapa aseguran que las diversas consecuencias de riesgo son identificadas.

Paso 7: Analizar Riesgos.

En este paso de la evaluación, se da una medida cuantitativa a la magnitud en que la organización se ve afectada por una amenaza. Esta puntuación de riesgo relativo se obtiene teniendo en cuenta el grado en que la consecuencia de un riesgo afecta a la organización en virtud de las diversas áreas de impacto, y su probabilidad. En otras palabras, si la reputación es más importante para una organización, los riesgos que tienen un impacto en la reputación van a generar mayor puntuación que los riesgos de impactos y probabilidades equivalentes en otra área. Al dar prioridad a estos criterios de impacto, una organización asegura que los riesgos se evalúan en el contexto de sus conductores de negocio.

Paso 8: Seleccionar enfoques de mitigación.

En este paso final del proceso OCTAVE Allegro, las organizaciones deben determinar cuál de los riesgos que han identificado requieren mitigación y desarrollar una estrategia de mitigación para ellos. Esto se lleva a cabo priorizando los riesgos en base a su puntuación de riesgo relativo. Una vez que los riesgos han sido priorizados, las estrategias de mitigación se desarrollan en virtud del valor del activo y sus requisitos de seguridad, sus contenedores, y su entorno operativo en la organización.

2.9. Proceso de Gestión de Continuidad de Negocios.

La última etapa para alcanzar la resiliencia operacional es la gestión de la continuidad operativa y comercial del negocio, la cual junto con los elementos revisados anteriormente conforman una coraza efectiva de la organización para mantenerla protegida de amenazas que impacten su prestigio, su alineamiento con las entidades reguladoras y el cumplimiento con los compromisos y niveles de servicio establecidos con sus clientes.

La gestión de continuidad de negocios es un proceso que al igual que la seguridad y la gestión de riesgos, tiene metodologías y buenas prácticas ya establecidas en el mercado, entre las cuales destacamos:

- El NIST (US National Institute of Standards and Technology) y su publicación 800-34.
- Las buenas prácticas del Disaster Recovery Institute International.
- La base de conocimientos del International Information Systems Security Certification Consortium, Inc., (ISC)²®.
- Los estándares internacionales BS 25999 y la ISO/IEC 27031:2011.

Cualquiera sea la metodología que se adopte, las etapas que generalmente componen la gestión de continuidad de negocios se indican en la Figura 13:

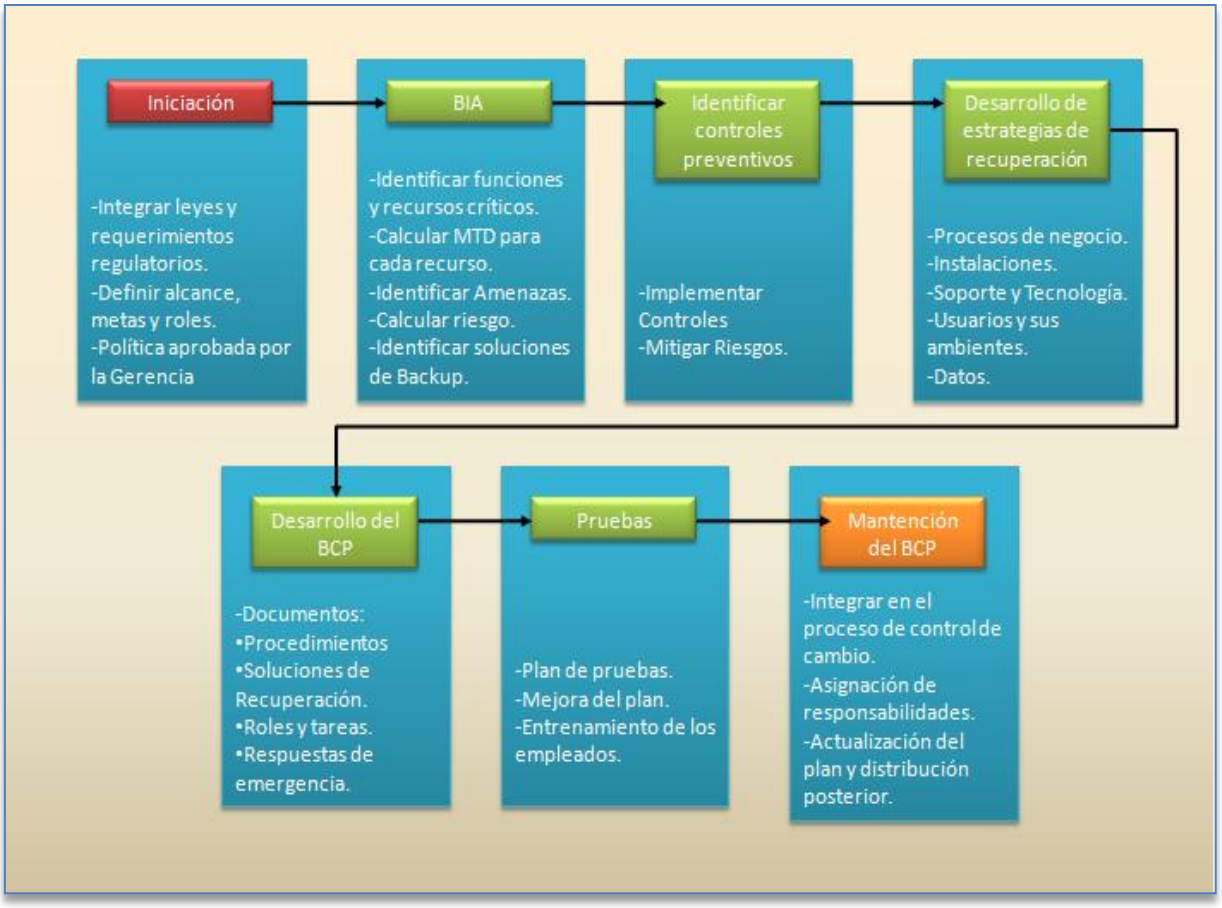

Figura 13. Principales etapas del proceso de BCP y sus actividades respectivas.

2.9.1. Iniciación del proyecto.

En el inicio del proyecto es fundamental designar un encargado o BCP Manager que tenga la responsabilidad de coordinar y conducir todas las actividades del proceso. Para el éxito de la iniciativa el BCP Manager debe trabajar en conjunto con:

- La alta gerencia.
- Las distintas unidades de Negocios.
- El departamento de TI.
- El área de Seguridad.
- El área de Comunicación.
- El área Legal.

Es necesario que la gerencia esté involucrada en el proceso, debido a que es necesario definir las premisas, objetivos y alcances del proyecto, para ser plasmados una política de BCP que será el estatuto que valide la implementación de la iniciativa en la organización.

El BCP Manager debe presentar la iniciativa como un proyecto formal indicando Hitos, el presupuesto estimado, factores de éxito y plazos. El cual debe ser aprobado por la gerencia antes de continuar con los pasos siguientes.

2.9.2. Análisis de Impacto de Negocio (BIA).

El Análisis de Impacto de Negocio es un paso clave en la implementación del proceso. El BIA permite al BCP Manager identificar los procesos de negocio, los componentes de sistema y las interdependencias. El propósito del BIA es correlacionar el sistema con el proceso de negocio crítico y los servicios prestados, y en base a esa información, se analizan las consecuencias de una interrupción. El BIA es una herramienta vital para determinar los requerimientos y prioridades del plan de recuperación. Los pasos típicos que conforman la creación del BIA son:

1) ***Determinar procesos de negocio y su criticidad de recuperación:*** Los procesos de negocio son identificados junto con los sistemas que los soportan, y el impacto de la interrupción para los procesos se determina realizando un risk assesment[6] que considere el impacto de corte y el tiempo de inactividad previsto. El tiempo de inactividad debe reflejar el tiempo máximo que una organización puede tolerar una interrupción sin perjudicar el cumplimiento de su misión.
2) ***Identificar los requerimientos de recursos:*** Los esfuerzos realistas de recuperación requieren una evaluación a fondo de los recursos requeridos para reanudar el proceso de negocio y sus interdependencias en el menor tiempo posible. Ejemplos de estos recursos pueden ser instalaciones, personal, equipamiento, software, datos, etc.

[6] En este paso del BIA es necesario integrar metodologías de análisis de riesgo tales como OCTAVE.

3) ***Identificar prioridades para los recursos de sistema:*** Basado en los resultados de las actividades previas, los recursos de sistema pueden ser enlazados más claramente a los procesos y funciones de negocio. Niveles de prioridad pueden ser establecidos para la secuencia de las actividades y recursos de recuperación, de esta manera los procesos más críticos y sus recursos relacionados serán recuperados en una primera fase y así sucesivamente.

Como resultado del BIA se obtienen tres indicadores fundamentales para continuar con el análisis y para la selección de la estrategia de recuperación:

- ***Máximum Tolerable Downtime (MTD):*** Este elemento se refiere a la cantidad de tiempo total en que la organización junto con su misión y procesos de negocio estará en estado de contingencia.
- ***Recovery Time Objetive (RTO):*** Este elemento se refiere al máximo de tiempo que un proceso de negocio específico puede estar indisponible antes de generar un impacto importante en el negocio. Por definición RTO no puede ser superior al MTD.

- ***Recovery Point Objetive (RPO):*** Representa el punto en tiempo, previo a la interrupción o caída del sistema, para la cual la data del proceso de negocio afectado pueda ser recuperada. En otras palabras es cuanta data estamos dispuestos a perder durante el proceso de recuperación.

2.9.3. Estrategias de recuperación.

Las estrategias de recuperación dependen en gran medida en los requerimientos identificados en el BIA, en términos del RTO y RPO, ya que es necesario tomar en cuenta cuanto es el tiempo que la organización o el proceso podrá estar inactivo y cuanta data podremos perder en la recuperación. En virtud de estos elementos se evalúan tres tipos de estrategias:

- ***Hot site:*** Son instalaciones arrendadas a un tercero que están completamente equipadas listas para funcionar cuando sea requerido. La data es obtenida desde un Sitio de Respaldo. Este tipo de soluciones se aplica a organizaciones que necesitan volver a su funcionamiento normal lo más pronto posible y tienen un gran presupuesto, producto que su implementación requiere muchos recursos.
- ***Warm site:*** Instalaciones arrendadas a un tercero que están parcialmente configuradas con algunos equipos. Es menos costoso que el Hotsite pero el tiempo de recuperación es mayor, producto que es necesario traer e instalar el equipamiento necesario para poder restablecer las operaciones críticas.
- ***Cold site:*** Instalaciones arrendadas a un tercero que no tienen ningún tipo de equipamiento, sólo los elementos de soporte necesarios como cableado y energía eléctrica, cableado de red, aire acondicionado, instalaciones de cañerías, luces, etc. Un sitio de estas características tarda varios días en recuperar los procesos críticos interrumpidos por un desastre. Esta alternativa es la menos costosa.
- ***Redundant site:*** Un sitio redudante es en principio un Hot site pero con la salvedad que las instalaciones son propiedad de la organización. Los datos se mantienen replicados en un sitio de respaldo obteniendo alta disponibilidad de los servicios.

2.9.4. Evaluación de soluciones para la recuperación de datos.

Las alternativas de recuperación de data son las siguientes:

- ***Replicación Síncrona:*** La data original y su copia se mantienen iguales lo que implica una duplicación en tiempo real o alta disponibilidad.
- ***Replicación Asíncrona:*** La data original y su copia se mantienen distintas sólo por pocos segundos, y su replicación se realiza por procesos batch.
- ***Cintas:*** Esta es la alternativa menos costosa pero si la más lenta, producto que es necesario restaurar la data desde cintas de respaldo, con varias horas y a veces días para recuperar la data necesaria.

La Figura 14 ilustra las alternativas de respaldo de la data y su relación costo/tiempo de recuperación.

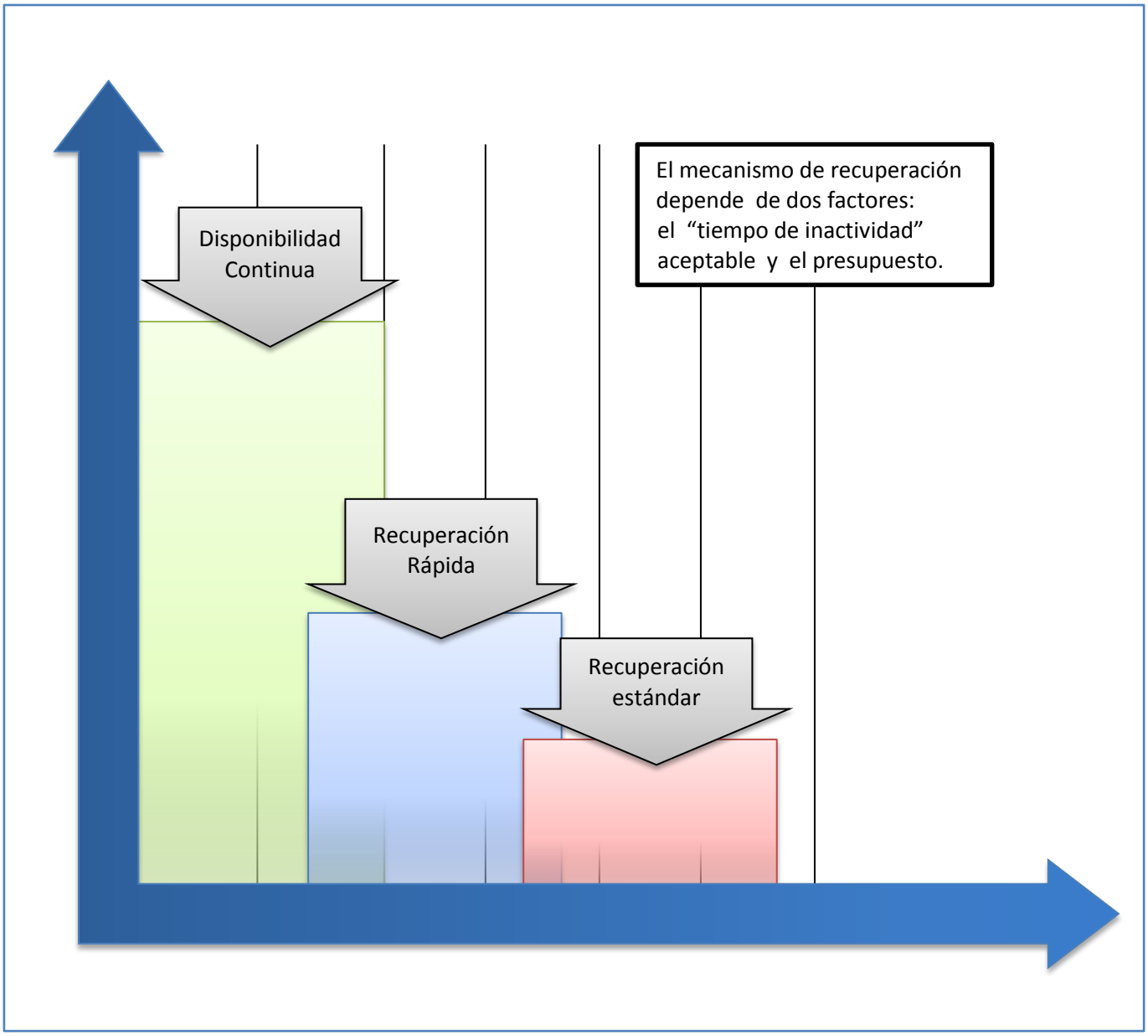

Figura 14. Soluciones de respaldo de data y su relación costo/tiempo de recuperación.

2.9.5. Desarrollo de los planes.

Los principales planes de recuperación que componen el proceso de continuidad operativa se exponen a continuación:

- ***Plan de continuidad de negocios***: Se enfoca en la recuperación de los procesos críticos de negocio en lugar de enfocarse en los elementos de TI.

- ***Plan de continuidad de operaciones***: Establece senior management y una oficina central después de un desastre. Esboza los roles y autoridades, las ordenes de sucesión, y las tareas asignadas a cada rol.
- ***Plan de contingencia de TI***: Plan con los procedimientos de recuperación de los sistemas, redes, y aplicaciones críticas después de una interrupción. Un plan de contingencia debería ser desarrollado por cada sistema crítico de la organización.
- ***Plan de comunicación de crisis***: Establece una estructura para la comunicación interna y externa y los roles asociados. Identifica los individuos específicos que se comunicarán con entidades externas.
- ***Plan de recuperación de desastres***: Establece los procedimientos de recuperación de los elementos de TI en las instalaciones definidas como sitio de recuperación, después de un desastre.
- ***Plan de emergencia***: Establece los procedimientos para la evacuación y seguridad del personal.

2.9.6. Pruebas y revisión de los planes.

El BCP debería ser probado regularmente, tomando en cuenta que el ambiente siempre está cambiando. Las pruebas y los ejercicios de recuperación de desastres deberían llevarse a cabo por lo menos una vez al año, los cuales deberían considerar aquellos escenarios que la compañía podría enfrentar algún día. Algunos tipos de pruebas se indican a continuación.

- ***Prueba de Cheklist:*** En este tipo de prueba, copias del BCP son distribuidas a los diferentes departamentos y áreas funcionales para su revisión. Cada Gerente de área puede revisar los planes para indicar si algo ha sido dejado fuera o si algún elemento debería ser modificado o eliminado.
- ***Prueba estructurada de Walk-Through:*** En este tipo de prueba se invita a delegados de distintos departamentos y áreas funcionales para que todos juntos evalúen el BCP. El grupo revisa los objetivos, discute el alcance, la organización, la estructura de reporte, la mantención y pruebas contempladas. El grupo avanza por

los distintos escenarios del plan desde el inicio al final asegurándose que nada quedó afuera.

- ***Prueba de simulación:*** En esta prueba todos los empleados quienes participan en las funciones operacionales y soporte, o sus representantes, van juntos para ejecutar en la práctica el plan de recuperación de desastres bajo un escenario específico. Este escenario es usado para probar la reacción de cada representante operativo y de soporte. Como en las otras pruebas, esto es hecho para asegurarse que algunos pasos no hayan quedado fuera o que algunas amenazas no hayan sido padas por alto.
- ***Pruebas en paralelo:*** Las pruebas en paralelo son hechas para validar que los sistemas puedan funcionar adecuadamente en el sitio de recuperación de desastres. Los resultados son comparados con el funcionamiento normal de los sistemas sujetos a prueba.
- ***Prueba de interrupción total:*** Se trabaja bajo el escenario de que el sitio principal está caído, por lo tanto todo el procesamiento debe llevarse a cabo en el sitio de contingencia. El equipo de recuperación cumple su obligación en preparar los sistemas y ambientes para el sitio de contingencia. Este tipo de ejercicio requiere bastante de planificación y coordinación, pero puede revelar muchas deficiencias en el plan que necesitan ser corregidas antes que un desastre real ocurra.

La Figura 15 indica la estructura que conforma el documento con el plan de continuidad de negocios en una organización, el cual debe indicar detalladamente las distintas fases que se deben tener en cuenta cuando se declara una catástrofe y se activa el plan.

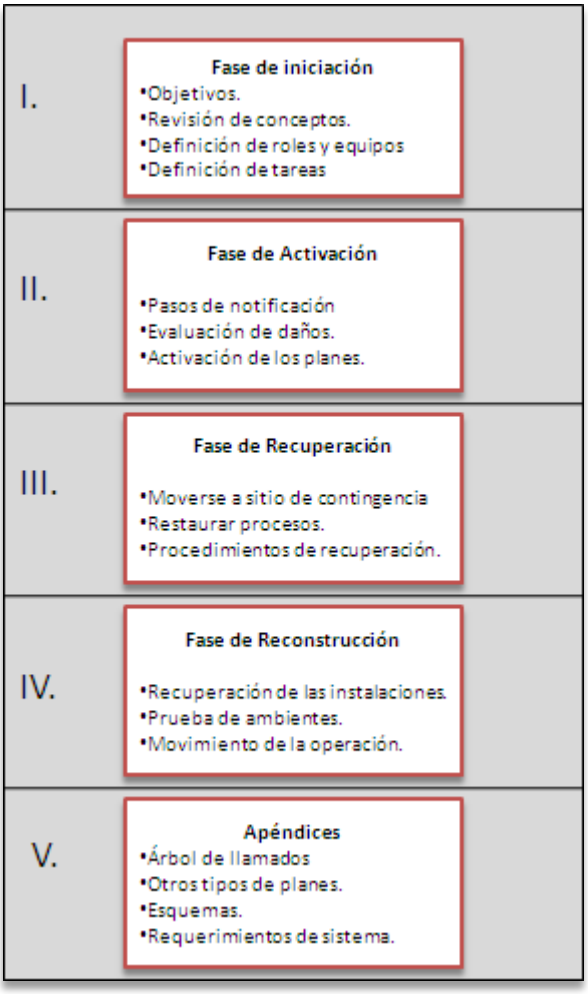

Figura 15. Estructura general del documento que contiene un plan de continuidad de negocios (BCP).

3. DESARROLLO DEL TRABAJO

3.1 Descripción de la problemática.

Para el desarrollo de este trabajo se implementará la iniciativa de resiliencia operativa en una compañía de seguros, la cual tiene como modelo de negocios la banca seguros, es decir, establecer alianza con bancos para vender a las personas sus productos de seguros a través de los créditos, servicios y productos que las entidades bancarias ofrecen a sus clientes, quedando un porcentaje de cada venta en la entidad bancaria (comisiones). Recientemente este modelo se amplió al sector del retail, estableciendo el mismo esquema con las principales casas comerciales del país. Bajo este escenario las entidades con las cuales establezca cada negocio serán llamados “socios”, siendo el principal valor de la compañía la confianza, dado que proporcionando operaciones confiables, seguras y garantizando una alta disponibilidad de los servicios, tiene un elemento contundente a la hora de negociar renovación de contratos y/o establecer nuevos negocios a mayor plazo.

En sus procesos de negocio es fundamental trabajar con las bases de datos con información de los clientes de los socios, en las cuales muchas veces se incluye datos sensible como los medios de pago. Es por esta razón que sus socios bancarios están volviéndose más exigentes en sus requerimientos operacionales, exigiendo un mayor control sobre los riesgos relativos a la seguridad y la tecnología. Es necesario indicar que las entidades bancarias tienen fuertes elementos reguladores del riesgo operacional, como BASILEA II y los requisitos de la SBIF, las cuales están exigiendo a sus proveedores y terceros homologar su marco de control interno y gestión sobre los riesgos, para no generar brechas en la cadena de custodia de los activos de información o caer en incumplimiento de sus propios requerimientos de seguridad.

Por otra parte los clientes del sector retail, quienes también manejan información sensible de sus clientes, es un mercado menos regulado pero si fuertemente

competitivo, es por esta razón que sus requerimientos guardan relación con la disponibilidad de los servicios, tendiendo a requerir servicios de alta disponibilidad con transacciones en línea. Este es el caso del negocio de Extensión de Garantía para aparatos electrónicos, computadores y electrodomésticos, ya que cuando se genera contratación del seguro en la tienda, se debe registrar en el menor tiempo posible el registro de esta operación en los sistemas de la compañía.

Junto con lo indicado en relación a los requerimientos de los socios y clientes, cabe destacar que el mercado de seguros es regulado por la SVS (Súper Intendencia de Valores y Seguros), la cual volviéndose más estricta en algunos de sus requerimientos producto de la apertura económica y su alineamiento con las normativas financieras de Europa y Estados Unidos. Tal es el caso de la norma de carácter general N° 309 de Gobiernos Corporativos y Sistemas de gestión de Riesgos y Control Interno, donde se plantea entre otras cosas que las compañía deben tener una gestión efectiva de su riesgo operacional junto con planes de contingencia que garanticen la continuidad de su operación. En carpeta existen otras normativas orientadas a evaluar la solvencia de las aseguradoras a través de su gestión del riesgo, resultando en que las organizaciones más riesgosas deben aportar mayor capital a su fondo de reserva.

La organización bajo este ambiente donde por una parte tiene expectativas y requerimientos de los socios, junto con los requisitos de la entidad reguladora, se hace mandatorio que tome acciones en virtud de cumplir satisfactoriamente estos conductores de negocio, primero evaluando cual es su situación actual para después comenzar a trabajar sobre sus elementos más críticos. Estas actividades deben obtener el valor estratégico que merecen dentro de la alta gerencia, producto que su realización exitosa indiscutiblemente ayudará a fortalecer la permanencia y crecimiento de la organización en el mercado.

3.2 Iniciación del proyecto.

La dirección de la empresa ha tomado la decisión de implementar una iniciativa de resiliencia operacional en la compañía, y como el elemento predominante a primera vista es la disponibilidad de los servicios se tomará como punto de partida la implementación de un proceso de Gestión de Continuidad de Negocios o BCM (Business Continuity Management) producto que a través de su desarrollo se identifican los procesos críticos de la organización junto con los activos que ayudan al cumplimiento de su misión y objetivos. De esta manera la implementación de controles ser hará de manera eficiente hacia los elementos más críticos de la organización.

La puesta en marcha del proceso se realizará tomando como referencia las buenas prácticas relacionadas, es por esto que el primer paso es designar un ***BCP Manager***, quien será responsable de conducir todas las etapas del proyecto junto con identificar las partes interesadas, definir los procesos y comunicar efectivamente los requerimientos a la dirección y a las distintas áreas involucradas.

3.3 Establecimiento del alcance y premisas.

Esta etapa es fundamental en la implementación del modelo, dado que es donde se identifican los procesos y las áreas de la organización que deberán ser cubiertos por su alcance. En algunos casos podría ser la organización completa, pero esta decisión depende en gran medida del apetito de riesgo de la dirección y de los recursos que estén dispuestos a invertir para una iniciativa de resiliencia operacional. El primer elemento a considerar es la misión de la organización y sus objetivos estratégicos. Para este caso los objetivos de la organización son:

- *Administrar eficientemente todos los negocios de la compañía.*
- *Establecer acuerdos de largo plazo con al menos el 50% de los socios.*

En virtud de los objetivos estratégicos se pueden obtener las premisas del análisis que permitirá definir los procesos que serán cubiertos por el alcance:

- Sólo se consideran las actividades críticas del negocio y todos aquellos procesos que las soportan.
- Sólo se evalúan los riesgos que pueden producir una interrupción seria y repentina de los procesos de negocio.
- Se toma como base de análisis la ocurrencia del peor escenario de catástrofe, *"La inhabilitación completa del negocio por un período de 30 días".*
- Los elementos que serán incluidos por defecto en el alcance serán:
    - Las áreas de TI y de Control Interno por ser soporte obligatorio de todos los procesos críticos.
    - El proceso de pago de remuneraciones.
    - Las instalaciones donde están ubicadas las oficinas.

3.4 Identificación de los Procesos críticos.

De acuerdo a lo definido anteriormente debemos explorar en la cadena de valor de la organización para encontrar los procesos críticos del negocio y determinar cuáles de estos entrarán en el alcance de la iniciativa.

De acuerdo al análisis de los procesos y al impacto de negocio frente al escenario de desastre considerado, se determina que los procesos operativos relacionados con la *Definición y configuración de Productos* quedan fuera del alcance de la iniciativa, considerando los procesos operacionales que tengan que ver con la recaudación, pago de comisiones y la evaluación y liquidación de siniestros, los cuales demandan cumplimiento de plazos con los socios y la entidad reguladora.

Para el propósito del análisis de este trabajo de titulo, de entre los procesos identificados dentro del alcance del modelo BCM, tomaremos el proceso más

representativo para el negocio de seguros: *Proceso de evaluación y liquidación de siniestros*. Dado que este proceso posee todos los requerimientos que serán satisfechos por el modelo propuesto: fuerte regulación para preservar la confidencialidad e integridad de la información sensible de los asegurados, y los plazos definidos por la Super Intendencia de Valores y Seguros para emitir el pago de siniestros y/o las cartas de rechazo a los asegurados solicitando más antecedentes para la evaluación de los mismos.

3.5 Desarrollo del Análisis de Impacto de Negocio (BIA).

Ahora que se determinó el proceso crítico donde comenzaremos a trabajar, se debe confeccionar el Análisis de Impacto de Negocio (BIA) donde se determinarán los elementos relevantes: RTO, RPO, y los activos personas, información y tecnología. Esta labor se debe desarrollar con la gerencia a cargo del proceso.

Análisis de Impacto de Negocio *Proceso: Denuncio y Evaluación de Siniestros*	
Descripción general del proceso	Evaluar la cobertura siniestrada verificando cumplimiento de las condiciones particulares y generando los pagos a los clientes.
RTO: ¿Cuántos días podría estar el área sin ejecutar el proceso sin que se produzca un daño significativo?	2
IMPACTO:¿Cuál sería el impacto financiero que podría producir la no ejecución del proceso? 1- Alto, 2-Medio, 3-Bajo	1
RPO:¿Cuál es el período más corto de información histórica que necesita obligatoriamente tener a disposición para poder ejecutar el proceso?	Últimos 12 meses
¿Cuál es el número de personas asignados a la ejecución y/o validación regular del proceso?	30
¿Cuáles son los roles de las personas asignadas a la ejecución y/o validación del proceso?	Liquidadores, digitadores y Jefatura del área de Siniestros
¿Se encuentra la actividad debidamente documentada y con personal de respaldo asignado en caso de contingencia?	Si
¿Qué aplicaciones de negocio se utilizan para la ejecución del proceso?	Sistema de Siniestros, Sistema Contable, Correo Electrónico, Base de Pólizas.

¿Existen otras aplicaciones de apoyo o directorios necesarias para la correcta ejecución del proceso? (Office, Notes, Access, etc.)	MS Office, Disco de red, Correo Electrónico, Conexión Internet.
¿Existe algún equipamiento, dispositivo o elemento adicional que deba tenerse en cuenta? (fotocopiadora, trituradora, scanner, etc.)	Impresora multifuncional
Criticidad del Proceso (RTO x Impacto)	2

Figura 16. Análisis de Impacto de Negocio con los parámetros fundamentales para determinar la criticidad de las actividades de negocio.

3.6 Inventario de Activos.

Posterior a la definición del proceso crítico y a su análisis de impacto en el negocio, es necesario realizar el inventario y clasificación de los activos que permiten que el proceso cumpla sus objetivos. En el documento se indica una breve descripción de los activos, junto con los requerimientos de seguridad en términos de confidencialidad, integridad y disponibilidad ***(C, I, D)*** y la clasificación resultante. Como premisa todo activo que tenga alto requerimiento de confidencialidad será clasificado como *confidencial*.

Activo	Descripción	Requerimientos de Seguridad			Tipo de activo	Clasificación
		C	I	D		
Expediente de Siniestros	Documentos con la información personal de cada asegurado siniestrado, los cuales permiten realizar la evaluación de los Siniestros. Ej.: Informe médico, certificado de defunción, fotocopia de carnet, cartola de AFP, parte policial, etc.	Alto	Alto	Alto	**Información**	**Confidencial**

Informe de liquidación de Siniestros	Documento que describe el resultado de la evaluación de un siniestro. Incluye los datos del asegurado, las coberturas, los montos a pagar, socio, dictamen, diagnóstico, etc.	Alto	Alto	Alto	**Información**	**Confidencial**
Sistema de Gestión de Siniestros	Sistema Informático que soporta el proceso de evaluación y liquidación de siniestros.	Alto	Alto	Alto	**Tecnológico**	**Confidencial**

Tabla 4. Levantamiento y clasificación de activos.

3.7 Proceso de Evaluación de riesgos.

Dado que ya identificamos los activos críticos para el proceso de negocio escogido, ya podremos realizar nuestra primera evaluación de riesgos. En este caso seguiremos lo planteado por la metodología OCTAVE para llevar a cabo este proceso.

La primera etapa del proceso de evaluación de riesgos es establecer los criterios contra los cuales mediremos los mismos, los criterios fundamentales para iniciar el proceso son priorizar las áreas de impacto del negocio e identificar el nivel de exposición que existe en la organización midiendo la implementación de controles.

3.7.1 Áreas de Impacto.

En la Tabla 5 se presenta la decisión ejecutiva para la priorización de las áreas de impacto, su valorización es directamente proporcional a la criticidad dada en el análisis.

OCTAVE	PRIORIZACIÓN DE LAS ÁREAS DE IMPACTO
PRIORIDAD	**ÁREAS DE IMPACTO**
5	**Reputación y confianza de los clientes**
4	**Financiero**
3	**Productividad**
2	**Legal y multas**
1	**Otra**

Tabla 5. Levantamiento de las áreas de impacto en el negocio y su valor de acuerdo a la prioridad en la organización.

3.7.2 Evaluación de controles y vulnerabilidades.

Antes de proceder con el análisis de riesgos, es necesario identificar como estamos expuestos y donde tenemos las vulnerabilidades, para esto es indispensable alinearse con una base de buenas prácticas madura y con prestigio en el mercado para obtener un punto confiable de referencia para saber “donde estamos”, ejemplo de esto son las normas ISO/IEC 27001-17799.

La evaluación de controles es la manera con la cual identificaremos el nivel actual de protección de los activos, para esto seleccionaremos parte de los 133 controles de la ISO 27001, auditando aquellos identificados como aplicables en la organización tomando en cuenta su nivel de madurez. Cabe destacar que la organización nunca ha realizado este tipo de actividad estando en un nivel 1 de madurez, implicando que muchos procedimientos y controles son tratados de manera ad-hoc, si una base metodológica que los sustente ni procedimientos documentados.

La evaluación de controles es una medición cualitativa de cumplimiento donde se asignan valores *Alto, Medio o Bajo* en virtud de los siguientes criterios:

Criterio	*Descripción*
Documentación que lo sustente	Todo control de seguridad requiere un estatuto respaldado por la dirección donde se defina como requerimiento. En muchos casos puede ser una política asociada, un estándar, un procedimiento, etc.
Nivel de implementación del control	La implementación y operación de cada control será evaluado contra lo indicado en la ISO/IEC 17799, la cual entrega el detalle de las buenas prácticas asociadas a los controles de la ISO/IEC 27001.
Nivel de Registro	Todo control debe entregar permanentemente evidencias de su operación, por ejemplo: logs de los sistemas, registro de acceso, bitácoras, autorizaciones firmadas, etc.

Tabla 6. Criterios para la medición de controles.

Cumplimiento	*Descripción*	*Puntuación*
BAJO	Cumplimiento insatisfactorio	1,00
MEDIO	Cumplimiento parcial o incompleto	2,00
ALTO	Cumplimiento satisfactorio	3,00

Tabla 7. Parámetros para la asignación de valores según el nivel de cumplimento de los controles.

Posteriormente la evaluación global se obtiene promediando linealmente los tres valores de cada control según su nivel de cumplimiento con la norma ISO 27001.

DOMINIO	*CONTROLES*		*Documentado*		*Implementado*		*Registrado*		*Evaluación global*
			Descripción	*Valor*	*Descripción*	*Valor*	*Descripción*	*Valor*	
POLITICA DE SEGURIDAD	**A.5.1.1**	El documento de la política de seguridad de la información debiera ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.	No existe una Política de seguridad formal	**1**	No existe el control	**1**	No existen registros	**1**	**1**

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	**A.6.1.1**	La gerencia debiera apoyar activamente la seguridad dentro de la organización	Existe un compromiso de la gerencia pero faltan las políticas formales.	**2**	Es una iniciativa reciente que todavía no es parte de todas las gerencias.	**2**	Actas de reunión de la Gerencia cuando se tomó decisión de implementar la iniciativa.	**3**	**2**
	A.6.1.4	Un proceso de la gerencia para la autorización de facilidades nuevas de procesamiento de información, debiera ser definido e implementado	Existe a nivel informal. No hay procedimiento documentado	**2**	No está formalizado pero las decisiones requieren la autorización del Gerente respectivo.	**2**	No se registran debidamente todas las autorizaciones.	**2**	**2**
GESTIÓN DE ACTIVOS	**A.7.1.1**	Todos los activos sensibles deben ser claramente identificados y mantenidos en un inventario	No existe una Política que defina este requerimiento	**1**	Sólo de manera parcial en algunas áreas.	**2**	Se registra en un inventario de activos	**3**	**2**
	A.7.1.2	Toda la información y los activos asociados con los medios de procesamiento de información debieran ser propiedad de una parte designada de la organización.	No existe una Política que defina este requerimiento	**1**	Sólo de manera parcial en algunas áreas.	**2**	No existen registros asociados	**1**	**1**
	A.7.1.3	Se debieran identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información.	Cumplimiento parcial a través del Manual de higiene y seguridad.	**2**	El control se implementa de manera insuficiente a cada empleado	**2**	El registro es el Manual de Higiene y seguridad	**2**	**2**
SEGURIDAD DE LOS RECURSOS HUMANOS	**A.8.1.1**	Se debieran definir y documentar los roles y responsabilidades de la seguridad de los empleados contratistas y terceros en concordancia con la política de seguridad de la información de la organización.	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**

	A.8.1.3	Como parte de su obligación contractual; los usuarios empleados, contratistas y terceros debieran aceptar y firmar un contrato con los términos y condiciones de su empleo, el cual debiera establecer sus responsabilidades y las de la organización para la seguridad de la información.	Clausula de seguridad en los contratos de trabajo de los empleados y en los contratos con proveedores de servicios externos.	**3**	Todos los empleados y contratistas deben firmar un contrato.	**3**	Contratos firmados	**3**	**3**
	A.8.2.2	Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceras personas debieran recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos organizacionales conforme sea relevante para su función laboral.	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.8.2.3	Debiera existir un proceso disciplinario para los empleados que han cometido un incumplimiento de la seguridad.	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.8.3.3	Los derechos de acceso de todos los usuarios empleados, contratistas y terceras personas a la información y los medios de procesamiento de información debieran ser retirados a la terminación de su empleo, contrato o acuerdo, o debieran ser reajustados de acuerdo al cambio.	No existe una Política que defina este requerimiento	**1**	Se realiza de manera ad-hoc en algunos casos	**2**	Nivel de registro a través de e-mails solicitando eliminación de acceso.	**2**	**2**
SEGURIDAD FÍSICA Y AMBIENTAL	**A.9.1.1**	Se debieran utilizar perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.	Planos de las oficinas contemplan los perímetros de seguridad	**2**	Cumple el control	**3**	Planos de las oficinas firmados por la gerencia	**3**	**3**

	A.9.1.2	Las áreas seguras debieran protegerse mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.	No existe una política formal pero si el requerimiento de la Dirección	**2**	Cumple el control	**3**	Logs de los sistemas de control de acceso	**3**	**3**
	A.9.1.4	Los lugares en donde se manipulen y/o almacenen activos sensibles deberán poseer controles de protección física contra daño por fuego, inundación u otras formas de desastre natural o creado por el hombre.	No existe una política formal pero si el requerimiento de la Dirección	**2**	En la sala de servidores sólo existe un extintor pero no hay detectores de humo ni humedad, su construcción es antisísmica.	**2**	Registro parcial de los equipos	**2**	**2**
	A.9.1.6	El ingreso a sitios en donde se almacenen o manipulen activos sensibles deberá ser controlado y restringido sólo a aquellas personas cuyas funciones requieran hacer uso de los mismos.	No existe una política formal pero si el requerimiento de la Dirección	**2**	Se controla con una llave en poder de soporte y del Gerente de Sistemas	**2**	Existe un libro de visitas a la sala de servidores que no siempre se completa	**2**	**2**
	A.9.2.1	El equipo debe ser ubicado y protegido para reducir los riesgos y amenazas ambientales.	No existe una política formal pero si el requerimiento de la Dirección	**2**	Todos los equipos críticos están en una sala de servidores cerrada	**3**	Inventario de equipos de TI	**3**	**3**
	A.9.2.2	El equipamiento debe ser protegido de los cortes de electricidad y otras fallas en los servicios de soporte.	No existe una política formal pero si el requerimiento de la Dirección	**2**	Existe UPS con autonomía de 30 minutos	**2**	Inventario de equipos de TI	**3**	**2**
	A.9.2.4	El equipamiento debe ser mantenido correctamente para permitir la continua disponibilidad del mismo.	No existe una Política que defina este requerimiento	**1**	Solo algunos equipos poseen contrato de mantención.	**2**	Actas de los técnicos de mantención	**3**	**2**
GESTIÓN DE OPERACIONES Y COMUNICACIONES	**A.10.1.1**	Los procedimientos operativos deben estar documentados, mantenidos y asequibles a todos los usuarios que los necesiten.	No existe una Política que defina este requerimiento	**1**	No existen procedimientos documentados.	**1**	No existen registros.	**1**	**1**
	A.10.1.2	Se debieran controlar los cambios en los medios y sistemas de procesamiento de la información.	No existe una Política que defina este requerimiento	**1**	Control parcialmente implementado	**2**	Registros de pasos a producción	**3**	**2**
	A.10.1.3	Se deben segregar las responsabilidades y deberes de las personas con acceso a los activos sensibles para reducir los riesgos sobre los mismos.	No existe una Política que defina este requerimiento	**1**	No existe segregación de responsabilidad es (el que ejecuta también autoriza)	**1**	No existen registros	**1**	**1**

GESTIÓN DE OPERACIONES Y COMUNICACIONS	**A.10.1.4**	Los medios de desarrollo, prueba y operación debieran estar separados para reducir los riesgos de acceso no-autorizado o cambios en el sistema operacional.	No existe una Política que defina este requerimiento	**2**	No existe el control	**3**	No existen registros	**3**	**3**
	A.10.4.1	Controles contra código malicioso	No existe una política formal pero si el requerimiento de la Dirección	**2**	Existe un producto instalado pero no hay una consola de administración	**2**	No existe un registro centralizado de la herramienta antivirus.	**1**	**2**
	A.10.5.1	Se debieran hacer copias de respaldo de la información y software y se debieran probar regularmente en concordancia con la política de copias de respaldo acordada.	No existe una política formal pero si el requerimiento de la Dirección	**2**	Respaldo de las cintas pero no hay pruebas de recuperación	**2**	Logs del sistema pero no hay informes con resultado del respaldo por parte del operador	**2**	**2**
	A.10.6.2	Características de seguridad, niveles de servicio, y administración de requerimientos de todos los servicios de red deben ser incluidos en cualquier contrato de servicios de red, ya sea para servicios in-house o subcontratados.	No existe una Política que defina este requerimiento	**1**	Sólo algunos proveedores de redes y servicios poseen clausulas solicitadas.	**2**	Los Contratos firmados	**3**	**2**
	A.10.7.1	Debieran existir procedimientos para la gestión de los medios removibles	No existe una Política que defina este requerimiento	**1**	No existen procedimientos documentados	**1**	No existen registros	**1**	**1**
	A.10.7.2	Los medios de almacenamiento deben ser dados de baja en forma segura cuando no sean necesarios.	No existe una Política que defina este requerimiento	**1**	No existe la implementación del control	**1**	no existen registros	**1**	**1**
	A.10.7.3	Se debieran establecer los procedimientos para el manejo y almacenaje de información para proteger esta información de una divulgación no-autorizada o mal uso	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros.	**1**	**1**

	A.10.10.1	Se debieran producir y mantener registros de auditoría de las actividades, excepciones y eventos de seguridad de la información durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.	No existe una Política que defina este requerimiento	**1**	No todos los sistemas poseen logs de auditoria	**2**	Logs de los sistemas habilitados	**2**	**2**
	A.10.10.2	Se debieran establecer procedimientos para el monitoreo del uso de los medios de procesamiento de la información y se debieran revisar regularmente los resultados de las actividades de monitoreo.	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros.	**1**	**1**
	A.10.10.4	Las actividades del administrador y operador del sistema deben ser registradas.	No existe una Política que defina este requerimiento	**1**	No todos los sistemas poseen logs de auditoria	**2**	Logs de los sistemas habilitados	**2**	**2**
CONTROL DE ACCESO	**A.11.1.1**	Se debiera establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad para el acceso	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.11.2.1	Debiera existir un procedimiento formal para el registro y des-registro del usuario para otorgar y revocar el acceso a todos los sistemas y servicios de información	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.11.2.2	Se debiera restringir y controlar la asignación y uso de privilegios	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.11.2.3	La asignación de claves secretas se debiera controlar a través de un proceso de gestión formal	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.11.2.4	La gerencia debiera revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**3**
	A.11.4.1	Los usuarios solo deben tener acceso directo a los servicios a los cuales han sido específicamente autorizados	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.11.4.4	Se debiera controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**

	A.11.4.6	Para las redes compartidas, especialmente aquellas que se extienden a través de las fronteras de la organización, se debiera restringir la capacidad de los usuarios para conectarse a la red, en línea con la política de control de acceso y los requerimientos de las aplicaciones comerciales (ver 11.1)	No existe una Política que defina este requerimiento	**2**	Existe un Firewall que filtra toda la comunicación desde la LAN a la red pública. Existe un proxy para centralizar la navegación web	**3**	Logs del Firewall	**3**	**3**
	A.11.5.2	Todos los usuarios tienen un identificador único (ID de usuario) para su uso personal, y se debiera escoger una técnica de autenticación adecuada para sustanciar la identidad de un usuario.	No existe una Política que defina este requerimiento	**1**	Existen usuarios que ocupan claves genéricas	**1**	El sistema de directorio activo posee los registros de todos los usuarios creados.	**3**	**2**
	A.11.5.3	Los sistemas para el manejo de claves secretas debieran ser interactivos y debieran asegurar claves secretas adecuadas.	No existe una Política que defina este requerimiento	**3**	El sistema de Active Directory implementado	**1**	Modulo de administrador del AD	**1**	**1**
	A.11.5.4	Se debiera restringir y controlar estrechamente el uso de los programas de utilidad que podrían ser capaces de superar los controles del sistema y la aplicación	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.11.6.1	El acceso de los usuarios y el personal de soporte a la información y las funciones del sistema de la aplicación debiera limitarse en concordancia con la política de control de acceso definida	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.11.6.2	Los sistemas confidenciales debieran tener un ambiente de cómputo dedicado (aislado).	No existe una Política que defina este requerimiento	**1**	Solo existe aislamiento físico en sala de servidores.	**2**	Registro parcial de servidores y aplicaciones	**2**	**2**
ADQUISICIÓN, DESARROLO Y MANTENIMIENTO DE LOS SISTEMAS	**A.12.2.1**	Se debe asegurar la existencia de controles que permitan garantizar que la información ingresada a los sistemas sea correcta y apropiada	No existe una Política que defina este requerimiento	**1**	Solo algunos campos son validados en la capa de presentación	**2**	Registro parcial de pruebas	**2**	**2**
	A.12.2.2	Se debe asegurar la existencia de controles que permitan detectar cualquier corrupción de la información debido ya sea a errores de procesamiento o actos deliberados	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.12.5.5	Supervisión para el desarrollo externalizado de software	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**

	A.12.6.1	Control de vulnerabilidad técnica	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**
GESTIÓN DE LA CONTINUIDAD COMENRCIAL	**A.14.1.1**	Se debiera desarrollar y mantener un proceso gerencial para la continuidad del negocio en toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.	No existe documentación asociada	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.14.1.2	Se debieran identificar los eventos que pueden causar interrupciones a los procesos comerciales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información	No existe documentación asociada	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.14.1.3	Se debieran desarrollar e implementar planes para mantener y restaurar las operaciones y asegurar la disponibilidad de la información	No existe documentación asociada	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.14.1.5	Los planes de continuidad del negocio debieran ser probados y actualizados regularmente para asegurar que sean actuales y efectivos.	No existe documentación asociada	**1**	No existe el control	**1**	No existen registros	**1**	**1**
CUMPLIMIENTO	**A.15.1.4**	Protección de la data y privacidad de la información personal.	No existe una Política que defina este requerimiento	**1**	No existen actividades relacionadas	**1**	No existen registros	**1**	**1**
	A.15.1.5	Prevención para el uso indebido de los privilegios de usuario en el acceso a información confidencial.	No existe una Política que defina este requerimiento	**1**	No existen actividades relacionadas	**1**	No existen registros	**1**	**1**
	A.15.2.1	Cumplimiento con Políticas internas de seguridad.	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**
	A.15.2.2	Chequeo a los sistemas de información para validar cumplimiento con estándares de implementación segura.	No existe una Política que defina este requerimiento	**1**	No existe el control	**1**	No existen registros	**1**	**1**

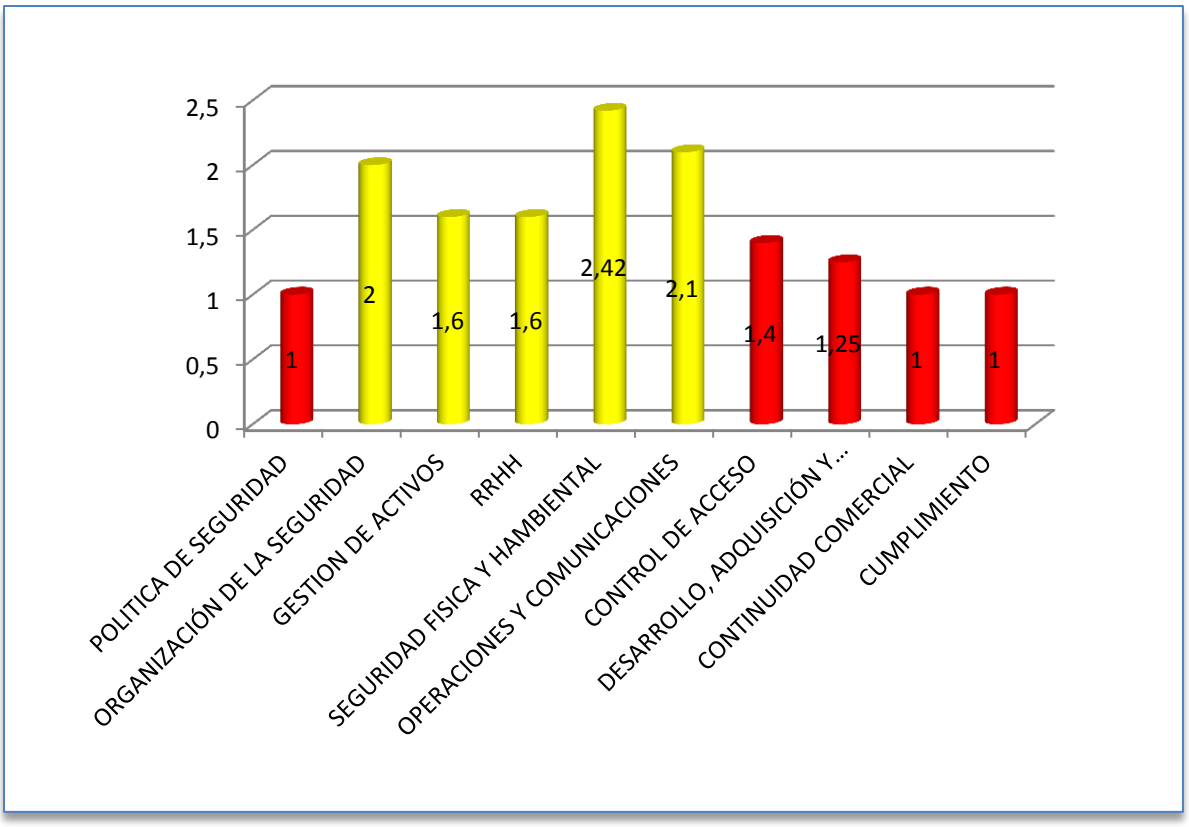

Figura 17. Gráfico con el nivel de cumplimiento obtenido tras la evaluación de controles, en relación a los dominios de la ISO 27001 en la organización.

3.7.3 Conclusiones de la medición de controles.

Echando un vistazo a los resultados de la medición de controles y al resumen ofrecido por el gráfico indicado en la Figura 17, podemos concluir que existe una gran brecha de cumplimiento con la norma, no obstante algunos elementos como los controles físicos de seguridad se acercan más hacia un nivel aceptable, podemos deducir que este comportamiento se debe a que las decisiones han sido conducidas hacia lo “visible” y lo tangible, dejando de lado los elementos de gestión y de control sobre los procesos, el recurso humano y el ambiente lógico e intangible de los datos. Si tomamos en cuenta que las brechas se traducen en vulnerabilidades que pueden ser explotadas por amenazas de seguridad, se concluye que nuestras vulnerabilidades más críticas guardan relación con los siguientes elementos:

- Control de Acceso
- Desarrollo de Sistemas
- Cumplimiento
- Políticas de Seguridad
- BCP
- Gestión de Activos

En un escenario de estas características los riesgos de mayor probabilidad guardan relación con la *confidencialidad* y la *disponibilidad* de los activos.

3.7.4 Perfilamiento de los activos.

Siguiendo lo planteado por el método OCTAVE, para realizar un adecuado análisis de riesgos debemos primero realizar el perfilamiento del activo de información para identificar sus requerimientos de *confidencialidad*, *disponibilidad*, *integridad* y de *cumplimiento*, junto con identificar también sus contenedores técnicos, físicos y a través de estos últimos determinar las personas que lo manejan. Realizaremos el perfilamiento al activo "*Expediente de Siniestro"*, dado que corresponde al activo crítico del proceso Evaluación y Liquidación de siniestros, el cual estamos evaluando. Para esta labor emplearemos el formulario ofrecido por la metodología OCTAVE.

HOJA DE TRABAJO	**PERFILAMIENTO DE ACTIVOS CRÍTICOS**	Uso Interno
Activo Crítico *¿Cuál es el activo de información evaluado?*	**Criterio de Selección** *¿Por qué este activo es importante para el área?*	**Descripción** *¿Cuál es la descripción detallada del activo?*
Expediente de Siniestro	Es la entrada para el proceso de Evaluación y liquidación de siniestros, crítico para su operación.	Información del asegurado que permite evaluar el reclamo del beneficio presentado por éste. Conforma las condiciones particulares de la póliza (mínimos requisitos). Aplicable a los procesos de evaluación, liquidación y pago de siniestros
Propietario: *¿Quién es el propietario del activo de información?*		
Gerente de Operaciones		
Requerimientos de Seguridad: *¿Cuáles son los requerimientos de seguridad para el activo de información?*		
☑ **Confidencialidad**	Sólo personal autorizado puede manejar el activo :	• Gerencia de Siniestros. • Gerente Comercial. • Proveedor del servicio de digitalización y

		almacenamiento.
☑ **Integridad**	Sólo personal autorizado puede modificar el activo de información, según lo siguiente:	Son documentos que deben mantenerse inmodificables, dado que corresponde a información personal del asegurado.
☑ **Disponibilidad**	El activo debe estar disponible para su utilización de acuerdo al siguiente requerimiento.	7x24x365
☑ **Otro**	El activo está sujeto al cumplimiento de requerimientos de seguridad exigidos por entidades regulatorias, según lo siguiente:	• Ley de la República 19.628 de protección de la vida privada. • Regulación de la SVS la cual requiere que la carpeta de cada siniestro esté activa por 5 años.

Requerimientos de Seguridad más Importantes: *¿Cuál es el requerimiento de seguridad más importante que posee este activo?*			
☑ Confidencialidad	☐ Integridad	☐ Disponibilidad	☐ Otro

Figura 18. Hoja de trabajo con el perfilamiento del activo Expediente de Siniestros.

3.7.5 Identificar los contenedores del activo.

Luego del perfilamiento del activo donde hemos identificado sus requerimientos de seguridad, debemos identificar los contenedores donde el activo es almacenado, transportado y procesado. El alcance de este análisis es dentro y fuera de la organización. Para esta labor emplearemos la hoja de trabajo "Mapa de Riesgo" ofrecido por OCTAVE.

CONTENEDORES TÉCNICOS	**EXPEDIENTE DE SINIESTROS**	Uso Interno
INTERNO		
DESCRIPCIÓN DE LOS CONTENEDORES	**DUEÑO(S)**	
Sistema de Gestión de siniestros donde se registra en su base de datos parte del expediente junto con el documento original digitalizado (evaluaciones médicas).	Gerente de Sistemas	
El activo de información es publicado a través de un sitio web	Gerente de Sistemas	

con acceso seguro (https) hacia el socio correspondiente.	
Carpetas en el Servidor de archivos, asignadas al área de Siniestros, donde se almacenan planillas de control y expedientes digitalizados.	Gerente de Operaciones
Red de datos de la empresa.	Gerente de Sistemas
Estaciones de trabajo del área de Siniestros.	Gerente de Sistemas
EXTERNO	
DESCRIPCIÓN DE LOS CONTENEDORES	**DUEÑO(S)**
Los expedientes de siniestros pagados y rechazados son digitalizados y almacenados en un proveedor externo que brinda este tipo de servicio.	Gerente de Operaciones
Internet	Proveedor del servicio

Tabla 8. Levantamiento de contenedores técnicos del activo.

CONTENEDORES FÍSICOS	**EXPEDIENTES DE SINIESTROS**	Uso Interno
INTERNO		
DESCRIPCIÓN DE LOS CONTENEDORES	**DUEÑO(S)**	
Oficina de partes, donde se reciben los expedientes desde los socios.	Gerente de Administración	
Muebles, cajas y fajos distribuidos dentro del área de Siniestros.	Gerente de Operaciones	
Data Center interno donde están servidores que soportan las carpetas de red y el sistema de gestión de siniestros.	Gerente de Sistemas	
Bodega de la Gerencia de Operaciones	Gerente de Operaciones	
Puestos de trabajo asignados a los colaboradores del área de Siniestros.	Gerente de Operaciones	
EXTERNO		

DESCRIPCIÓN DE LOS CONTENEDORES	DUEÑO(S)
Las carpetas con los expedientes son enviadas a un proveedor externo para su almacenamiento y custodia.	Gerente de Operaciones.
Las cintas donde se respalda la información de la empresa, las cuales son enviadas a un proveedor externo que brinda el servicio de custodia de este tipo de activos.	Gerente de Sistemas.

Tabla 9. Levantamiento de contenedores físicos del activo.

Contenedores Personas	**EXPEDIENTE DE SINIESTROS**	Uso Interno
INTERNO		
DESCRIPCIÓN DE LOS CONTENEDORES	**DEPARTAMENTO O UNIDAD**	
Personal de la oficina de partes	Gerencia de Administración y Finanzas	
Personal de Siniestros	Gerencia de Operaciones	
Personal de Infraestructura Tecnológica	Gerencia de Sistemas	
Administrador de Bodega	Gerencia de Operaciones	
EXTERNO		
DESCRIPCIÓN DE LOS CONTENEDORES	**DEPARTAMENTO O UNIDAD**	
Personal de proveedores para los servicios de digitalización y custodia del activo.	Proveedor del servicio	
Personal del proveedor para el almacenamiento de cintas	Proveedor del servicio	
Personal de los socios (Web Socios)	Socios	
Médicos asesores del área	Gerencia de Operaciones	

Tabla 10. Levantamiento de contenedores personas del activo.

3.7.6 Análisis de riesgos y definición de controles.

Una vez definidos los contenedores del activo el siguiente paso es comenzar con el análisis de riesgos, registrando los resultados en la hoja de trabajo para “Escenarios particulares de riesgos” el cual se basa en el formulario entregado por OCTAVE. Esta herramienta es muy útil ya que permite sintetizar varias etapas del proceso: capturar las amenazas y los impactos asociados con un riesgo, medir el nivel de los mismos junto con determinar los planes de mitigación y las actividades asociadas.

Para determinar los controles necesarios en el plan de mitigación, hemos tomado como referencia el estándar ISO/IEC 27001, el cual está conformado por una serie de controles técnicos y administrativos que permiten mitigar los riesgos de seguridad en una organización.

A continuación entregaremos las hojas de trabajo donde se registra todo el análisis de riesgo realizado en el activo de información, determinando los escenarios particulares de riesgo para las siguientes amenazas:

1. Acceso no autorizado a los contenedores tecnológicos que soportan el activo: carpetas del servidor de archivos y sistema de gestión de siniestros.
2. Presencia de virus y/o código malicioso.
3. Error en el establecimiento de perfiles de acceso y/o uso inapropiado de los privilegios del administrador en los contenedores tecnológicos.
4. Error en la carga o actualización de los datos desde los papeles al sistema de gestión.
5. Interrupción en la continuidad operativa de los servicios y sistemas que soportan el activo.

HOJA DE TRABAJO	**ESCENARIOS PARTICULARES DE RIESGO**	Clasificación: Uso Interno

Riesgo del Activo de Información

Amenaza

Nombre del Activo	Expedientes de Siniestros	
Situación de Riesgo	Acceso no autorizado a los contenedores tecnológicos que soportan el activo: carpetas del Servidor de archivos y sistema de gestión de siniestros.	**1**
Actor *¿Quién o qué sería el responsable de la ocurrencia de la situación?*	1. Personal de sistemas con privilegios de administrador en los servidores y sistemas. 2. Usuario interno de la compañía.	
Forma *¿De qué manera se llevaría a cabo?*	1. Acceso directo a las tablas de la Base de Datos o creación de usuario y contraseña sin autorización. 2. Exploit de vulnerabilidades técnicas en contenedor y vulnerabilidades en la configuración de privilegios en las Bases de Datos, para tener acceso directo a las tablas.	
Motivo *¿Cuál sería el motivo?*	1. Accidental debido a un cambio de área el cual no fue debidamente actualizado al administrador de accesos. 2. Intencional en el caso que sea un ataque interno para extraer información de los siniestros.	
Resultado *¿Cuál sería el efecto resultante sobre el activo?*	**Divulgación**	**Modificación**
	Interrupción	**Destrucción / Pérdida**
Requerimientos de Seguridad *¿De qué forma los requerimientos de seguridad serían vulnerados?*	Acceso de lectura y/o modificación de información sensible sin la debida autorización. (Actualmente no existe un control de acceso riguroso para los activos de información).	
Probabilidad *¿Cuál es la probabilidad que la situación se produzca?*	**Alta**	**Media** Baja

Consecuencias *¿Cuáles son las consecuencias que el resultado de la situación y la vulneración de los requerimientos de seguridad producirían sobre el área/compañía?*	**Severidad** *¿Cuán severas podrían ser las consecuencias para el área/compañía?*		
El impacto de la divulgación de información confidencial se vería materializado en impacto de imagen de la compañía, lo que además podría generar algún impacto legal, producto que el activo contiene información protegida por ley	**Área de Impacto**	**Valor**	**Puntuación**
	Reputación (5)	4	20
	Financiera (4)	3	12

	La modificación del activo podría impactar sobre la continuidad de las operaciones del área lo que significaría una pérdida de productividad.	Productividad (3)	0	0
		Legal (2)	4	8
		Otra (1)	0	0
		Puntuación Relativa		**38**

HOJA DE TRABAJO	**ESCENARIOS PARTICULARES DE RIESGO**	Uso Interno

Mitigación del Riesgo

En función de la puntuación relativa del riesgo, ¿qué acciones deberían ser tomadas?

Aceptar	Postergar	Mitigar	Transferir

Si decide mitigar el riesgo indique lo siguiente:

¿Sobre qué contenedor aplicaría los controles?	*¿Qué controles (administrativos, técnicos, físicos) aplicaría a este contenedor?*	*ISO/IEC 27001*
Administrador de la Base de Datos y personal del sistemas	Firmar acuerdo de confidencialidad.	A.8.1.3
Todos los contenedores	Formalizar la designación del propietario quien será responsable del activo de información, a quien se le pedirá autorización para el acceso y uso del mismo.	A.7.1.3
Usuarios de la Gerencia de Operaciones	Implementar un procedimiento de control de accesos auditable, registrando la debida autorización del propietario designado.	A.11.2.1
Sistema de Gestión de Siniestros y carpetas del Servidor de archivos	Implementar auditorías periódicas a los privilegios de los usuarios sobre el activo de información.	A.11.2.4
Sistema de Gestión de Siniestros y carpetas del Servidor de archivos	Garantizar la trazabilidad de las operaciones con el registro en logs de las acciones realizadas por los usuarios y el administrador.	A.10.10.4, A.10.10.1
Servidores donde se aloja el FileServer y el sistema de Gestión de Siniestros	Cerrar todos los puertos que no correspondan a los servicios autorizados en los hosts, principalmente FTP, TFP y HTTP.	A.11.4.1, A.11.4.4
Servidores donde se aloja el FileServer y el sistema de Gestión de Siniestros	Asegurar la correcta implementación de parches de seguridad en forma periódica y controlar las vulnerabilidades técnicas en los sistemas operativos.	A.12.6.1

Figura 19. Escenarios particulares de riesgo: Acceso no autorizado a los contenedores tecnológicos que soportan el activo.

HOJA DE TRABAJO	**ESCENARIOS PARTICULARES DE RIESGO**	Clasificación: Uso Interno

Riesgo del Activo de Información

Amenaza

Nombre del Activo	Expedientes de Siniestros	
Situación de Riesgo	Presencia de Virus y/o código malicioso	**2**

Actor *¿Quién o qué sería el responsable de la ocurrencia de la situación?*	Usuarios internos que ingresen desde el exterior algún gusano, virus o Malware.		
Forma *¿De qué manera se llevaría a cabo?*	Usuarios de la red interna que naveguen en sitios web infectados con malware, o que conecten periféricos infectados en sus estaciones de trabajo.		
Motivo *¿Cuál sería el motivo?*	Accidental		
Resultado *¿Cuál sería el efecto resultante sobre el activo?*	**Divulgación**	**Modificación**	
	Interrupción	**Destrucción / Pérdida**	
Requerimientos de Seguridad *¿De qué forma los requerimientos de seguridad serían vulnerados?*	Privilegios sobre los activos tecnológicos para instalar programas y dispositivos periféricos. No existe una consola de administración para el producto antivirus adquirido en la organización.		
Probabilidad *¿Cuál es la probabilidad que la situación se produzca?*	**Alta**	**Media**	Baja

Consecuencias *¿Cuáles son las consecuencias que el resultado de la situación y la vulneración de los requerimientos de seguridad producirían sobre el área/compañía?*	**Severidad** *¿Cuán severas podrían ser las consecuencias para el área/compañía?*		
Interrupción de los servicios lo que trae consigo impacto en la productividad de la organización y en el cumplimiento de plazos con los socios para la liquidación de siniestros. Impacto de imagen si un ataque de malware provoca una caída de los sistemas por un tiempo prolongado.	**Área de Impacto**	**Valor**	**Puntuación**
	Reputación (5)	4	20
	Financiera (4)	2	8
	Productividad (3)	4	12

		Legal (2)	0	0
		Otra (1)	0	0
		Puntuación Relativa		**40**

HOJA DE TRABAJO	**ESCENARIOS PARTICULARES DE RIESGO**		Uso Interno
Mitigación del Riesgo *En función de la puntuación relativa del riesgo, ¿qué acciones deberían ser tomadas?*			
Aceptar	Postergar	Mitigar	Transferir
Si decide mitigar el riesgo indique lo siguiente:			
¿Sobre qué contenedor aplicaría los controles?	*¿Qué controles (administrativos, técnicos, físicos) aplicaría a este contenedor?*		*ISO/IEC 27001*
Usuarios del sistema	Redactar una política de seguridad donde se indique claramente los lineamientos para la seguridad de la información y las reglas para dar uso adecuado de los activos tecnológicos dentro de la organización. El documento debe ser respaldado por la gerencia y publicado a todos los empleados.		A.5.1.1, A.7.1.3
Usuarios del sistema	Implementar restricciones en las estaciones de trabajo para limitar los privilegios de los usuarios sobre estas. Se sugiere aprovechar las funcionalidades del dominio Active Directory existente para la creación de políticas.		A.11.5.4, A.11.4.1
Estaciones de trabajo y Servidores donde se aloja el FileServer y el sistema de Gestión de Siniestros	Garantizar la actualización periódica de herramientas de antivirus, implementar una consola de administración de esta y la ejecución de búsquedas de virus y troyanos al menos una vez por semana a toda la red.		A.10.4.1

Figura 20. Escenarios particulares de riesgo: Presencia de Virus y/o código malicioso.

HOJA DE TRABAJO	**ESCENARIOS PARTICULARES DE RIESGO**	Clasificación: Uso Interno

Riesgo del Activo de Información

Amenaza

Nombre del Activo	Expediente de siniestros		
Situación de Riesgo	Error en el establecimiento de perfiles de acceso y/o uso inapropiado de los privilegios del administrador en los contenedores tecnológicos.		**3**
Actor *¿Quién o qué sería el responsable de la ocurrencia de la situación?*	Personal de sistemas con privilegios de administrador en la base de batos del sistema y los directorios del Servidor de archivos.		
Forma *¿De qué manera se llevaría a cabo?*	1. Acceso directo a las tablas de la Base de Datos o al módulo de administración de los sistemas		
Motivo *¿Cuál sería el motivo?*	1. Intencional, en colusión con usuarios internos para extraer o modificar información sensible del negocio. 2. Accidental por el movimiento no controlado de personal hacia otras áreas. 3. Accidental por el error humano durante la operación del administrador de sistemas al realizar la asignación de privilegios.		
Resultado *¿Cuál sería el efecto resultante sobre el activo?*	**Divulgación**	**Modificación**	
	Interrupción	**Destrucción / Pérdida**	
Requerimientos de Seguridad *¿De qué forma los requerimientos de seguridad serían vulnerados?*	Abuso de privilegios en el acceso a información sensible del negocio, no existe trazabilidad para las operaciones del administrador. El personal de sistemas no posee acuerdos de confidencialidad.		
Probabilidad *¿Cuál es la probabilidad que la situación se produzca?*	**Alta**	**Media**	Baja

Consecuencias *¿Cuáles son las consecuencias que el resultado de la situación y la vulneración de los requerimientos de seguridad producirían sobre el área/compañía?*	**Severidad** *¿Cuán severas podrían ser las consecuencias para el área/compañía?*		
Podría existir impacto financiero si alguien se coludiera con un	**Área de Impacto**	**Valor**	**Puntuación**

	administrador para modificar en la base de datos los montos de liquidación o la resolución en el Informe de Liquidación para la aprobación o rechazo del siniestro. Esta situación también trae consigo impacto en la reputación de la compañía lo que podría causar perdida de nuevos negocios. La divulgación de información confidencial de los asegurados trae un impacto legal producto que es un delito a la Ley 19628.	Reputación (5)	4	20
		Financiera (4)	3	12
		Productividad (3)	0	0
		Legal (2)	4	8
		Otra (1)	0	0
		Puntuación Relativa		**40**

HOJA DE TRABAJO	**ESCENARIOS PARTICULARES DE RIESGO**		Uso Interno
Mitigación del Riesgo *En función de la puntuación relativa del riesgo, ¿qué acciones deberían ser tomadas?*			
Aceptar	Postergar	Mitigar	Transferir
Si decide mitigar el riesgo indique lo siguiente:			
¿Sobre qué contenedor aplicaría los controles?	*¿Qué controles (administrativos, técnicos, físicos) aplicaría a este contenedor?*		*ISO/IEC 27001*
Administrador de la Base de Datos y usuarios del sistema	Firmar acuerdo de confidencialidad.		A 8.1.3
Servidores donde se aloja el FileServer y el sistema de Gestión de Siniestros	Habilitar el registro de logs de la operación del Administrador en los sistemas, y realizar auditorías periódicas de estos.		A.10.10.4

Figura 21. Escenarios particulares de riesgo: Error en el establecimiento de perfiles de acceso y/o uso inapropiado de los privilegios del administrador.

HOJA DE TRABAJO	**ESCENARIOS PARTICULARES DE RIESGO**	Clasificación: Uso Interno

Riesgo del Activo de Información

Amenaza

Nombre del Activo	Expediente de Siniestros		
Situación de Riesgo	Error en la carga o actualización de los datos desde los papeles al sistema de gestión de siniestros.		**4**
Actor *¿Quién o qué sería el responsable de la ocurrencia de la situación?*	Personal del área de Beneficios a cargo de la carga de datos al sistema		
Forma *¿De qué manera se llevaría a cabo?*	En forma accidental durante la digitación de datos en el sistema de gestión de los siniestros.		
Motivo *¿Cuál sería el motivo?*	N/A		
Resultado *¿Cuál sería el efecto resultante sobre el activo?*	**Divulgación**	**Modificación**	
	Interrupción	**Destrucción / Pérdida**	
Requerimientos de Seguridad *¿De qué forma los requerimientos de seguridad serían vulnerados?*	A través de la falta de controles en el ingreso de datos y consistencia de la información ingresada.		
Probabilidad *¿Cuál es la probabilidad que la situación se produzca?*	Alta	**Media**	Baja

Consecuencias *¿Cuáles son las consecuencias que el resultado de la situación y la vulneración de los requerimientos de seguridad producirían sobre el área/compañía?*	**Severidad** *¿Cuán severas podrían ser las consecuencias para el área/compañía?*		
Los errores en la carga de datos provocan un impacto en la productividad del área, dado que sería necesario invertir horas de RRHH para el reproceso. Si los errores no son detectados oportunamente en la etapa de validación del proceso, podría traer impacto Financiero, ya que podrían liquidarse siniestros no cubiertos por la póliza del asegurado.	**Área de Impacto**	**Valor**	**Puntuación**
	Reputación (5)	2	10
	Financiera (4)	3	12
	Productividad (3)	4	12

		Legal (2)	0	0
		Otra (1)	0	0
			Puntuación Relativa	**34**

HOJA DE TRABAJO	**ESCENARIOS PARTICULARES DE RIESGO**		Uso Interno
Mitigación del Riesgo *En función de la puntuación relativa del riesgo, ¿qué acciones deberían ser tomadas?*			
Aceptar	Postergar	Mitigar	Transferir
Si decide mitigar el riesgo indique lo siguiente:			
¿Sobre qué contenedor aplicaría los controles?	*¿Qué controles (administrativos, técnicos, físicos) aplicaría a este contenedor?*		*ISO/IEC 27001*
Sistema de gestión de siniestros	Implementar controles en la capa de presentación del sistema que validen los datos en los parámetros críticos de entrada.		A.12.2.
Sistema de gestión de siniestros	Implementar validaciones en la salida de datos para evitar que se procese información errónea en el sistema.		A.12.2

Figura 22. Escenarios particulares de riesgo: Error en la carga o actualización de los datos desde los papeles al sistema de gestión de siniestros.

HOJA DE TRABAJO	**ESCENARIOS PARTICULARES DE RIESGO**	Clasificación: Uso Interno

Riesgo del Activo de Información	**Amenaza**	**Nombre del Activo**	Expediente de siniestros		
		Situación de Riesgo	Interrupción en la continuidad operativa de los servicios y/o sistemas que soportan el activo.		**5**
		Actor *¿Quién o qué sería el responsable de la ocurrencia de la situación?*	Evento mayor que provoque un cese prolongado de las operaciones. Ej.: Terremoto, incendio, inundación, corte de energía, inhabilitación de acceso a las oficinas, atentados, etc.		
		Forma *¿De qué manera se llevaría a cabo?*	1. Fallas graves en cualquiera de los componentes de hardware / software que soporta al activo. 2. Cualquier evento que impacte en la continuidad de la operación de los procesos críticos.		
		Motivo *¿Cuál sería el motivo?*	1. Accidental por falta de controles preventivos y mitigadores. 2. Intencional a través de acciones que provoquen daño a la organización.		
		Resultado *¿Cuál sería el efecto resultante sobre el activo?*	Divulgación	Modificación	
			Interrupción	**Destrucción / Pérdida**	
		Requerimientos de Seguridad *¿De qué forma los requerimientos de seguridad serían vulnerados?*	1. Falta de controles preventivos que permitan evitar el corte de servicios. 2. Falta de controles que permitan reaccionar de manera eficiente ante eventos que interrumpan la operación de los procesos críticos del negocio.		
		Probabilidad *¿Cuál es la probabilidad que la situación se produzca?*	**Alta**	**Media**	**Baja**
	Consecuencias *¿Cuáles son las consecuencias que el resultado de la situación y la vulneración de los requerimientos de seguridad producirían sobre el área/compañía?*		**Severidad** *¿Cuán severas podrían ser las consecuencias para el área/compañía?*		

	El mayor impacto es de productividad debido a la interrupción de los servicios y al esfuerzo necesario para recuperase. Impacto financiero por la cantidad de recursos que se deben disponer en la recuperación de un evento para el cual no se estaba preparado. Impacto de imagen si no es posible cumplir con los plazos definidos en los contratos ni con los requerimientos de los clientes. Posibles multas.	**Área de Impacto**	**Valor**	**Puntuación**
		Reputación (5)	3	15
		Financiera (4)	4	16
		Productividad (3)	5	15
		Legal (2)	0	0
		Otra (1)	3	3
			Puntuación Relativa	**49**

HOJA DE TRABAJO	**ESCENARIOS PARTICULARES DE RIESGO**		Clasificación: Uso Interno
Mitigación del Riesgo *En función de la puntuación relativa del riesgo, ¿qué acciones deberían ser tomadas?*			
Aceptar	Postergar	Mitigar	Transferir
Si decide mitigar el riesgo indique lo siguiente:			
¿Sobre qué contenedor aplicaría los controles?	*¿Qué controles (administrativos, técnicos, físicos) aplicaría a este contenedor?*		*ISO/IEC 27001*
Servidor en donde se aloja el activo.	Garantizar que los equipos estén en un recinto que a lo menos brinde soporte eléctrico, control de humedad y T°, que posea sistema de detección y extinción de incendios, un control de acceso restringido y auditable, su construcción debe ser sólida, antisísmica y de material ignifugo, libre de elementos inflamables.		A.9.1.2, A.9.1.4, A 9.2.1, A.9.2.2,
Servidores donde se aloja el activo.	Política de respaldo de información, almacenando los medios en un recinto externo con pruebas periódicas de recuperación de datos.		A.10.5.1
Todos los contenedores	Implementar un proceso de gestión de continuidad de negocios que permita evaluar los riesgos y controles necesarios para garantizar la continuidad operativa de los procesos críticos de la organización.		A.14.1.1, A.14.1.2, A. 14.1.3, A. 14.1.4

Figura 23. Escenarios particulares de riesgo: Interrupción en la continuidad operativa de los servicios y/o sistemas que soportan el activo.

3.8 Estrategias de Mitigación.

3.8.1 Reporte ejecutivo con al resultado del análisis.

Posterior a los análisis de los escenarios particulares de riesgo, se entrega a la Gerencia un resumen con los resultados obtenidos señalando los elementos más relevantes del análisis, para facilitar la toma de decisiones con respecto a la estrategia de mitigación.

EVALUACIÓN DE RIESGO	**Expediente de Siniestro**	Confidencial

DESCRIPCIÓN DE LA MATRIZ DE RIESGO RELATIVO

GRUPO	ESTRATEGIA DE MITIGACION
High Risk	Mitigar los Riesgos
Medium Risk	Mitigar ó Transferir
Low Risk	Transferir o Aceptar

RESULTADO DEL ANÁLISIS DE RIESGO

PROBABILIDAD	IMPACTO RELATIVO		
	30 a 45	16 a 29	0 a 15
ALTA	2		
MEDIA	3		
BAJA			

TIPO DE RIESGO	CANTIDAD
Destrucción / Pérdida	1
Divulgación	2
Interrupción	3
Modificación	2

ELEMENTOS INCLUIDOS EN LA MATRIZ

PROB.	IMPACTO	DESCRIPCIÓN DEL ESCENARIO DE RIESGO
ALTA	30 a 45	1) Acceso no autorizado a los contenedores tecnológicos que soportan el activo: carpetas del Servidor de archivos y sistema de gestión de siniestros. 2) Error en el establecimiento de perfiles de acceso y/o uso inapropiado de los privilegios del administrador en los contenedores tecnológicos.
MEDIA	30 a 45	1) Presencia de Virus y/o código malicioso. 2) Error en la carga o actualización de los datos desde los papeles al sistema de gestión de siniestros podría ocasionar errores en el proceso de la liquidación 3) Interrupción en la continuidad operativa de los servicios y sistemas que soportan el activo.

3.8.2 Decisión ejecutiva.

Una vez analizados los riesgos y evaluado los controles necesarios para mitigarlos se presentan los resultados del análisis a la plana ejecutiva de la organización, ya que es suya la responsabilidad de tomar la decisión sobre su tratamiento. Cabe destacar que se hace indispensable el respaldo de la dirección en todo el proceso, ya que la implementación de una iniciativa de resiliencia operacional demanda bastantes recursos tanto para implementar los controles de seguridad identificados como en el desarrollo de los planes de continuidad de negocio, así como también en definición de políticas que sean transversales en la organización. La Tabla 11 indica el resumen de riesgos y la estrategia definida por la Gerencia para su tratamiento.

N°	*Escenarios de riesgo*	*Evaluación del riesgo*	*Estrategia*
1	Acceso no autorizado a los contenedores tecnológicos que soportan el activo: carpetas del servidor de archivos y sistema de gestión de siniestros.	High Risk	Mitigar
2	Presencia de Virus y/o código malicioso.	Medium Risk	Mitigar
3	Error en el establecimiento de perfiles de acceso y/o uso inapropiado de los privilegios del administrador en los contenedores tecnológicos.	High Risk	Mitigar
4	Error en la carga o actualización de los datos desde los papeles al sistema de gestión de siniestros podría ocasionar errores posteriores en la liquidación.	Medium Risk	Aceptar
5	Interrupción en la continuidad operativa de los servicios y sistemas que soportan el activo.	Medium Risk	Mitigar

Tabla 11. Cuadro con la evaluación de los riesgos y la estrategia definida por la Gerencia para cada uno.

3.9 Planes de acción

3.9.1 Desarrollo del plan de controles.

Este plan no es otra cosa que la definición de plazos y responsables para implementar los controles de seguridad sugeridos por el proceso de análisis y evaluación de riesgos, en virtud de la respuesta del riesgo definida por la Gerencia.

id	*Control*	*Tipo de control*	*ISO/IEC 27001*	*Área Responsable*	*Plazo de implementación*
CTR001	Firmar acuerdo de confidencialidad anexo a los contratos.	Administrativo	A.8.1.3	RRHH	1 mes
CTR002	Formalizar la designación de los propietarios de los activos de información, a quienes se les pedirá autorización para el acceso y uso de los mismos	Administrativo	A.7.1.3	Control Interno	1 mes
CTR003	Implementar un procedimiento de control de accesos auditable, registrando la autorización de acceso a los activos de información del propietario designado.	Administrativo	A.11.2.1	Control Interno	2 meses
CTR004	Implementar auditorías periódicas a los privilegios de los usuarios sobre los activo de información.	Administrativo	A.11.2.4	Control Interno	6 meses
CTR005	Garantizar la trazabilidad de las operaciones con el registro en logs de las acciones realizadas por los usuarios y el administrador.	Técnico	A.10.10.4, A.10.10.1	Sistemas	3 meses
CTR006	Cerrar todos los puertos que no correspondan a los servicios autorizados en los hosts, principalmente FTP, TFP y HTTP.	Técnico	A.11.4.1, A.11.4.4	Sistemas	3 meses
CTR007	Asegurar la correcta implementación de parches de seguridad en forma periódica y controlar las vulnerabilidades técnicas en los sistemas operativos.	Técnico	A.12.6.1	Sistemas	4 meses
CTR008	Redactar una política de seguridad donde se indique claramente los lineamientos para la seguridad de la información y las reglas para dar uso adecuado de los activos tecnológicos dentro de la organización. El documento debe ser respaldado por la gerencia y publicado a todos los empleados.	Administrativo	A.5.1.1, A.7.1.3	Control Interno	2 meses
CTR009	Implementar restricciones en las estaciones de trabajo para limitar los privilegios de los usuarios sobre estas. Se sugiere aprovechar las	Técnico	A.11.5.4, A.11.4.1	Sistemas	2 meses

	funcionalidades del dominio Active Directory existente para la creación de políticas.				
CTR010	Garantizar la actualización periódica de herramientas de antivirus, implementar una consola de administración de esta y la ejecución de búsquedas de virus y troyanos al menos una vez por semana a toda la red.	Técnico	A.10.4.1	Sistemas	1 mes
CTR011	Garantizar que los equipos estén en un recinto libre de elementos inflamables, que a lo menos brinde soporte eléctrico, control de humedad y T°, que posea sistema de detección y extinción de incendios, un control de acceso restringido y auditable, su construcción debe ser sólida, antisísmica y de material ignifugo.	Físicos	A.9.1.2, A.9.1.4, A 9.2.1, A.9.2.2,	Sistemas	6 meses
CTR012	Política de respaldo de información, almacenando los medios en un recinto externo con pruebas periódicas de recuperación de datos.	Técnico	A.10.5.1	Sistemas	2 meses
CTR013	Implementar un proceso de gestión de continuidad de negocios que permita evaluar los riesgos y los controles necesarios, con el objetivo de garantizar la continuidad operativa de a lo menos los procesos críticos de la organización.	Administrativo	A.14.1.1, A.14.1.2, A. 14.1.3, A. 14.1.4	Control Interno	12 meses

Tabla 12. Plan para implementar los controles de seguridad en virtud de la estrategia de mitigación de la Gerencia.

3.9.2 Desarrollo de la estrategia de recuperación.

Para desarrollar la estrategia de recuperación es necesario tomar en cuenta 3 elementos fundamentales[7] que para el caso de nuestro análisis sus valores se indican en la siguiente tabla:

MTD	30 días, definido como una de las premisas del análisis por la dirección de la empresa.
RTO	48 horas, identificado en el BIA del proceso.
RPO	Últimos 12 meses, definido en el BIA del proceso lo que equivale a 1 TB en archivos sin considerar la base de datos de la aplicación.

Tabla 13. Parámetros fundamentales para definir la estrategia de recuperación del BCP.

3.9.3 Identificación de requerimientos de TI.

A través del BIA se obtiene el levantamiento de los componentes tecnológicos que soportan el proceso crítico.

Recursos/Componentes de Sistema	*Plataforma/ Versión de OS*	*Descripción*
Servidor de aplicaciones	Windows 2003 Server, SP2/TOMCAT/JBOSS	Es el servidor que publica la aplicación de Siniestros a los usuarios.
Servidor de Bases de Datos	Windows 2003 Server, SP2/DB ORACLE	Servidor con la capa de datos de la aplicación.
Enlace a internet	NA	Proveedor que brinda conexión para servicios web, e-mail y WAN.
Firewall	Checkpoint VPN-1	Sistema que protege la red local de la red pública a través de accesos controlados y restringidos.

[7] Estos elementos son explicados con mayor profundidad en el subcapítulo 2.9 *Proceso de Continuidad de Negocios.*

Servidor de accesos	Windows 2003 Server, SP2/Active Directory	Servidor que provee servicio de autentificación, control de acceso a los recursos de la red y DNS.
Servidor de archivos	Windows 2003 Server, SP2	Servidor que provee el servicio de carpetas compartidas en la red local.
Servidor Proxy	Windows 2003 Sever, ISA Server	Servidor que concentra el acceso web desde la red local.
Servidor de correo electrónico	Windows 2003 Server, Lotus Notes V5	Servidor que provee el servicio de correo electrónico a la organización.

Tabla 14. Listado de los recursos de TI que soportan el proceso crítico.

3.9.4 Evaluación de estrategias de contingencia.

Tomando en cuenta el margen de tiempo (RTO) que tenemos para la continuidad del proceso de evaluación y liquidación de siniestros, junto con el tamaño en data que necesitamos tener disponible (RPO) y considerando además las proyecciones de la iniciativa para dar alcance a otros procesos críticos de la organización con requerimientos similares, evaluamos las siguientes estrategias de recuperación.

1) Hotsite

Desde el punto de vista operacional esta solución satisface nuestros requerimientos siendo su obstáculo el presupuesto necesario para llevarla a cabo. Las alternativas para implementarlo son las siguientes:

Alternativa	*Descripción*
Hotsite 1	Contratar el servicio completo con una empresa externa para implementar el sitio de recuperación de desastres, la cual provea el data center para los servidores y equipos de comunicación de respaldo, implementar replicación asíncrona con el sitio principal para actualizar datos, junto con la disposición de puestos de trabajo listos para continuar con la operación en virtud de las exigencias del RTO de nuestros procesos críticos.

Hotsite 2	Solución mixta contratando el servicio de data center con una empresa externa para los sistemas de respaldo, implementar replicación asíncrona con el sitio principal para mantener actualizados los datos, junto con el arriendo y equipamiento de oficinas para instalar nuestro propio sitio de recuperación de desastres.

Tabla 15. Alternativas contempladas para implementar la estrategia de Hotsite en el plan de continuidad.

2) Warmsite

El Warmsite es otra opción cuyo presupuesto requerido es inferior al Hotsite, no obstante cubre sólo parcialmente los requerimientos de RTO y no es posible proyectar el crecimiento de la iniciativa a otros procesos críticos de la organización

Alternativa	*Descripción*
Warmsite	Contratar servicio de Data Center con una empresa externa para los servidores de respaldo, implementar replicación asíncrona con el sitio principal para mantener actualizados los datos. Habilitar un servicio de acceso remoto para un porcentaje de los liquidadores los cuales puedan realizar la operación de manera off-site. Si el tiempo de recuperación del site principal es superior a 5 días, se contratará el servicio de liquidación de siniestros con una empresa externa.

Tabla 16. Alternativas contempladas para implementar la estrategia de Warmsite.

Cabe destacar que contratar un servicio de data center es mandatorio dentro de la estrategia de recuperación ya que necesitamos mantener un sitio de respaldo que mantenga actualizados los sistemas críticos, tomando en cuenta que en el mercado existen proveedores que cuentan con una infraestructura acorde con los requerimientos de seguridad y disponibilidad que demanda nuestra iniciativa de resiliencia operacional.

3.9.5 Evaluación de Costos.

La siguiente información es una evaluación de costos para la primera alternativa, implementar un *Hot site,* donde evaluamos si el off-site será contratado con una empresa externa (*Hotsite1*) o si la organización implementa uno propio (*Hotsite2*).

COSTOS DE HABILITACION	m2	Valor m2	Carga de trabajo necesaria (%)	Hotsite 1	Hotsite 2
Adecuación de la oficina (pintura, arreglos en gral.)	80	$ 243.452	25%	-	$ 4.869.040
Instalación eléctrica de la oficina	80	$ 4.426	25%	-	$ 88.528
Instalación sanitaria	80	$ 2.213	25%	-	$ 44.264
Instalación aire acondicionado	80	$ 3.320	25%	-	$ 66.396
Instalación alfombra	80	$ 26.558	100%	-	$ 2.124.672
Costo set up	-	-	-	$ 1.106.600	$ 1.239.392
TOTAL COSTO HABILITACION SERVICIO				$ 1.106.600	$ 8.432.292

COSTOS DE TI	Cant.	Hotsite 1	Hotsite 2
Computadores para los puestos a incorporar	22	-	$ 13.633.312
Central Telefónica para 24 anexos	1	-	$ 1.000.000
Equipo de Fax	1	-	$ 150.000
Aparatos telefónicos	22	-	$ 500.000
Infraestructura de red y comunicaciones	1	-	$ 1.100.000
Mudanza de enlaces	2	$ 200.000	$ 200.000
TOTAL COSTO INFRAESTRUCTURA DE TI		$ 200.000	$ 16.583.312

COSTOS DE SERVICIOS ASOCIADOS	Valor Mensual	Cant. Períodos	Hotsite 1	Hotsite 2
Servicio de Data Center de Respaldo	$ 708.224	36	$ 25.496.064	$25.496.064
Arriendo enlaces Vitacura/Recovery Site/Concepción	$ 2.478.784	36	$ 89.236.224	$89.236.224
Servicio de Recovery Site	$ 1.504.976	36	$ 54.179.136	-
Arriendo oficina propia	$619.696	-		$22.309.056
Costo 2 pruebas anuales	-	3	-	-
TOTAL COSTO ANUAL DE SERVICIOS			$168.911.424	$137.041.344

Tabla 17. Resumen de costos.

Parámetros	
Housing equipos (UF)	**32**
Enlaces (UF)	**112**
Valor UF	**$22.132**
Valor mensual m2 arriendo + servicios adic. (UF) Santiago Centro	**0,40**
Valor contrato mensual servicio recovery propuesto Sonda (UF)	**68,00**
PCs Necesarias	**22**
Valor m2 construcción (UF)	**11,00**
Valor m2 instalación eléctrica (UF)	**0,20**
Valor m2 instalación sanitaria (UF)	**0,10**
Valor m2 instalación aire acondicionado (UF)	**0,15**
Valor m2 carpet (UF)	**1,20**
Valor PCs	**28,00**
Cantidad de puestos a habilitar	**22**
Período de Evaluación (meses)	**12**
Costo cableado voz, datos y fuerza (por puesto)	**1,24**
Valor incidente diario GTD	**9,00**
Metros cuadrados necesarios opción arriendo	**130**

Tabla 18. Cuadro con los parámetros considerados para el análisis de costos, incluyendo la propuesta de un proveedor externo (Sonda).

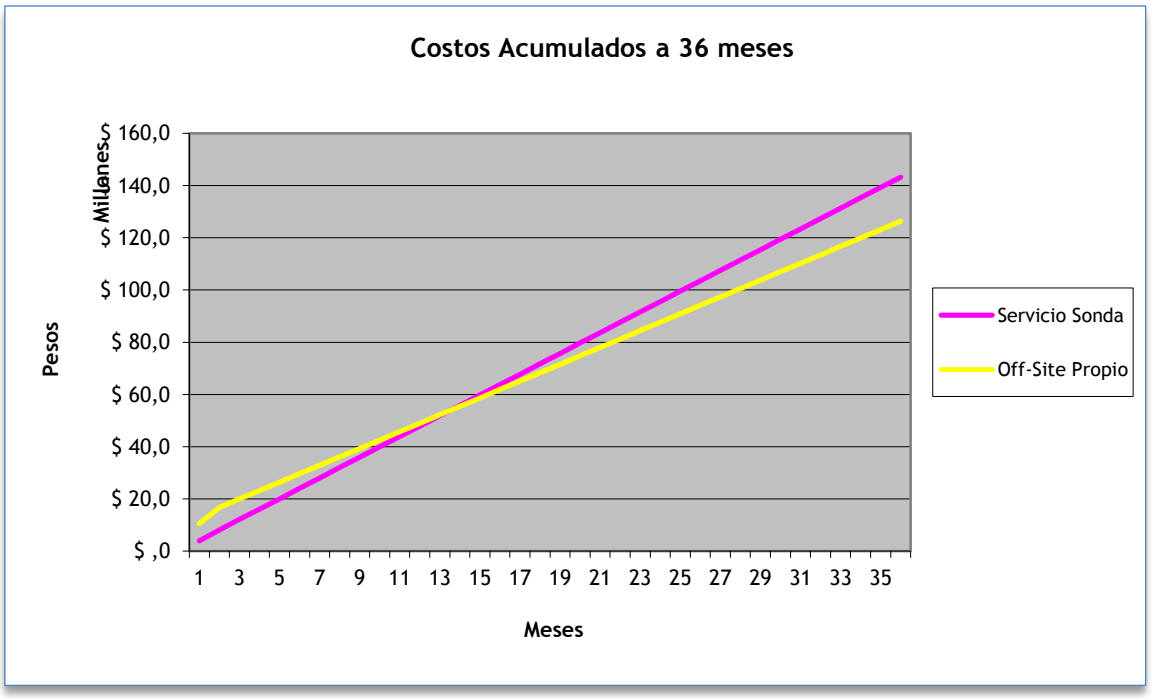

Figura 24. Gráfico con la proyección de costos acumulados a 36 meses entre Servicio contratado y un Off-site propio.

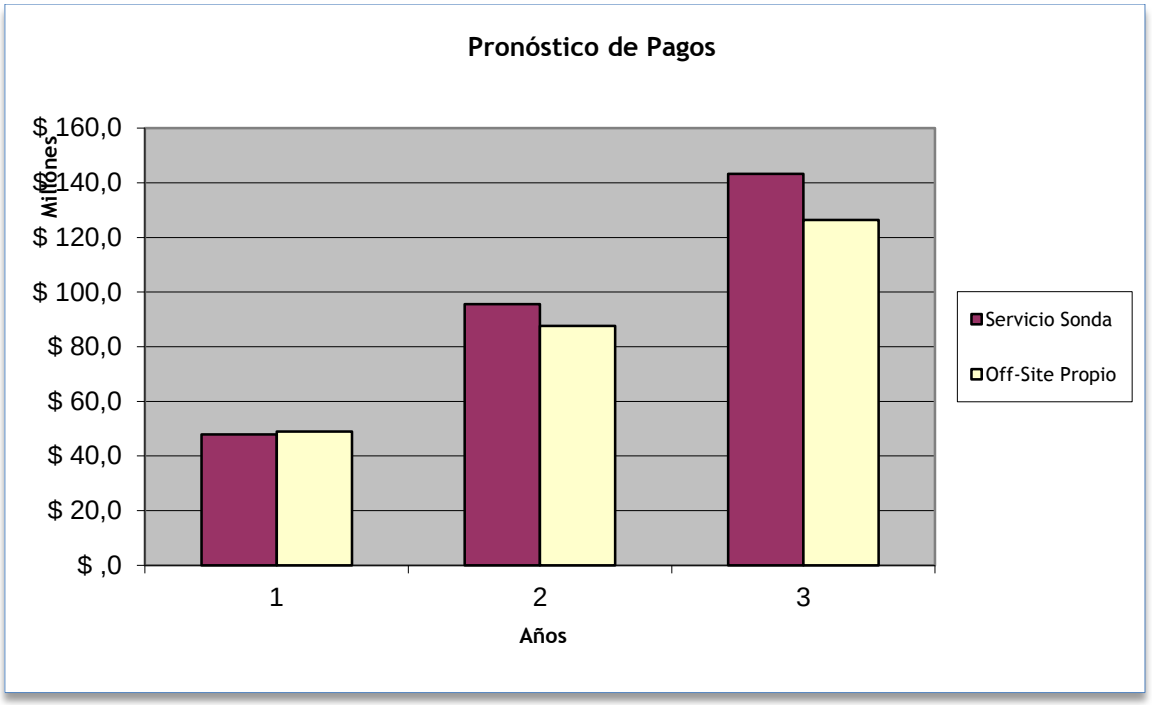

Figura 25. Gráfico con la proyección de costos comparativa entre una solución Off-Site propia y una solución contratada con un tercero.

3.10 Los pasos a seguir.

Una vez considerados los controles y las estrategias de mitigación, junto con la evaluación de costo beneficio de la estrategia a implementar, el BCP Manager deberá presentar esta información a la gerencia como un caso de negocio formal, para que el nivel ejecutivo tome la decisión pertinente, en virtud del apetito de riesgo y de los recursos disponibles en la organización.

Frente a la decisión ejecutiva, el BCP Manager y su equipo deberá trabajar en el desarrollo de los planes de contingencia para completar el set de procedimientos que conforman el BCP, entre los que se destaca el *plan de comunicación de crisis*, el *plan de recuperación de desastres*, el *plan de emergencia* y el *plan de continuidad de negocios* con los procesos críticos abordados. Otro punto importante es la confección del plan de pruebas para verificar que todos los elementos necesarios hayan sido considerados en el BCP documentado.

Junto con el plan de pruebas los cuales podrán llevarse a cabo una vez se implemente la estrategia de contingencia, deberá realizarse una auditoría de los controles de seguridad implementados, para asegurar que las medidas de contención estén adecuadamente dispuestas para la protección de los activos y sus elementos de TI.

Un elemento importante que la dirección debe tener en cuenta, es que tanto la iniciativa de seguridad como la iniciativa de continuidad de negocios requiere una evaluación y mejora permanente, y que las actividades realizadas hasta ahora conforman un primer paso para alcanzar un nivel de resiliencia operacional adecuado. Es por esto que la organización debe considerar seriamente la adopción de un gobierno de riesgo más consolidado, que integre las buenas prácticas y controle la iniciativa de resiliencia en las áreas y procesos donde sea implementada, junto con conducir el crecimiento de su alcance hacia los otros procesos críticos del negocio, en virtud de factores de riesgo

interno y externos, junto los requerimientos regulatorios y las expectativas de los socios y clientes.

Tal como se expone con el SGSI de la ISO 27001, o como lo refleja COBIT, la dirección no debe bajar la guardia dejando la responsabilidad de los riesgos operacionales a TI. Debe tomar las riendas de la organización con un enfoque de riesgo, implementando un proceso consolidado de seguridad y continuidad de negocios que aporte valor a todas las actividades operativas y comerciales que la sustentan, para obtener una zona operativa de confort que le permita sostener satisfactoriamente su negocio y generar nuevas oportunidades de crecimiento en el mercado.

4 CONCLUSIONES

El desarrollo de este trabajo ha permitido demostrar lo planteado en la hipótesis, con respecto a la aplicación del concepto de Resiliencia en una empresa, común en ámbitos como la psicología más que en el mundo de la gestión y operación de negocios, a través de un modelo de gestión de riesgos. En este ámbito se puede concluir lo siguiente:

1) La gestión de seguridad de la información y de continuidad de negocios son totalmente complementarias.

La implementación de la iniciativa es posible si la componen dos elementos fundamentales: la seguridad de la información y la continuidad de negocios. La primera provee a la organización la capacidad necesaria para contener las distintas amenazas que puedan interrumpir su funcionamiento normal, dotando a los activos de controles que los mantengan protegidos; y la segunda, la continuidad de negocios otorga la flexibilidad para reaccionar ante un evento mayor que interrumpa los procesos productivos, y retornar en el menor tiempo posible a su equilibrio operacional. Tanto la seguridad como la continuidad de negocios proveen control sobre los riesgos operacionales, siendo ambos elementos totalmente complementarios y necesarios para el desarrollo de la iniciativa.

2) La inversión para implementar controles se hace de manera eficiente.

El componente de BCM nos permite enfocar los recursos hacia los procesos críticos del negocio y sus activos relacionados, de esta manera se destinan los recursos necesarios para cubrir los riesgos que traigan mayor impacto al cumplimiento de los objetivos del negocio, evitando el despilfarro o gasto innecesario en elementos que no tienen un nivel de criticidad alto para la organización.

3) Es fundamental el apoyo de la dirección de la empresa.

El apoyo de la alta gerencia es fundamental en todo el desarrollo de la iniciativa, producto que en la dirección de la organización cae la responsabilidad última de proteger la empresa y sus activos. Son varias las ventajas de esta consideración:

- En la definición del alcance de la iniciativa son considerados de manera eficaz los requerimientos del negocio y los objetivos estratégicos, definiendo un apetito de riesgo alineado con estos elementos.
- Se acelera la toma de decisiones ante medidas correctivas que sea necesario evaluar o implementar.
- Al tener el apoyo político de la máxima autoridad de la organización, se garantiza la participación de todas las áreas involucradas, logrando afinar de manera adecuada el alcance de la iniciativa considerando todos los elementos críticos de los procesos de negocio.
- La mantención del proceso de resiliencia se hace menos costosa, producto que se puede delegar la responsabilidad en cada unidad de negocio para mantener actualizados los elementos relevantes de sus procesos críticos en el BCP corporativo.

4) La iniciativa es aplicable a cualquier organización sin importar su tamaño.

El modelo planteado en este trabajo se ajusta a cualquier tipo de organización cuya operación dependa de las tecnologías de información, sin importar su tamaño. Producto que permite enlazar los objetivos de TI con los objetivos estratégicos, al orientar la gestión de riesgos hacia sus procesos críticos. Cada empresa maneja sus propios criterios y factores de riesgo, aunque sea de manera informal, y esta iniciativa permite alinear los controles de manera realista. No es una certificación de una norma donde deben cumplir una seria de elementos y protocolos que muchas veces se vuelven inmanejables para empresas de recursos limitados.

5 GLOSARIO

Activo: Algo ya sea tangible o intangible que es necesario proteger por la organización, incluyendo personas, información, infraestructura, finanzas y reputación.

Activo de información: Información y/o datos que tienen valor para la organización y deben ser protegidos de acuerdo a su criticidad.

Accountability: Responsabilidad individual de los sujetos sobre los activos. También define el rol sobre los sistemas y procesos de negocio.

Active Directory: Directorio Activo, es la herramienta de Microsoft para administrar el control de acceso a las redes de computadores y sus recursos.

Amenaza: Cualquier elemento (Ej. Objeto, sustancia, persona) que es capaz de actuar contra un activo de tal manera que provoque un daño.

Análisis de riesgo: Proceso por el cual se estima la frecuencia e impacto de un riesgo.

Apetito de riesgo: El nivel de riesgo, a un nivel general, que una entidad está dispuesta a aceptar en virtud de su misión.

Autenticación: El acto de verificar identidad, también se puede referir a la verificación de la exactitud de una pieza de data.

Business Continuity Management (BCM): Gestión de continuidad de negocios, actividades destinadas a dirigir y controlar la continuidad operativa y comercial de una organización.

BCP: Siglas en inglés del Plan de Continuidad de Negocios, el cual es empleado por una organización para responder ante una interrupción de sus procesos críticos de negocio.

Análisis de Impacto de Negocio (BIA): Actividad que determina el impacto de perder el soporte de cualquier recurso de una organización, establece la escalada de perdidas en el tiempo, identifica los recursos mínimos necesarios para recuperarse, y prioriza la recuperación de los procesos y los sistemas que lo soportan.

British Standards Institution (BSI): Institución británica responsable del desarrollo y difusión de los estándares ISO a nivel mundial.

Caso de Negocio: Documentación que ayuda a sustentar la razón por la cual es necesario hacer una inversión de negocio, este documentos es usado para soportar una decisión de negocio, proceder con la inversión y para dar soporte a la dirección durante todo su ciclo de vida comercial.

Capability maturity model (CMM): Modelo desarrollado por el Instituto de Ingeniería de Software de la Universidad Carneggie Mellon, empleado por muchas organizaciones para identificar las mejores prácticas aplicables a la evaluación e incremento de la madurez de sus procesos. Adoptado ampliamente entre las empresas desarrolladoras de software.

Comité de Basilea: Comité organizado por los presidentes de los bancos centrales de los 10 países más industrializados del planeta (G-10), cuyas sesiones son realizadas en la ciudad de Basilea en Suiza desde 1975. Su propósito fundamental es fortalecer la solidez de los sistemas financieros, estableciendo las normativas y estándares para la supervisión bancaria.

Confidencialidad: Es la condición por la que la información no es divulgada a individuos, programas o procesos no autorizados.

Contenedor: Elemento ya sea técnico, humano o físico donde un activo de información es procesado, almacenado o transportado.

Control: Medida aplicada en un activo como resultado de un análisis y evaluación de riesgo para mitigar el impacto y/o probabilidad de ocurrencia del mismo.

Control de Acceso: Procesos, reglas y mecanismos de despliegue con los cuales se controla el acceso a los sistemas, recursos e instalaciones.

Custodio: Individuos y departamentos responsables del almacenamiento y protección de los datos.

Disponibilidad: Atiende la necesidad que la información, los sistemas y los recursos estén disponibles para los usuarios, de manera oportuna, de tal forma de no afectar la productividad.

Disaster recovery plan (DRP): Plan de recuperación de desastres, complementa al BCP aportando los procedimientos para la puesta en marcha de la tecnología en el sitio de contingencia.

Conductor de negocio: Elementos del ambiente de la organización que impulsa sus decisiones estratégicas de negocio. Ej: la competencia, las características del mercado, etc.

Firewall: Cortafuego, dispositivo que permite filtrar el acceso desde una red a otra a través de la implementación de políticas, destinado para proteger la red local y sus recursos críticos de otras redes y sistemas estableciendo un perímetro de protección.

Servidor de archivos: Dispositivo de red que es el contenedor de los archivos procesados por los usuarios en la operación del negocio, cuyo acceso se otorga en virtud de los privilegios autorizado por el propietario de la información.

Factor de Riesgo: Una condición que puede influenciar la frecuencia y/o magnitud de un riesgo.

Gestión de riesgo: Actividades destinadas para dirigir y controlar los riesgos en una organización.

ISO/IEC: Siglas en inglés de Organización Internacional para la Estandarización / Comisión Electrotécnica Internacional, responsables de los estándares ISO/IEC 17999 y 27001.

ITIL: Siglas en inglés de La Biblioteca de Infraestructura de Tecnologías de la Información, la cual conforma un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas.

Magnitud: Una medida de la severidad de pérdidas potenciales tras eventos y/o escenarios de riesgo concretados.

Mapa de riesgo: Una herramienta gráfica para clasificar y mostrar el riesgo de acuerdo a rangos definidos de frecuencia y magnitud.

Objetivo de negocio: Un desarrollo de las metas de la organización en objetivos tácticos y los resultados deseables.

Proceso de negocio: Conjunto de actividades relacionadas entre sí llevadas a cabo para lograr un resultado de negocio que de valor a la organización.

Privilegios de Acceso: Los permisos o privilegios otorgados a los usuarios, programas o estaciones de trabajo para crear, cambiar, borrar o ver datos y archivos en los sistemas, definidos por los dueños de los datos y las políticas de seguridad.

Resiliencia: La habilidad de una organización o sistema para resistir fallas y de recuperase de una interrupción rápidamente, usualmente con un impacto mínimo.

Riesgo: Es la combinación de la probabilidad de eventos o amenazas y el impacto que esos eventos tengan en la organización.

Riesgo residual: Es el riesgo resultante posterior a la gestión y tratamiento de riesgos.

Riesgo de TI: Riesgo de negocio asociado con el uso, propiedad, operación, la participación, influencia y adopción de TI en la organización.

Tecnología de Información (TI): Tecnología asociada al proceso, presentación, almacenamiento y transporte de la información y los datos que soportan los procesos de negocio.

Tolerancia de Riesgo: El nivel aceptable de variación que la organización está dispuesto a permitir por un riesgo particular en virtud de sus objetivos.

Vulnerabilidad: Una debilidad en el diseño, implementación, operación o control interno de un proceso que podría exponer a los activos a las amenazas y sus escenarios adversos

6 BIBLIOGRAFIA.

- CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL (CRISC) Review Manual 2011. ISACA. www.isaca.org.

- All In One CISSP Exam Guide, 4° Edition. Shon Harris, MC Graw Hill. 2008

- US NIST Publication 800-34. Contingency Planning Guide for Federal Information Systems.

- US NIST Publication 800-30. Risk Management Guide for Information Technology Systems.

- Estándar BSI ISO/IEC 27001:2005, Sistemas de Gestión de Seguridad de la Información.

- Estándar BSI ISO/IEC 17999, Código para la práctica de la seguridad e la información.

- Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Software Engineering Institute. May 2007. Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson.

- Requerimiento de capital por riesgo operacional en Basilea II: enfoque estándar alternativo. Luis Raúl Romero. Enero 2007.

- Norma de carácter general N° 309 de la Super intendencia de Valores y Seguros. Principios de Gobiernos Corporativos y Sistemas de Gestión de Riesgo y Control Interno.

- Sustaining Operational Resiliency: A Process Improvement Approach to Security Management. Richard A. Caralli. April 2006.

- Marcos de Riesgos de TI. Risk IT basado en Cobit. 2009 ISACA. www.isaca.org.