UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

DESARROLLO DEL PLAN DE CONTINUIDAD DEL NEGOCIO PARA LA EMPRESA EQUIVIDA S.A PARA EL PERÍODO 2012-2015

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR: ANDRÉS LEONARDO CÁRDENAS PALLO

Sangolquí, Noviembre del 2013

AUTORIZACIÓN

Yo, ANDRÉS LEONARDO CÁRDENAS PALLO, autorizo a la Universidad de las Fuerzas Armadas - ESPE a que publique en el repositorio digital de la biblioteca Alejandro Segovia el presente proyecto de tesis, así como también los materiales y documentos relacionados a la misma.

Sangolquí, Noviembre del 2013

_____

ANDRÉS CÁRDENAS

DECLARACIÓN

Yo, Andrés Leonardo Cárdenas Pallo, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad de la Fuerzas Armadas - ESPE, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Sangolquí, Noviembre del 2013

_____

ANDRÉS CÁRDENAS

CERTIFICACIÓN

Certificamos que el presente trabajo, fue realizado en su totalidad por el Sr. Andrés Leonardo Cárdenas Pallo como requerimiento parcial a la obtención del Título de **INGENIERO EN SISTEMAS E INFORMÁTICA,** bajo nuestra supervisión.

Sangolquí, Noviembre del 2013

_____	_____
Ing. Mario Ron	Ing. Víctor Paliz
DIRECTOR	**CODIRECTOR**

DEDICATORIA

Dedico este trabajo a mis padres, que gracias a su esfuerzo y apoyo constante me permitieron culminar una etapa más de mi vida con éxito. Gracias por inculcarme valores, principios y lo más importante entregarme su amor.

A mi amada esposa Liseth y mi tesoro Emmy que son la base fundamental para lograr todos los objetivos que me he propuesto.

A mis hermanos por siempre estar a mi lado, apoyándome y enseñándome con su ejemplo el concepto de perseverancia.

ANDRÉS CÁRDENAS

AGRADECIMIENTO

Agradezco a la Universidad de las Fuerzas Armadas junto a todos mis profesores que participaron en mi formación académica.

A la empresa de Seguros Equivida por la apertura prestada para el desarrollo del tema y su apoyo en información y tiempo entregado.

A mi Director de Carrera Ing. Mauricio Campaña por el apoyo en todo el proceso.

A mi Director de Tesis Ing. Mario Ron, a mi Codirector Ing. Víctor Paliz por su apoyo, tiempo y paciencia para el desarrollo del tema.

Gracias

ANDRÉS CÁRDENAS

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES Y TABLAS

RESUMEN

Constantemente se experimentan situaciones de emergencia, directa o indirectamente dentro de las empresas, las cuales necesitan respuestas inmediatas. El Plan de Continuidad del Negocio (BCP) permite establecer los procedimientos para asegurar la continuidad de una empresa en caso de que esta se viera sometida a una interrupción no deseada de su negocio. El desarrollo del presente trabajo está orientado al desarrollo del Plan de Continuidad del Negocio (BCP) dentro de una empresa de servicios de Seguros de Vida. Para el desarrollo se incluye una breve descripción de la empresa, se evalúa los posibles riesgos y amenazas a las que está expuesta, se realiza un Análisis de Impacto del Negocio que es el punto de partida para crear estrategias de continuidad, se define un conjunto de equipos para el restablecimiento de operaciones y los procedimientos que los mismos necesitan para dar continuidad al negocio, finalmente se da a conocer las conclusiones y recomendaciones del trabajo desarrollado.

Palabras Clave:

BCP - Continuidad del Negocio

BIA- Impactos del Negocio

Amenazas al Negocio

CAPÍTULO 1

ANÁLISIS DE LA EMPRESA DE SEGUROS EQUIVIDA

La competitividad creciente entre las organizaciones empresariales, las demandas cada vez más exigentes de los stakeholders y de los requerimientos regulatorios cada vez más restrictivos, son agentes que hoy en día fuerzan a las empresas a demostrar la resistencia de las actividades de negocio a permanecer activas ante cualquier posible incidente grave.

Uno de los inconvenientes a las que se enfrentan las organizaciones es cuando deciden afrontar cualquier tipo de iniciativa relacionada con la continuidad del negocio, es la falta de conocimiento y de procedimientos claros y concisos que detallen por dónde empezar y los factores a tener en cuenta para garantizar el éxito.

La Continuidad del Negocio es un concepto que abarca tanto la Planeación para Recuperación de Desastres (DRP) como la Planeación para el Restablecimiento del Negocio.

Recuperación de Desastres es la capacidad para responder a la interrupción de los servicios mediante la implementación de un plan para restablecer las funciones críticas de la organización.

La planeación para el restablecimiento del negocio es un plan con procedimientos secuenciales y lógicos que permiten volver a la normalidad los servicios críticos y dar continuidad a los procesos.

1.1. ANTECEDENTES

EQUIVIDA COMPAÑÍA DE SEGUROS Y REASEGUROS S.A, es una empresa que se dedica a ofrecer seguros y reaseguros para vida y riesgos personales a través de pólizas individuales y colectivas desde hace 18 años, la misma tiene 300 colaboradores los mismos que se encuentran en las diferentes ciudades donde opera.

La matriz está situada en el cantón Quito, cuenta con sucursales en Guayaquil, Cuenca y agencias en Ambato y Manta.

EQUIVIDA en los últimos años ha tenido un crecimiento acelerado, por lo cual se ven en la necesidad de mejorar los procesos y políticas; el último año se pone énfasis en determinar los servicios considerados críticos en la compañía, lo cual generó la necesidad de crear un Plan de Continuidad del Negocio en caso de que estos servicios se vean afectados y contar con procedimientos para el restablecimiento de los mismos.

1.2. JUSTIFICACIÓN

La empresa EQUIVIDA S.A entró a un proceso de mejoramiento de sus políticas y procesos con lo cual encontró la necesidad de desarrollar un Plan de Continuidad del Negocio con enfoque en los servicios críticos de la compañía, además en auditorías externas realizadas al área de tecnología se realizaron observaciones por no contar con un Plan de Continuidad del Negocio.

La empresa pone énfasis en tener un Plan para proteger la continuidad de las operaciones, salvaguardar al recurso humano y tecnológico, mantener resguardada la información y que cumpla con sus pilares fundamentales de: seguridad, disponibilidad y confiabilidad.

El Plan es necesario para identificar roles y responsabilidades específicas, que se encarguen del seguimiento y continuidad de los procesos para entregar los servicios necesarios a sus clientes y proveedores aún fuera de las instalaciones normales a la compañía.

Al desarrollar el Plan de Continuidad del Negocio (BCP) se tendrá al alcance de los directivos una herramienta que aporte a tomar decisiones asertivas en momentos de crisis y tener identificados los activos críticos.

De la misma manera el tener identificado los riesgos primordiales a los que se vería expuesta la compañía permite una mejor planificación para la asignación de recursos humanos, técnicos y económicos a largo plazo.

El resultado de la investigación permitirá a la empresa Equivida contar con un plan estratégico de prevención y recuperación de los servicios críticos en caso de un desastre, además la empresa afirmará la solidez de sus servicios ante cualquier desastre permitiendo servir a sus clientes, demostrando la responsabilidad social y evitando cualquier tipo de demanda por negligencia como empresa.

Desde la perspectiva institucional este proyecto permitirá fortalecer al negocio implementando planes que ayuden a mitigar desastres que impidan el normal desenvolvimiento del mismo.

1.3. EL PROBLEMA

La empresa Equivida está expuesta a un alto riesgo de pérdida de activos, información y prestigio debido a la paralización de los servicios informáticos, ante la falta de un plan de continuidad.

1.4. PREGUNTAS DE INVESTIGACIÓN

- ¿Cómo la empresa Equivida podrá minimizar el impacto de la materialización de riesgos?
- ¿Cuáles son los servicios críticos de Equivida?
- ¿Qué es el Análisis de Impacto del Negocio?
- ¿Qué metodología se utilizará para realizar el Plan de Continuidad del Negocio para aplicarse en Equivida?
- ¿Cuáles son las actividades a seguir en caso de una contingencia?

1.5. OBJETIVOS

1.6.1 OBJETIVO GENERAL

Desarrollar el Plan de Continuidad del Negocio para la empresa Equivida para asegurar la continuidad de los servicios críticos del negocio.

1.6.2 OBJETIVOS ESPECÍFICOS

- Realizar la investigación bibliográfica para determinar la metodología del Plan de Continuidad del Negocio.
- Diseñar el plan y establecer políticas de Continuidad del Negocio.
- Identificar los servicios críticos del negocio.
- Analizar y evaluar los riesgos.
- Realizar el análisis de impacto en el negocio (BIA).
- Definir estrategias de mitigación y recuperación.

1.6. ALCANCE

El plan es exclusivamente para la compañía Equivida para la ciudad de Quito, el entregable será un documento físico el cual contendrá el Plan de Continuidad del Negocio

El plan considera los siguientes aspectos:

- Identificación de los servicios críticos de la empresa y análisis de riesgo de los mismos.
- Listado de amenazas que pueden afectar a la compañía en su situación actual.
- Escenarios de vulnerabilidad de la empresa.
- Evaluación y valoración de riesgos.
- Recomendaciones y contramedidas.
- Estrategia de recuperación de los servicios críticos.
- Lista de los servicios y la información que debe recuperarse en orden de prioridad.
- Roles, responsabilidades y procedimientos establecidos para la utilización del Plan de Continuidad del Negocio.
- Las tareas y actividades que se llevarán a cabo, la identificación de responsabilidades para cada tarea.
- Tareas que se emprenderán después de la recuperación y restauración.

El plan no considera los siguientes aspectos:

- Procedimientos de evacuación y Emergencias de edificios.
- Procedimientos de restauración de infraestructura que no participe en los servicios críticos.
- Plan de recuperación de las sucursales de Equivida.
- Plan de restablecimiento de servicios considerados no críticos.

1.7. ACTIVIDADES

Para el desarrollo del proyecto se utilizará la Metodología del Business Continuity Plan (BCP) cuyas fases y actividades se presenta

Ilustración 1 Metodología del Plan de Continuidad del Negocio

Fase 1.- Análisis de Impacto al Negocio: Se determina que procesos son esenciales para la continuidad de las operaciones y se calcula su posible impacto.

Fase 2.- Estudio de Riesgos: En esta fase se calcula el riesgo, la apreciación de su impacto en el negocio y la posibilidad de ocurrencia.

Fase 3.- Estrategias de Continuidad: Es el conjunto de procedimientos definidos para asegurar la reanudación oportuna y ordenada de los procesos del negocio generando un impacto mínimo o nulo ante una contingencia

Fase 4.- Desarrollo del Plan: Se diseña, desarrolla e implementa los planes de continuidad del negocio para proveer continuidad en los marcos establecidos por la Estrategia de Continuidad.

Fase 5.- Pruebas del Plan: En esta fase se planifica y coordina el plan de ejercicios y documenta los resultados de los mismos, se define escenarios, criterios de evaluación y cronogramas.

CAPÍTULO 2

2.1. NORMA ISO 22301

La norma ISO 22301 es a nivel mundial, la primera norma internacional para la gestión de la continuidad de negocio (SGCN) y ha sido desarrollada para ayudar a las organizaciones a minimizar el riesgo de este tipo de interrupciones, la ISO 22301 tiene se define: “Seguridad de la sociedad – Sistemas de gestión de la continuidad de negocio – Requisitos”, y es la nueva norma internacional para sistemas de gestión de la continuidad de negocio (SGCN). Esta norma remplazará la norma actual británica BS25999.

La norma ISO 22301 especifica requisitos para planificar, establecer, implantar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión documentado para prepararse, responder y recuperarse de eventos que generan interrupciones, cuando éstos ocurren.

Los requisitos especificados en ISO 22301 son genéricos y pretenden ser aplicables a todas las organizaciones (o partes de las mismas), sin importar su tipo, tamaño y naturaleza. El grado de aplicación de estos requisitos depende del ambiente operativo y de la complejidad de la organización.

La estandarización de la continuidad de negocio evoluciona con ISO 22301, agregando:

- Mayor énfasis en el establecimiento de objetivos, seguimiento del desempeño y de los indicadores.
- Expectativas más claras sobre la Dirección.
- Planificación y preparación más cuidadosas de recursos requeridos para el aseguramiento de la continuidad de negocio.

La norma ISO 22301 puede ser aplicada a todo tipo y tamaño de organizaciones que quieran:

- Establecer, implantar, mantener y mejorar un SGCN.
- Asegurar conformidad con la política establecida de la continuidad de negocio de la organización.
- Demostrar conformidad a los demás.
- Buscar certificación/registro de su SGCN por un organismo externo de certificación.
- Realizar una autodeterminación y auto declaración de conformidad con esta norma internacional.

La norma ISO 22301 está organizada en las siguientes cláusulas principales:

CLÁUSULA 4: Contexto de la organización

Ilustración 2 Alineamiento estratégico

Determine temas internos y externos que son relevantes para el propósito de la organización y que afectan su habilidad de alcanzar los resultados esperados de su SGCN, tales como:

- Las actividades de la organización, sus funciones, servicios, productos, sociedades, cadenas de suministros, relaciones con las partes interesadas y el impacto potencial relacionado con un incidente que genere una interrupción.
- Vínculos entre la política de continuidad de negocio y los objetivos de la organización y otras políticas, incluyendo, la estrategia de gestión de riesgos globales; el apetito por el riesgo de la organización; las necesidades y expectativas de las partes interesadas relevantes; leyes, regulaciones y otros requisitos aplicables, a los cuales la organización está suscrita.
- Identificar el alcance del SGCN, tomando en cuenta los objetivos estratégicos de la organización, sus productos y servicios claves, su tolerancia al riesgo y cualquier obligación reglamentaria, contractual o de sus partes interesadas, también forma parte de esta cláusula.

CLÁUSULA 5: LIDERAZGO

La alta dirección debe demostrar un compromiso continuo con el SGCN. A través de su liderazgo y acciones, la dirección puede crear un ambiente en el cual distintos miembros del personal estén completamente involucrados y el sistema de gestión pueda funcionar de manera eficaz en sinergia con los objetivos de la organización. La dirección es responsable de:

- Asegurar que el SGCN es compatible con la dirección estratégica de la organización.

- Integrar los requisitos del SGCN en los procesos de negocios de la organización.
- Proveer los recursos necesarios para el SGCN.
- Comunicar la importancia de la gestión de continuidad de negocio eficaz.
- Asegurar que el SGCN alcanza sus resultados esperados.
- Dirigir y apoyar la mejora continua.
- Establecer y comunicar la política de continuidad de negocio.
- Asegurar que los objetivos y planes del SGCN se establecen.
- Asegurar que las responsabilidades y autoridades, para las funciones relevantes, se asignen.

CLÁUSULA 6: PLANIFICACIÓN

Esta es una etapa crítica en la que se establecen objetivos estratégicos y principios para la orientación del SGCN en su totalidad. Los objetivos del SGCN son una expresión del propósito de la organización para el tratamiento de los riesgos identificados y/o para cumplir con los requisitos de las necesidades de la organización. Los objetivos de la continuidad de negocio deben:

- Ser consistentes con la política de continuidad de negocio.
- Tomar en cuenta el nivel mínimo de productos y servicios que es aceptable para que la organización alcance sus objetivos.
- Ser medibles.
- Tomar en cuenta requisitos aplicables.

CLÁUSULA 7: SOPORTE

La gestión diaria de un sistema de gestión de la continuidad de negocio, se basa en el uso de recursos apropiados para cada actividad, estos recursos incluyen personal competente en base a formaciones y servicios de soporte, toma de conciencia y comunicación pertinentes (y demostrables), esto debe ser apoyado por información documentada adecuadamente gestionada.

Las comunicaciones, tanto internas como externas, deben ser consideradas en esta área, incluyendo su formato, contenido y el momento oportuno de estas comunicaciones.

Los requisitos para la creación, actualización y control de la información documentada, también se especifican en esta cláusula.

CLÁUSULA 8: OPERACIÓN

Después de la planificación del SGCN, la organización debe ponerlo en funcionamiento. Esta cláusula incluye:

Análisis de impacto en el negocio (Business Impact Analysis-BIA): Esta actividad permite que una organización identifique los procesos críticos que apoyan a sus productos y servicios claves, las interdependencias entre procesos y recursos requeridos para operar los procesos en un nivel mínimamente aceptable**.**

Ilustración 3 Análisis de riesgos empresarial y bcp

Evaluación de riesgos: La norma ISO 22301 propone referirse a la norma ISO 31000 para implantar el proceso, la meta de este requisito es establecer, implantar y mantener un proceso formal documentado de valoración de riesgos que identifique, analice y evalúe sistemáticamente el riesgo de incidentes que generen interrupciones en la organización.

Estrategia de continuidad de negocio: Una vez que los requisitos se han establecido a través del análisis de impacto en el negocio y la evaluación de riesgos, las estrategias pueden ser desarrolladas para identificar disposiciones que permitan que la organización proteja y recupere actividades críticas, basadas en la tolerancia de riesgo organizacional y dentro de objetivos de tiempo de recuperación definidos, la experiencia y las buenas prácticas indican claramente, que las previsiones tempranas de una estrategia global de SGCN, aseguran que las actividades de SGCN estén alineadas y apoyen la estrategia global de negocios de la organización.

La estrategia de continuidad de negocios debe ser un componente integral de la estrategia corporativa de la institución.

Procedimientos de continuidad de negocio: La organización debe documentar los procedimientos (incluyendo las disposiciones

necesarias) para asegurar la continuidad de las actividades y la gestión de un incidente que genere una interrupción. Los procedimientos deben:

- Establecer un protocolo adecuado de comunicaciones internas y externas.
- Ser específicos en relación a los pasos inmediatos a ser tomados durante una interrupción.
- Ser flexibles para responder a amenazas no anticipadas y a condiciones internas y externas cambiantes.
- Enfocarse en el impacto de eventos que puedan potencialmente interrumpir operaciones.
- Ser desarrollados bajo hipótesis establecidas y análisis de interdependencias.
- Ser efectivos en minimizar las consecuencias a través de la implantación de estrategias de mitigación adecuadas.

Ejercicios y pruebas: Para asegurar que los procedimientos de continuidad de negocio son consistentes con sus objetivos de continuidad de negocio, las organizaciones deben hacer pruebas regularmente.

Los ejercicios y las pruebas son procesos de validación de planes y procedimientos de la continuidad de negocio para asegurar que las estrategias seleccionadas son capaces de proveer resultados de respuesta y recuperación dentro de plazos acordados con la gerencia

Tipo de ejercicio	¿Qué es?	Beneficios	Desventajas
Lista de verificación	Distribuye planes para revisión	Asegura que el plan cubra todas las actividades	No está dirigido hacia la eficacia
Recorrido estructurado	Mirada detallada a cada paso del Plan de Continuidad de Negocio (PCN)	Asegura que las actividades planificadas estén descritas correctamente en el PCN	Valor bajo al probar las capacidades de respuesta
Simulación	Escenario para representar los procedimientos de recuperación	Sesión práctica	Cuando los subconjuntos son muy distintos
Paralelo	Prueba total, pero procesamiento principal no es interrumpido	Asegura un alto nivel de confiabilidad sin interrumpir las operaciones normales	Costoso ya que todo el personal se involucra
Interrupción total	El desastre es replicado al punto de interrumpir las operaciones normales	Prueba más confiable del PCN	Arriesgado

Ilustración 4 Tipo de pruebas

CLÁUSULA 9: EVALUACIÓN DEL DESEMPEÑO

Una vez que el SGCN se ha implementado, la norma ISO 22301 requiere permanente seguimiento del sistema, así como revisiones periódicas para mejorar su operación:

- Seguimiento de la medida en la cual la política, objetivos y metas de continuidad de negocio son cumplidos.
- Medición del desempeño de los procesos, procedimientos y funciones que protegen las actividades priorizadas.
- Seguimiento de la conformidad con esta norma y con los objetivos de la continuidad de negocio.
- Seguimiento histórico de evidencia de desempeño deficiente del SGCN.
- Realización de auditorías internas a intervalos planificados.
- Evaluación de todo lo anterior en las revisiones por la dirección, a intervalos planificados.

CLÁUSULA 10: MEJORA

La mejora continua puede ser definida como todas las acciones, realizadas a lo largo de la organización, para aumentar la eficacia (cumplir objetivos) y la eficiencia (proporción costo/beneficio óptima) de los procesos y controles de seguridad para brindar más beneficios a la organización y a sus partes interesadas.

Una organización puede mejorar continuamente la eficacia de su sistema de gestión a través del uso de la política de continuidad de negocio, los objetivos, los resultados de auditorías, el análisis de eventos controlados, los indicadores, las acciones correctivas y preventivas y la revisión por la dirección

¿Cómo encaja la continuidad del negocio en la gestión general?

La continuidad del negocio es parte de la gestión general del riesgo en una compañía y tiene áreas superpuestas con la gestión de seguridad y tecnología de la información.

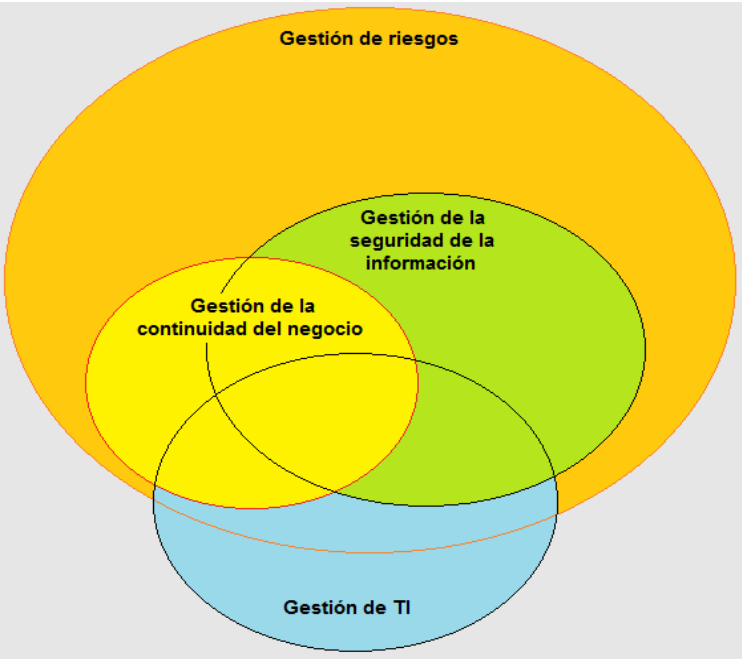


Ilustración 5 Mapa de gestión de riesgos empresariales

BENEFICIOS DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

- La adopción de una estrategia de continuidad constituye un ejercicio de responsabilidad y predisposición a anticiparse a cualquier tipo de evento adverso que haga peligrar el negocio.
- Aparte de prevenir o minimizar las pérdidas para el negocio que un desastre puede causar, el objetivo principal de cualquier programa orientado a gestionar la continuidad de negocio de una organización es garantizar que ésta dispone de una respuesta planificada ante cualquier trastorno importante que puede poner en peligro su supervivencia, esta afirmación de por sí constituye un argumento irrefutable que explica la necesidad de instaurar en todas las compañías tales estrategias, independientemente de su tamaño y/o sector de actividad.
- Ventaja competitiva frente a otras organizaciones: el hecho de mostrar que se toman medidas para garantizar la continuidad de negocio mejora la imagen pública de la organización y revaloriza la confianza frente a accionistas, inversores, clientes y proveedores.
- Por otra parte, el retorno de la inversión (ROI) en aspectos de continuidad es más perceptible en términos de reputación e imagen pública.

- Gestión preventiva de los riesgos: a través de la gestión de la continuidad, una organización es capaz de abordar la gestión proactiva de amenazas y riesgos que pueden impactar en sus operaciones.
- Previene o minimiza las pérdidas de la organización en caso de desastre: es capaz de identificar de forma proactiva los posibles impactos e inconvenientes que una interrupción de sus actividades de negocio puede provocar.
- Asegura la “resiliencia” de las actividades de negocio ante interrupciones, aumentando la disponibilidad de los servicios dispuestos para el cliente.
- Menor riesgo de sufrir sanciones económicas al adaptarse a requerimientos regulatorios.
- Asignación más eficiente de las inversiones en materia de seguridad, todo plan de continuidad de negocio está diseñado conforme a un proceso previo de análisis de riesgos, el cual permite priorizar los mismos y fijar los esfuerzos y los presupuestos en las áreas más necesitadas.

Términos básicos utilizados en la norma

Sistema de gestión de la continuidad del negocio (SGCN): parte del sistema general de gestión que se encarga de planificar, mantener y mejorar continuamente la continuidad del negocio.

Interrupción máxima aceptable (MAO): cantidad máxima de tiempo que puede estar interrumpida una actividad sin incurrir en un daño inaceptable (también Período máximo tolerable de interrupción [MTPD]).

Objetivo de tiempo de recuperación: tiempo predeterminado que indica cuándo se debe reanudar una actividad o se deben recuperar recursos.

Objetivo de punto de recuperación (RPO): pérdida máxima de datos; es decir, la cantidad mínima de datos que necesita ser restablecida.

Objetivo mínimo para la continuidad del negocio (MBCO): nivel mínimo de servicios o productos que necesita suministrar o producir una organización una vez que restablece sus operaciones comerciales.

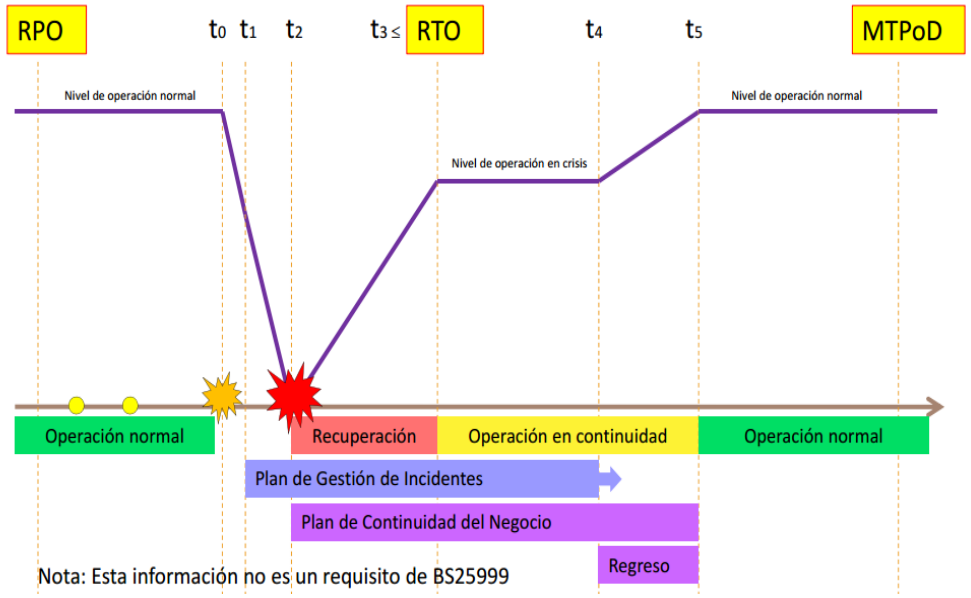


Ilustración 6 Términos utilizados en la norma

Si una organización desea implementar esta norma, la siguiente documentación es obligatoria:

1. Alcance del SGCN
2. Política de la Continuidad del Negocio

3. Objetivos de la continuidad del negocios
4. Evidencia de competencias del personal
5. Registros de comunicación con las partes interesadas
6. Análisis del impacto en el negocio
7. Evaluación de riesgos, incluido un perfil de riesgo
8. Estructura de respuesta a incidentes
9. Planes de continuidad del negocio
10. Procedimientos de recuperación
11. Resultados de acciones preventivas
12. Resultados de supervisión y medición
13. Resultados de la auditoría interna
14. Resultados de la revisión por parte de la dirección
15. Resultados de acciones correctivas

Normas relacionadas

Otras normas de ayuda en la implementación de la continuidad del negocio son:

ISO/IEC 27031:2011 – Lineamientos para preparación de tecnología de la información y comunicación para la continuidad del negocio

PAS 200 – Gestión de crisis: orientación y buenas prácticas

PD 25666 – Orientación para prueba y verificación de programas de continuidad y contingencia

PD 25111 – Orientación sobre aspectos humanos de la continuidad del negocio

ISO/IEC 24762 – Lineamientos sobre servicios de tecnología de la información y comunicación para recuperación de desastres

ISO/PAS 22399 – Lineamientos sobre preparación para incidentes y gestión de continuidad operativa

ISO/IEC 27001 – Sistemas de gestión de seguridad de la información: requisitos

2.2. ¿QUÉ ES UN PLAN DE CONTINUIDAD DEL NEGOCIO (BCP)?

Es el conjunto de procedimientos y estrategias de una organización para asegurar la reanudación oportuna y ordenada de los procesos del negocio en un plazo predefinido y con un coste acotado ante un incidente o interrupción.

Un Plan de Continuidad de Negocio está orientado al mantenimiento del negocio de la organización, con lo que priorizará las operaciones de negocio críticas necesarias para continuar en funcionamiento después de un incidente no planificado.

Un Plan de Continuidad reducirá el número y la magnitud de las decisiones que se toman durante un período en que los errores pueden resultar mayores.

El Plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos, acuerdos con entidades internas y externas.

La activación de un Plan de Continuidad debería producirse solamente en situaciones de emergencia y *cuando las medidas de seguridad hayan fallado.*

2.3. BENEFICIOS DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

- Identifica los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto financiero, humano y de reputación sobre la organización.
- Obliga a conocer los tiempos críticos de recuperación para volver a la situación anterior al desastre sin comprometer al negocio.
- Mantener el servicio prestado por los sistemas de información a los procesos del negocio, minimizando el impacto en la operación.
- Previene o minimiza las pérdidas para el negocio en caso de desastre.
- Clasifica los activos para priorizar su protección en caso de desastre.
- Aporta una ventaja competitiva frente a la competencia.
- Fomenta e implica a los recursos humanos de la compañía en las actividades de continuidad.

2.4. ENFOQUE DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

Para el desarrollo de un plan de continuidad exitoso, se tendrá en cuenta ciertos criterios:

- Compromiso, la alta administración deberá decidir y comunicar que es lo importante.
- Alcance, definir el alcance es uno de los puntos más importantes, aquí se define las fases, tiempo, recursos que se asignará al proyecto.
- Simple, evitar el diseño de planes complicados y con información que en el momento de un desastre no aportará a la continuidad.
- Personalizado, el tomar un plan ya desarrollado de una compañía de la misma línea, no aportará mayor valor; toda empresa siempre tiene sus procesos propios del negocio que necesitaran otro tipo de estrategias de recuperación.
- Entendible, el plan tiene que ser de fácil lectura y con procedimientos claros y sencillos de seguir.
- Probado, todo plan para que de valor al negocio tiene que ser probado y mejorado según los nuevos cambios de la empresa.

2.5. METODOLOGÍA DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

Para desarrollar un Plan de Continuidad de Negocio tenemos que empezar por obtener un conocimiento de la compañía: sus productos/servicios, sus objetivos empresariales, procesos internos, etc.

El propósito general de un Plan de recuperación es **obtener un mapa de acciones** que reduzcan “la toma de decisiones” durante las operaciones de recuperación, restaure los servicios críticos rápidamente y permita un normal funcionamiento de los sistemas y procesos lo antes posible, minimizando costes y aumentando la efectividad.

Se puede dividir un Plan de Continuidad de Negocio en cuatro Fases:

Ilustración 7 Diagrama de fases del plan de continuidad

2.5.1 FASE I. ANÁLISIS DEL NEGOCIO Y EVALUACIÓN DE RIESGOS

Para desarrollar un Plan de Continuidad con garantía de éxito, lo primero es conocer y entender cuáles son los procesos de negocio que son esenciales dentro de la compañía en la que se va a desarrollar el Plan, con

el objetivo de asegurar la continuidad de la actividad en caso de contingencia

Las actividades/procesos que se clasifican como esenciales dentro de una compañía suelen ser en su mayoría los Operacionales. Estos procesos interactúan directamente con los clientes o con otras organizaciones externas a la compañía

2.5.1.1 ANÁLISIS DE IMPACTO (BIA – BUSINESS IMPACT ANALYSIS):

Permite identificar la urgencia de recuperación de cada función de negocio, determinando el impacto en caso de interrupción, esta información permite seleccionar cuál es la estrategia más adecuada.

El nivel de criticidad de una actividad dentro de la compañía se mide en función de lo dependiente de ella, que es la organización y de lo que repercutiría su indisponibilidad.

En términos económicos esta valoración sería responder a la pregunta de cuánto perdería la organización si la actividad/proceso no estuviera disponible.

Dentro del Análisis de Impacto podemos distinguir las siguientes actividades:

a) **Obtención de la Relación de Procesos**

Establecer los procesos de negocio que se realizan en la compañía.

Clasificar los procesos en operativos y procesos de soporte. Los procesos operativos son aquellos que guardan una relación directa con el cliente (comercial, facturación, almacenaje, atención al cliente, etc.). Los procesos de soporte, serían aquellos que facilitan los “recursos” para poder realizar los procesos operativos (recursos humanos, gestión financiera, etc.)

b) **Obtención de la Relación de Aplicaciones**

Establecer la relación de aplicaciones que soportan los procesos de la compañía. Es el inventario de los recursos tecnológicos que soportan los procesos de la compañía, a fin de identificar aquellos que den soporte directo a los servicios críticos.

Los tipos de recursos que se deben analizar son:

- **Hardware,** identificando cada uno de los elementos hardware que soportan los sistemas de información de la compañía.
- **Software Base,** recogiendo todos aquellos componentes de software, incluido todos los asociados al sistema operativo, indispensables para el funcionamiento y optimización del Sistema de Información de la compañía.
- **Software de Aplicaciones,** inventariando las aplicaciones de gestión que son utilizadas en la empresa.
- **Sistemas de Infraestructura,** considerando aquellos elementos o componentes que sin disponer de una tecnología enfocada propiamente

al tratamiento de la información sí son requeridos para garantizan la operatividad del servicio.

c) **Relación de Departamentos y Usuarios**

Se identifican los departamentos que hay en la empresa y el nombre de las personas que la componen y que intervienen en los procesos.

Dentro del inventario de procesos es necesario conocer el personal involucrado en los mismos.

d) **Determinar los Procesos Críticos**

Pueden darse dos valoraciones, una basada en la importancia para la compañía de los procesos cuya ausencia tendría un impacto alto en la actividad de la compañía (valoración cualitativa). La otra, se referiría a las pérdidas económicas por período debido a la ausencia de los procesos (valoración cuantitativa).

Para simplificar esta valoración de los procesos podemos establecer una clasificación numérica, asignando mayor prioridad (p.e. 1) a aquellos procesos que se consideren más críticos y menor prioridad (p.e. 3) a aquellos que se consideren menos críticos.

e) **Período Máximo de Interrupción**

El acumulado de pérdidas suele ir creciendo linealmente a medida que pasan los días y las actividades están interrumpidas. No obstante, a

partir de un momento que denominaremos Período Máximo de Interrupción, las pérdidas sufren un aumento significativo y las funciones no podrían ser reasumidas.

Pueden existir procesos en los que el tiempo de recuperación es muy pequeño (horas), por ejemplo el servicio de banca electrónica de un banco, y otros procesos como la facturación a clientes en una empresa de servicios, pueden tener un periodo de recuperación mayor (días o semanas).

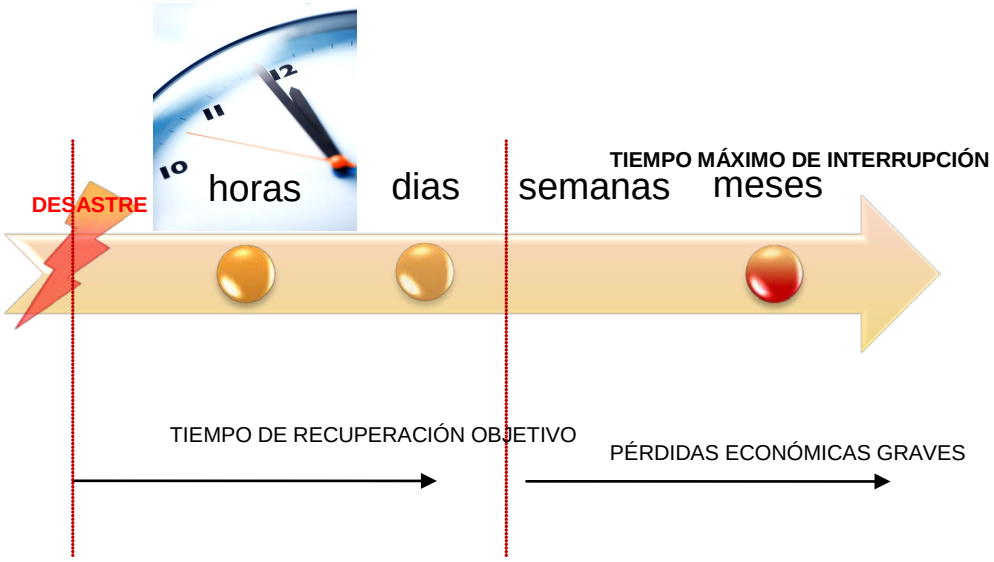


Ilustración 8 Tiempo de recuperación

En definitiva, el Análisis de Criticidad da una visión de los procesos, actividades y recursos a proteger con la prioridad de recuperación de cada uno de ellos, junto con los tiempos objetivo de puesta en marcha tras un incidente.

2.5.1.2 ANÁLISIS DE RIESGOS

La seguridad y el control dentro de las operaciones diarias de un negocio es una preocupación constante de sus clientes. Reducir el impacto de potenciales amenazas se logra estableciendo controles adecuados, procedimientos y prácticas antes de que los eventos de interrupción o desastre se materialicen.

El objetivo de un Análisis de Riesgos es poner de manifiesto aquellas debilidades actuales que por su situación o su importancia pueden poner en marcha, antes de lo deseable, el Plan de Recuperación de Negocio.

El Análisis de Riesgo debe centrarse en los procesos/actividades del negocio que se han considerado críticos, aunque también puede extenderse a aquellos que no lo son.

La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el coste que supondría. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

Las actividades principales son las siguientes:

- Identificar las amenazas físicas y las medidas correspondientes para la mitigación en el sitio, incluyendo amenazas internas y externas, seguridad y controles ambientales, seguridad y procedimientos de

respuesta a incidentes, procedimientos de respaldo y recuperación de datos, y prácticas de personal.

- Análisis de vulnerabilidad, identificar amenazas y debilidades en los controles que pudieran no haber sido diseccionados, o identificar posibles mejoras que puedan implementarse.
- Desarrollar sugerencias y recomendaciones para reducir la probabilidad de ocurrencia de las amenazas, incluyendo acciones de prevención y correctivas.
- Los objetivos de un Análisis de Riesgos son evaluar las amenazas físicas en contraposición con los controles para reducir la probabilidad de ocurrencia, y para mitigar el impacto de dichas amenazas. Los tipos de controles incluyen políticas y procedimientos de seguridad física, preparación para la respuesta a incidentes, y planes en sitio para implementar procedimientos y políticas para controles adicionales dentro de la organización. Los resultados de esta investigación se documentan en un reporte.

Los resultados del trabajo permitirán determinar:

- La probabilidad de potenciales amenazas identificadas.
- La vulnerabilidad de diversas funciones dentro de la compañía, para cada una de las amenazas.
- El costo efectivo de los controles en el sitio.
- La priorización requerido para la implementación de los controles.
- El cronograma de implementación de los controles requeridos.

Esquema del análisis del Riesgos

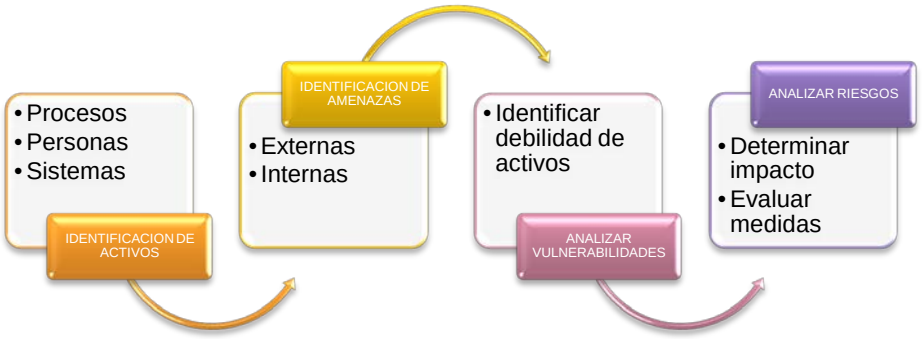


Ilustración 9 Esquema del análisis del riesgo

a) Análisis de Riesgos (definiciones)

Antes de iniciar con la metodología de ejecución del Análisis de Riesgos, es importante aclarar algunos conceptos que están asociados directamente con el tema y cuyo dominio es relevante.

Ilustración 10 Análisis de riesgos (definiciones)

b) Identificar los Activos

Los activos se definen como los recursos de una compañía que son necesarios para la consecución de sus objetivos de negocio.

Ejemplos de activos de una compañía pueden ser:

- Información
- Equipamiento
- Conocimiento
- Sistemas

Cada activo de la compañía tendrá unos costes asociados. En algunos casos estos costes pueden ser cuantificados con un valor económico (activos tangibles) como el software o el hardware, y en otros casos es más complicado cuantificar el activo con valores monetarios (activos intangibles) tales como el prestigio o la confianza de los clientes.

El proceso de elaborar un inventario de activos es uno de los aspectos fundamentales de un correcto análisis de riesgos. En este inventario se identificará claramente su propietario y su valor para la organización, así como su localización actual.

c) Identificar amenazas

Una amenaza se define como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus servicios.

Atendiendo a su origen, existen dos tipos de amenazas:

- **Externas:** que son causadas por alguien (hackers, proveedores, clientes, etc.), por situaciones naturales (tornados, tormentas, diluvios, etc.) o algo que no pertenece a la organización.
- **Internas:** estas amenazas son causadas por alguien que pertenece a la organización, por ejemplo errores de usuario o errores de configuración.

Las amenazas también pueden dividirse en dos grupos según la intencionalidad del ataque en deliberadas y accidentales:

- **Deliberadas**: cuando existe una intención de provocar un daño, por ejemplo un ataque de denegación de servicio o la ingeniería social.
- **Accidentales**: cuando no existe tal intención de perjudicar, por ejemplo las derivadas de desastres naturales.

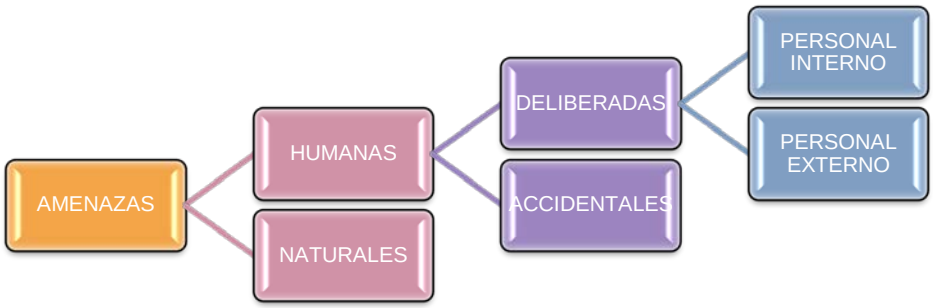


Ilustración 11 Esquema de amenazas

Evaluar vulnerabilidades

La vulnerabilidad es la posibilidad de la materialización de una amenaza sobre un activo, se mide con relación al nivel de sensibilidad que tiene una instalación, organización, sistema o un servicio a sufrir daños ante sucesos accidentales o intencionales.

Las vulnerabilidades en sí mismas no causan daño alguno, sino que es una condición o un conjunto de condiciones que pueden permitir a una amenaza afectar a un activo.

Evaluar el impacto y probabilidad

El impacto mide el nivel de daño provocado una vez manifestado el riesgo. Este nivel de impacto se puede medir (como ejemplo) con la calificación siguiente: insignificante, menor, moderado, significativo o catastrófico.

La probabilidad mide la capacidad de ocurrencia del riesgo en el tiempo, considerando niveles de (como ejemplo): muy poco probable, poco probable, moderada, probable y casi cierta.

Evaluación del riesgo

Los riesgos son la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Los riesgos pueden ser naturales o provocados por el hombre, son típicamente medidos en términos de probabilidad de ocurrencia y el impacto que estos generen.

El riesgo suele expresarse en términos cualitativos (Alto, Medio, Bajo).

Cuanto más baja sea la probabilidad de ocurrencia (no existan vulnerabilidades) y el impacto sobre la compañía sea también bajo, estaremos en un nivel de riesgo bajo, sin embargo, si existen vulnerabilidades que aumenten la probabilidad de ocurrencia o el impacto del incidente sea alto para la compañía, estaremos en unos niveles de riesgo medio-alto.

¿Qué es el nivel de riesgo?

Grado de exposición al riesgo que se determina a partir del análisis de la probabilidad y vulnerabilidad de ocurrencia del evento y de la magnitud de

su consecuencia potencial sobre el cumplimiento de los objetivos fijados. Permite establecer la importancia relativa del riesgo.

Ilustración 12 Acciones ante los riegos

2.5.1.3 METODOLOGÍAS DE ANÁLISIS DE RIESGO

Para la realización de un análisis de riesgos es recomendable tomar como referencia un modelo que nos brinde la certeza de considerar todos los escenarios de riesgos posibles por lo cual existen varias metodologías que ayudan a la correcta realización del análisis, detectando los riesgos existentes y asegurando la implantación de medidas. Las metodologías a considerarse son:

MAGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información fue desarrollada por el ministerio de administraciones públicas de Madrid, está enfocada a la información mecanizada y a los sistemas

informáticos que la tratan, dicha metodología nos permitirá saber cuánto de los activos de la empresa están en juego y como protegerlos.

MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de tratarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

Esta metodología propone las siguientes tareas a realizar:

Análisis de Riesgos

El análisis de riesgos es una técnica utilizada para determinar el riesgo siguiendo los siguientes pasos establecidos:

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- Determinar a qué amenazas están expuestos aquellos activos.
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Gestión del Riesgo

En esta tarea se resuelve que hacer con los riesgos e impactos determinados, incluye los siguientes pasos:

- Interpretación de los valores de impacto y riesgo residual.
- Selección de salvaguardas.
- Análisis de pérdidas y ganancias.
- Colaboración de la dirección de la empresa.
- Revisión de los activos de la empresa

OCTAVE

OCTAVE es una técnica efectiva de evaluación de riesgos creado por la oficina de patentes y negocios de los Estados Unidos.

OCTAVE es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo, esta técnica está en contra de la consultoría enfocada en el campo tecnológico, que tiene como objetivo los riesgos tecnológicos y en los temas tácticos, OCTAVE se enfoca en el riesgo organizacional y su objetivo principal son los temas relativos a la estrategia y a la práctica.

OCTAVE equilibra los siguientes aspectos:

- Riesgos operativos.
- Practicas de seguridad.
- Tecnología.

Lo cual permite a las compañías tomar decisiones de protección de información basados en los riesgos de confidencialidad, integridad y disponibilidad de los bienes relacionados a la información crítica.

Características:

- Es diferente de los análisis tradicionales enfocados a la tecnología.
- Es Auto dirigido.
- Flexible.

OCTAVE percibe los siguientes objetivos:

- Permitir la comprensión del manejo de los recursos
- Identificación y evaluación de los riesgos que afectan la seguridad dentro de una organización.
- Exige llevar la evaluación de la organización y del personal de la tecnología de información.

El método OCTAVE se enfoca en tres fases para examinar los problemas organizacionales y tecnológicos.

Fase 1

Durante esta fase se identifica la información de la organización. Los procesos que se realizan en esta fase son:

- Establecer criterios de evaluación de impacto
- Identificar sus criterios de seguridad
- Identificar sus amenazas
- Analizar los procesos tecnológicos relacionados

Fase 2

En esta fase se examina la infraestructura tecnológica y se realizan los siguientes procesos:

- Examinar rutas de acceso
- Analizar procesos tecnológicos

Fase 3

Durante esta fase se realiza la identificación de los riesgos, así como también se realizan estrategias de mitigación y planes de protección. Los procesos que intervienen en esta fase son:

- Evaluar el impacto de las amenazas
- Evaluar la probabilidad de ocurrencia de amenazas
- Seleccionar formas de mitigación de riesgos
- Desarrollar planes de mitigación de riesgos

2.5.2 FASE II. ESTRATEGIA DE RECUPERACIÓN

En esta fase se seleccionarán los métodos operativos alternativos que se van a utilizar en el caso de que ocurra un incidente que provoque una interrupción en la organización. El método seleccionado deberá garantizar la restauración de los procesos afectados en los tiempos determinados por el Análisis de Impacto.

2.5.2.1 SELECCIÓN DE ESTRATEGIAS

Ilustración 13 Selección de estrategias

De todas las alternativas existentes hay que elegir la más adecuada en cada caso. Dependerá de las necesidades de cada compañía, en cuanto a tiempos de recuperación, costes económicos, recursos, etc., Además deberá considerarse otros factores como:

- Ubicación y superficie requerida.
- Espacio suficiente.
- Zonas acondicionadas para acoger a personal.

Recursos técnicos necesarios:

- Hardware
- Software
- Comunicaciones
- Datos de respaldo

Recursos humanos requeridos

- Recursos materiales y de infraestructura.
- Servicios auxiliares necesarios.
- Tiempos de activación.
- Coste

2.5.2.2 DISEÑO ÓPTIMO DE LA ESTRATEGIA DE CONTINUIDAD

Desarrollar la Estrategia de Continuidad del Negocio (Lenner) que guíe a la organización a la restauración de sus operaciones de manera

rápida y controlada, manteniendo óptimo balance entre los costos de la interrupción y los costos de la estrategia de recuperación.

Suele ocurrir que cuanto menor sea el tiempo de recuperación objetivo, mayor será el coste de la solución. Por ello es conveniente realizar un análisis con tiempos de recuperación adecuados y adaptados a la realidad de la compañía.

Una vez tomada la decisión sobre el tipo de estrategia que se utilizará como respaldo en caso de interrupción del negocio, pasaremos a desarrollar todos los procedimientos, funciones y actividades que permitirán restablecer los procesos de negocio en unos plazos razonables.

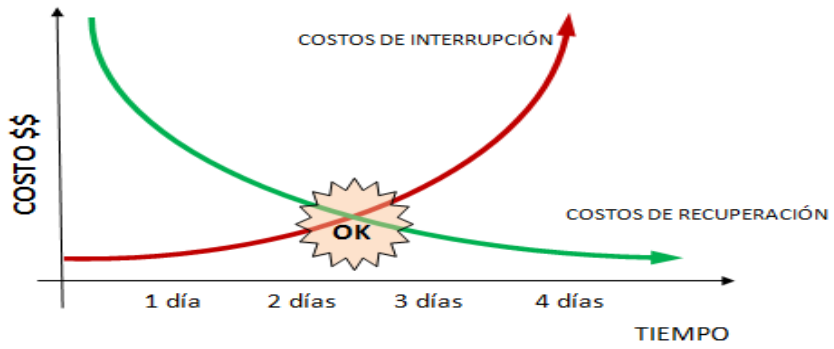


Ilustración 14 Costo vs. Tiempo

2.5.3 FASE III. DESARROLLO DEL PLAN DE CONTINUIDAD DEL NEGOCIO

2.5.3.1 COMPOSICIÓN DE EQUIPOS PARA EL PLAN

En esta fase se define:

- Los equipos necesarios para el desarrollo del Plan.
- Las responsabilidades y funciones de cada uno de los equipos.
- Las dependencias orgánicas entre los diferentes equipos.
- El desarrollo de los procedimientos de alerta y actuación ante eventos que puedan activar el Plan.
- Los procedimientos de actuación ante incidentes.
- La estrategia de vuelta a la normalidad.

Los equipos que se pueden integrar dependiendo de la empresa son:

a) **Equipo Comité de Crisis:** Encargado de dirigir las acciones durante la contingencia y recuperación.

Tareas:

- Análisis de la situación.
- Decisión de activar o no el Plan de Continuidad.
- Iniciar el proceso de notificación a los empleados a través de los diferentes responsables.
- Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación.

Equipo de Recuperación: Encargado de restablecer todos los sistemas necesarios (voz, datos, comunicaciones, etc.)

Tareas:

Restablecer todos los elementos necesarios para la restauración de un servicio considerado en el plan.

Equipo Logístico: Responsable de toda la logística necesaria en el esfuerzo de recuperación

Tareas:

- Transporte de material y personal al lugar de recuperación.
- Suministros
- Alimentación
- Contacta con proveedores.

Equipo de Atención a clientes: Encargados de concentrar la información y de la comunicación a los clientes

Tareas:

Ser el canal oficial de comunicación con todos los clientes.

Equipo de Unidades del Negocio: Personas que trabajan con las aplicaciones críticas.

Tareas:

Encargados de realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas.

2.5.3.2 DESARROLLO DE PROCEDIMIENTOS

Desarrollo de los procedimientos en cada una de sus fases

FASE DE ALERTA

- Procedimiento de lanzamiento del Plan
- Procedimiento de notificación de la puesta en marcha del Plan a los equipos implicados.

FASE DE TRANSICIÓN

- Procedimiento de concentración de equipos.
- Procedimiento de traslado y puesta en marcha de la recuperación.

FASE DE RECUPERACIÓN

- Procedimientos de restauración.
- Procedimientos de soporte y gestión.

FASE DE VUELTA A LA NORMALIDAD

- Análisis del impacto.
- Procedimientos de vuelta a la normalidad.

Ilustración 15 Fases y actividades del Plan de continuidad

2.5.4 FASE IV. PRUEBAS Y MANTENIMIENTO

2.5.4.1 PRUEBAS

OBJETIVOS DEL PLAN DE PRUEBAS

El Plan de Continuidad no se considerará válido hasta que no se haya superado satisfactoriamente el Plan de Pruebas que asegure la viabilidad de las soluciones adoptadas.

El Plan de Pruebas diseñado tiene como objetivos:

- Evaluar la capacidad de respuesta ante una situación de desastre que afecte a los recursos de la compañía.
- Probar la efectividad y los tiempos de respuesta del Plan para comprobar que están alineados con la definición realizada en el diseño.
- Identificar las áreas de mejora en el diseño y ejecución del Plan.
- Comprobar si los procedimientos desarrollados son adecuados para soportar la recuperación de las operaciones de negocio.
- Evaluar si los participantes del ejercicio están suficientemente familiarizados con la operativa en situación de contingencia.
- Concienciación y formación para los empleados a través de la realización de pruebas.

2.5.4.1 TIPOS DE PRUEBAS

Las pruebas de un Plan de Continuidad deben tener dos características principales:

a) Realismo: La utilidad de las pruebas se reduce con la selección de escenarios irreales. Por ello es importante reproducir escenarios que proporcionen un nivel de entrenamiento adecuado a las situaciones de riesgo.

b) Exposición Mínima: Las pruebas deben diseñarse de forma que impacten lo menos posible en el negocio, es decir, que si se programa una prueba que suponga una parada de los sistemas de información.

En algunos casos puede resultar complicado realizar una prueba completa del Plan de Continuidad de Negocio. Por ello, es necesario desarrollar un programa de pruebas planificado para garantizar que todos los aspectos de los planes y personal se han ensayado durante un período de tiempo.

EJERCICIOS TÉCNICOS

Este tipo de ejercicio requerirá la ejecución de procedimientos de notificación y operativos, el uso de equipos de hardware, software y posibles centros y métodos alternativos para asegurar un rendimiento adecuado. Ejemplos de elementos verificados durante un ejercicio de simulación son:

- Líneas de telecomunicaciones de backups.
- Procedimientos de notificación Vendedores / Clientes.
- Capacidad y rendimiento del hardware.
- Portabilidad del software.
- Accesibilidad al centro de respaldo.
- Movilización de los equipos de trabajo.
- Recuperación de ficheros y documentación almacenados en lugar externo.
- Recuperación de datos.

TEST COMPLETO

Los ejercicios de test son ejercicios planificados que implican la restauración real de la capacidad de proceso en un centro alternativo. Generalmente, los procesos en producción no son interrumpidos, pero puede planificarse su restauración y validación en el centro alternativo. Normalmente, este tipo de prueba requiere la participación de toda la organización de continuidad del negocio, incluyendo usuarios, personal técnico y de operaciones.

2.5.4.1 MANTENIMIENTO DEL PLAN DE CONTINUIDAD

Por la propia dinámica de negocio, se van incorporando nuevas soluciones a los Sistemas de Información y los activos informáticos van evolucionando para dar respuesta a las necesidades planteadas.

La correcta planificación del mantenimiento del Plan de Continuidad evitará que quede en poco tiempo obsoleto y que en caso de contingencia no pueda dar respuesta a las necesidades.

CAPÍTULO 3

3.1. ANTECEDENTES: CONOCIMIENTO DEL NEGOCIO

3.2. DESCRIPCIÓN FUNCIONAL DEL NEGOCIO

EQUIVIDA COMPAÑÍA DE SEGUROS Y REASEGUROS S.A, es una empresa que se dedica a ofrecer seguros y reaseguros para vida y riesgos personales a través de pólizas individuales y colectivas desde hace 18 años, la misma tiene 300 colaboradores los mismos que se encuentran en las diferentes ciudades donde opera.

3.3. RESEÑA HISTÓRICA DE LA EMPRESA EQUIVIDA

EQUIVIDA compañía de Seguros y Reaseguros S.A., empresa del GRUPO FUTURO nació jurídicamente el 19 de mayo de 1994, como una decisión estratégica de los socios y en respuesta a la creciente necesidad del mercado ecuatoriano por encontrar una compañía que responda a los requerimientos de seguridad, transparencia y eficiencia; autorizándose su funcionamiento con un capital social de mil millones de sucres.

EQUIVIDA tiene sus orígenes en el departamento de vida de Seguros Equinoccial, el grupo asegurador con más brillante trayectoria en el país, es justamente de allí donde la iniciativa por brindar una opción hasta esa entonces inexplotada, se convierte en la idea de lo que hoy en día es EQUIVIDA.

Para ello, no solo cuentan con el conocimiento y apoyo de Equinoccial, sino que se apoyan en el grupo de seguros de personas de mayor renombre de Colombia, Suramericana quienes para ese entonces, no solamente contaban con todo el conocimiento y herramientas para operar exitosamente en ese país, sino que contaban además con la misión de un mercado ecuatoriano que hasta ese entonces no había sido explotado.

Se suscribe entonces un acuerdo de Asociación entre el Grupo Equinoccial y Suramericana, de forma que existía coparticipación en el proyecto, así como el compromiso para que el menor tiempo posible EQUIVIDA pudiera entrar en funcionamiento; para lo que era necesario un entrenamiento exhaustivo y un estudio detallado de las pólizas y las cláusulas que se empezarían a comercializar.

EQUIVIDA cuenta con el respaldo de los mejores reaseguradores del mundo, tales como Swiss Re, Hannover Life Re, Mapfre RE.

El primer presidente del Directorio fue el Eco. Roque Sevilla y el primer Gerente General fue el Sr. José Morillo; ambos nombrados en la sección extraordinaria del Directorio efectuado el 24 de Junio de 1994.

EQUIVIDA emite su primera póliza en el mes de septiembre de 1994, siendo este un hito histórico para la compañía, ya que a partir de esta fecha se inicia el crecimiento de la gestión.

3.4. DIRECCIONAMIENTO ESTRATÉGICO

a) Misión

Crear con el cliente soluciones innovadoras que le permitan visualizar y tangibilizar un futuro tranquilo ante los eventos trascendentales de su vida y la de su familia.

Condiciones necesarias para cumplimiento de la misión

- Ser una empresa sólida y rentable.
- Crear productos y servicios innovadores y de alta calidad.
- Contar con personal profesional y comprometido
- Mejorar continuamente los productos y servicios al cliente.

b) Visión

Ser siempre la primera elección de respaldo económico durante la vida de las personas, en los países donde actuamos.

c) Valores

- **Actuamos éticamente:** Somos honestos, íntegros, transparentes, responsables y buscamos el bien común.
- **Damos lo mejor de nosotros:** Entregamos nuestro mejor esfuerzo, siendo eficaces, trabajando en equipo y manteniendo siempre una actitud constructiva y positiva.
- **Buscamos la auto-superación:** Somos creativos y proactivos, buscamos mejorar permanentemente. Creemos en el valor de nuestro desarrollo personal y profesional.
- **Respetamos a las personas:** Buscamos un ambiente de cordialidad, comunicación oportuna, relaciones transparentes y sinceras al interior de la empresa, hacia nuestros clientes, socios, proveedores y comunidad.
- **Humildad:** Comprender que siempre podremos aprender y deberemos enseñar con responsabilidad y objetividad en cada puesto dentro de la organización. Humildad significa, entender que somos parte de un equipo y que nos debemos al mismo. Implica confianza en las decisiones organizacionales y aporte constructivo hacia decisiones de mejora y cambio permanente.
- **Compromiso con la sostenibilidad y cuidado del medio ambiente:** Es responsabilidad de todo colaborador EQUIVIDA y de la organización, el cuidar el entorno y provocar acciones individuales o grupales que promuevan el cuidado del medio ambiente y aportar con acciones sostenibles en cada ámbito de actuación, personal y profesional.

3.4.1. OBJETIVO ADMINISTRATIVO.

Al posicionarse como líder del sector de seguros de vida, el poder contribuir al fortalecimiento corporativo del Grupo Futuro convirtiéndose así en los primeros aseguradores del país; y en el futuro ser los primeros aseguradores internacionales.

3.4.2. OBJETIVO OPERACIONAL

Ser una empresa exitosa en el sector de seguros de vida, brindando productos y servicios de calidad para la satisfacción de los clientes y confianza de la sociedad en general.

3.4.3. OBJETIVO DE COMERCIALIZACIÓN

Para poder establecer sus objetivos de comercialización es de gran ayuda hacer énfasis en estos tres aspectos:

- Horizonte de Tiempo: su misión y visión están proyectados para 5 años.
- Ámbito de acción: está considerado como nacional, con prioridad en la ciudad de Quito ya que es donde se encuentra su matriz.
- Posicionamiento de Mercado: persigue el liderazgo sectorial.

Ser la primera asegura de vida en el mercado ecuatoriano ofreciendo productos y servicios confiables y de calidad a sus clientes, dentro de un periodo de 5 años plazo.

Este objetivo se justifica por la coherencia que mantiene con la visión y misión de la empresa y por las pretensiones que buscan los directivos que forman parte de la misma.

Crecer en los próximos 5 años el valor anual de las ventas a diferencia del año anterior.

Este objetivo se justifica porque la empresa tiene como política y aspiración ser reconocida, al menos en un 3% adicional de la participación en el mercado que mantiene el sector. Es decir que se busca tener un reconocimiento mayor reflejado en mejores niveles de participación del mercado y ventas

3.4.4. OBJETIVO DE MARKETING

Establecer estrategias publicitarias a través de propaganda en medios masivos de comunicación (televisión, radio e internet) y anuncios en revistas técnicas de circulación (gestión, vistazo, líderes) a nivel nacional.

EQUIVIDA S.A. ha mantenido la constante aspiración de alta competencia para lograr su propósito estratégico que es alcanzar el liderazgo en el mercado de seguros de vida en el país, por su servicio al cliente. Para lograr esta meta los directivos que conforman la compañía aspiran mantener sus buenas relaciones con instituciones financieras y sus respectivos asesores de seguros, que de cierta manera también buscan ser parte del mercado y a la vez expandir su imagen organizativa en la sociedad.

3.5. FILOSOFÍA DE LA EMPRESA

EQUIVIDA S.A. desarrolla sus actividades en base a las siguientes premisas.

Cultura de servicio: mantener el interés y compromiso por dar mejor servicio a sus clientes.

Innovación: ser creativos día a día en sus productos, estrategias, talento humano y tecnológico.

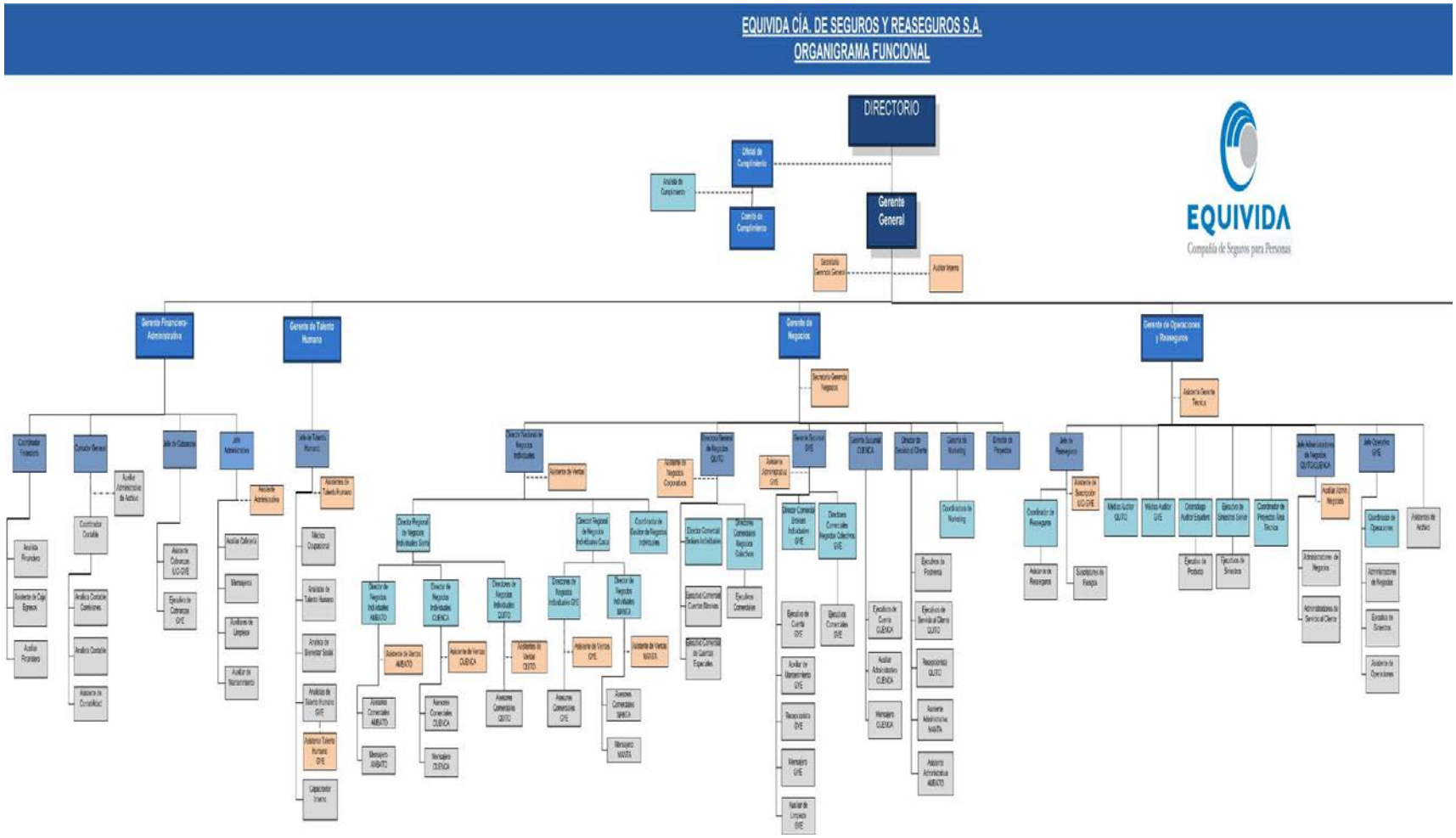
Éxito: persigue el crecimiento personal, profesional e institucional.

Líder: establecer calidad y variedad de sus productos en el mercado de seguros de vida.

Transparencia: ser claros y oportunos a la hora de informar sobre sus productos.

Crear con el cliente soluciones innovadoras que le permitan visualizar y tangibilizar un futuro tranquilo ante los eventos trascendentales de su vida y la de su familia.

3.6. ORGANIGRAMA



3.7. UNIDADES ORGANIZATIVAS DE EQUIVIDA

Gerencia General

Objetivo

Liderar el desarrollo y crecimiento sustentable y a largo plazo de la compañía, que garantice el cumplimiento de su visión, por medio de la determinación y consecución de los objetivos estratégicos, análisis profundo de desempeño del negocio y sus indicadores y del liderazgo y trabajo en equipo con sus colaboradores.

Gerencia Financiera - Administrativa

Objetivo

Planear, ejecutar y dirigir la gestión financiera administrativa de la empresa con el fin de optimizar el uso de los recursos para obtener los mejores resultados, los mismos que están alineados a los grandes objetivos institucionales

Gerencia Talento Humano

Objetivo

Orientar y brindar asesoría permanente a las líneas de supervisión, mediante herramientas técnicas y prácticas en gestión de personal, con el fin de obtener, mantener y retener personal calificado y comprometido con la

compañía, orientados a la consecución de resultados individuales y generales de manera permanente y positiva.

Gerencia de Negocios

Objetivo

Tener y / o mantener un equipo comercial exitoso a fin de lograr los resultados esperados en cuanto a presupuesto comercial y de calidad de cartera de clientes.

Gerencia de Operación y Reaseguros

Objetivo

Garantizar una eficaz planificación, elaboración y cumplimiento de políticas; y estandarización de procesos a nivel nacional, en relación a las áreas a cargo en función de los objetivos estratégicos de la compañía. Mantener directamente y a través del equipo excelentes relaciones con aliados estratégicos (bróker, proveedores, reaseguradores y demás prestadores).

Gerencia de Innovación y Desarrollo Tecnológico

Objetivo

Proveer visión tecnológica/procesos, liderazgo para desarrollar e implementar iniciativas de IT y adopción de mejores prácticas capaces de

crear y mantener a la empresa en una posición de liderazgo dentro de un mercado altamente competitivo y constantemente cambiante.

Gerencia Actuarial

Objetivo

Desarrollar y mantener modelos que propendan al cumplimiento del nivel de retorno objetivo de la corporación.

3.8. ANÁLISIS DEL NEGOCIO Y EVALUACIÓN DE RIESGOS

La empresa Equivida durante los últimos años ah realizado un esfuerzo enorme para levantar la información, documentar y diagramar los procesos que soportan a la compañía.

Los procesos levantados son divididos en Procesos Primarios, Procesos de Apoyo y Procesos de Gestión.

Para el desarrollo de este Plan el Comité Directivo ah solicitado poner énfasis en el análisis de los PROCESOS PRIMARIOS que son los que sustentan la cadena de valor y son aquellos enfocados en el cliente.

Diagrama de los Macro procesos de la compañía:

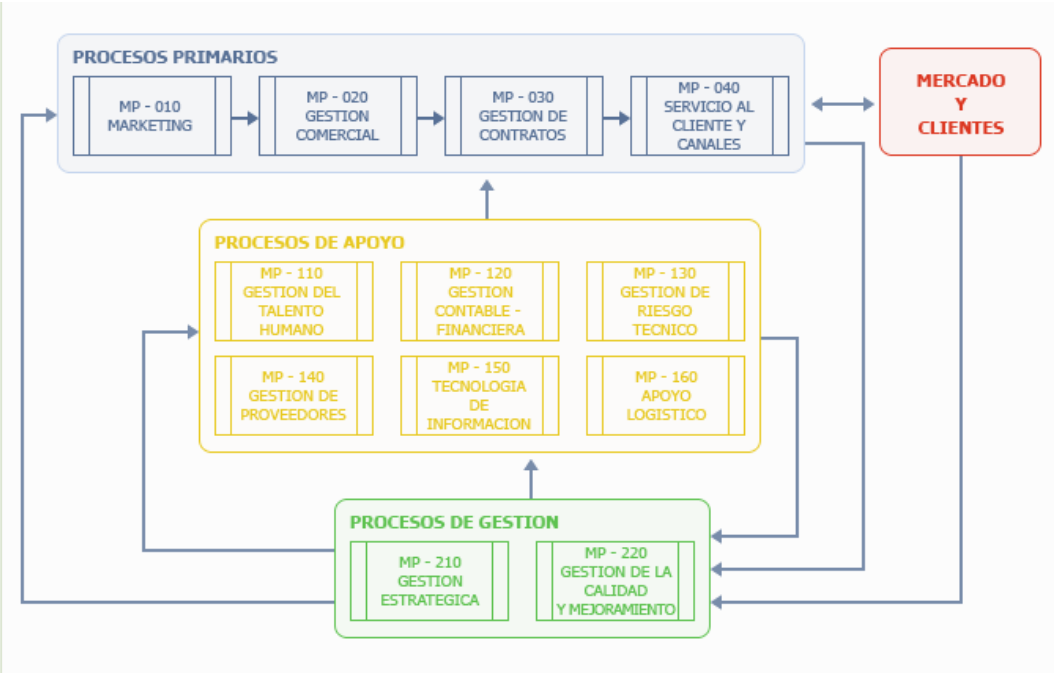


Ilustración 16 Macro procesos de Equivida

3.9. ANÁLISIS DE PROCESOS DE EQUIVIDA

Para la selección de los procesos considerados críticos de la compañía se realiza un acercamiento a través de la cadena de valor, definidos en el mapa como Procesos Primarios.

Los Macro procesos a considerar son:

MP 010 – Marketing

MP 020 – Gestión Comercial

MP 030 – Gestión de Contratos

MP 040 – Servicio al Cliente y Canales

De la presentación de los 4 Macroprocesos considerados anteriormente se realiza un análisis para definir los procesos prioritarios que soportan a estos Macroprocesos; para el desarrollo del Plan se define que los procesos críticos a tomar en consideración son los siguientes:

Tabla 1 Procesos prioritarios de Equivida

Macroproceso: Gestión Comercial
Proceso: (PR-021) Ventas Colectivo
Responsable: Inés San Lucas/Marco Avilés
Descripción: Generar negocios colectivos rentables con clientes y canales satisfechos, buscando una relación ganar-ganar a largo plazo

ACTIVIDADES/RESPONSABLE	NEGOCIOS/ G. SUCURSALES	DIRECTOR COMERCIAL
Entregar directrices, estrategias y plan de compensación e incentivos al equipo comercial	X	
Prospectar y realizar la introducción del producto en el canal y/o cliente		X
Desarrollar necesidades del cliente		X
Realizar y presentar propuesta		X
Realizar seguimiento, negociación y cierre		X
Elaborar orden de emisión		X
Revisar póliza emitida		X
Entregar pólizas a Adm.de contratos		X
Comunicación con el cliente o adm.de contratos		X
Entregar directrices, estrategias y plan de compensación e incentivos al equipo comercial		X

FUENTE: ANDRÉS CÁRDENAS
ELABORADO: ANDRÉS CÁRDENAS

Macroproceso: Gestión Comercial
Código: (PR-022) Incremento de negocio y fidelización de los clientes
Responsable: María Fernanda Álava
Descripción: Incrementar y fidelizar los negocios existentes en el segmento colectivo

ACTIVIDADES/RESPONSABLE	EJECUTIVO COMERCIAL/DIRECTOR COMERCIAL	JEFE DE REASEGURO	CONTRATANTE Y/O CANAL
Elaborar registro de ofertas no aceptadas	X		
Presentar el nuevo producto/cobertura al canal y/o cliente	X	X	
Desarrollar necesidades del cliente	X	X	
Receptar información del cliente a ser reasegurado	X	X	
Analizar información de cliente		X	
Presentar tasas y condiciones a aplicar		X	
Revisar el análisis de incrementos			X

FUENTE: ANDRÉS CÁRDENAS
ELABORADO: ANDRÉS CÁRDENAS

Macroproceso: Gestión Comercial
Código: (PR-023) Ventas Masivas
Responsable: Jenny Méndez/Stewart Aguilar
Descripción: Generar ventas masivas a través de un tercero (cliente/APS), en segmentos a los cuales no podemos acceder rentablemente de forma directa**.**

ACTIVIDADES/RESPONSABLE	EJECUTIVO COMERCIAL/DIRECTOR COMERCIAL
Seleccionar los prospectos potenciales	X
Obtener información básica del prospecto	X
Personalizar la presentación	X
Presentar oportunidad de negocio	X
Analizar información y elaborar propuesta	X
Levantar información del proceso de venta	x
Planificar implementación proyecto	X
Monitorear rentabilidad	X

FUENTE: ANDRÉS CÁRDENAS
ELABORADO: ANDRÉS CÁRDENAS

Macroproceso: Gestión de Comercial

Código: (PR-025) Gestión Posventa Individual – Mantenimiento

Descripción: Administrar y fidelizar los negocios existentes a mediano y largo plazo en Pólizas Vida individual

Responsable: Tania Estrella

ACTIVIDADES/RESPONSABLE	EJECUTIVO COMERCIAL/EJECUTIVO DE SERVICIO AL CLIENTE	DIRECTOR DE SERVICIO AL CLIENTE
Ejecutar plan de postventa	X	
Sacar reporte de pólizas huérfanas	X	
Hacer una actualización y/o corrección de datos de clientes en el sise	X	
Segmentar y analizar la cartera de clientes		X
Generar reporte del análisis de la atención y coberturas		X
Definir necesidades actuales del cliente		X
Analizar viabilidad de la idea		X
Hacer un informe semestral de los planes posventa		X
Analizar idea de fidelización		x

FUENTE: ANDRÉS CÁRDENAS
ELABORADO: ANDRÉS CÁRDENAS

Macroproceso: Gestión de Contratos

Código: (PR-031) Administración de operaciones contractuales colectivo

Descripción: Generar contratos de seguros colectivos de acuerdo con lo convenido con el cliente, cumpliendo estándares de tiempo y calidad.

Responsable: Yessenia Córdova

ACTIVIDADES/RESPONSABLE	JEFE DE OPERACIONES UIO	ADMINISTRADOR DE NEGOCIOS	DIRECTOR COMERCIAL
Revisar la orden de Emisión/Renovación y los documentos adjuntos	X		
Cargar parámetros faltantes	X		
Revisar y firmar la póliza	X		
Crear, modificar o verificar Contratantes/asegurados		X	
Emitir póliza y endoso		X	
Cargar condiciones particulares		X	
Imprimir pólizas		X	
Armar pólizas		X	
Distribuir pólizas		X	
Verificar requisitos de asegurabilidad manualmente		X	
Registrar información en archivo Excel		X	
Imprimir factura en sistema Sise		X	
Armar factura		X	
Reportar y verificar pólizas			X
Dar de baja póliza en el vector			x

FUENTE: ANDRÉS CÁRDENAS
ELABORADO: ANDRÉS CÁRDENA

Macroproceso: Gestión de Contratos

Código: (PR-032) Movimientos y facturación colectivo

Descripción: Registrar con calidad la información del cliente para cobro y prestación de beneficios

Responsable: Priscila Guevara

ACTIVIDADES/RESPONSABLE	ADMINISTRADOR DE NEGOCIOS	JEFE DE OPERACIONES UIO	DESPACHADOR
Verificar requisitos de asegurabilidad	X		
Registrar movimientos en Sise	X		
Generar ajuste en el sistema	X		
Imprimir ajuste en el sistema	X		
Imprimir factura	X		
Armar factura	X		
Verificar requisitos de asegurabilidad	X		
Generar factura en el sistema Sise	X		
Imprimir factura en el sistema Sise	X		
Armar factura	X		
Verificar calidad de factura	X		
Generar el control de facturación en el sistema Sise		X	
Modificar el control de facturación		X	
Distribuir a Administradores		x	
Imprimir y modificar según el cliente la carta del Sise			X

FUENTE: ANDRÉS CÁRDENAS
ELABORADO: ANDRÉS CÁRDENAS

Macroproceso: Gestión de Contratos

Código: (PR-034) Beneficios y prestaciones al cliente – siniestros

Descripción: Generar Tangibilizar la protección económica y entrega de prestaciones a los beneficiarios del seguro, a través de un servicio oportuno, eficiente e integral.

Responsable: Héctor Maldonado

ACTIVIDADES/RESPONSABLE	EJECUTIVO DE SINIESTROS	GERENTE TÉCNICA	MEDICO AUDITOR
Enviar carta al canal o cliente	X		
Abrir reserva y liquidar reclamo	X		
Generar orden de pago	X		
Ingresar al modulo contable para completar datos para transferencia	X		
Recibir por parte de contabilidad un correo con datos de transferencia realizada	X		
Entrega de documentos del siniestros para autorización y firmas de responsabilidad	X		
Enviar al cliente o canal el finiquito junto con correo de transferencia	X		
Entregar cheque con documentos del siniestros para autorización y firmas autorizadas	X		
Enviar cheque y finiquito correspondiente al canal o cliente	X		
Revisar carta de negativa y firmar		x	
Realizar auditoria medica			X
Solicitar a cliente o canal documentación faltante			x

FUENTE: ANDRÉS CÁRDENAS
ELABORADO: ANDRÉS CÁRDENAS

Macroproceso: Servicio al cliente y canales

Código: (PR-035) Administración de contratos individuales

Descripción: Generar contratos de seguros individuales y facturas, cumpliendo estándares de tiempo y calidad

Responsable: Natalia Moncayo/ Paulina Martínez

ACTIVIDADES/RESPONSABLE	COORDINADORA DE OPERACIONES/ADMINISTRADORA DE NEGOCIOS SENIOR	ADMINISTRADORES DE NEGOCIO	EJECUTIVO DE SERVICIO AL CLIENTE
Revisar solicitudes y documentación	X		
Distribuir solicitudes y requerimientos	X		
Aprobar emisión del cheque por cancelación	X		
Revisar y firmar el contrato	X		
Entregar documentos a archivo	X		
Entregar contratos	X		
Correr proceso de solicitud de renovaciones cada inicio de mes	X		
Imprimir cartas de renovación y estados de cuenta	X		
Generar solicitud de renovaciones manuales	X		
Procesar la cancelación en el sistema		X	
Imprimir endosos de cancelación		X	
Generar notas de crédito		X	
Solicitar cruce de endosos a cobranzas		X	
Solicitar la aprobación del cheque		X	X
Solicitar la emisión del cheque		X	x
Crear modificar o verificar contratantes y o asegurados		X	

Generar el contractual	X	
Imprimir a armar contrato	X	
Emitir contrato endoso y factura	X	
Cancelar la póliza vigente	X	
Entregar autorizaciones de debito	X	
Cancelar la póliza vigente	X	
Correr proceso de facturación automática de proteger plus	X	
Imprimir y repartir factura	X	
Generar reporte de solicitudes de renovación a pólizas	X	
Correr proceso de renovaciones	X	
Verificar solicitudes procesadas	X	
Generara factura manual e imprimir factura	X	
Verificar y actualizar datos		X
Generar reporte de direcciones y teléfonos de pólizas renovadas		X
Enviar cartas de renovación y estados de cuenta		X
Ordenar y archivar documentación		X
Aplicar pago		x

FUENTE: ANDRÉS CÁRDENAS
ELABORADO: ANDRÉS CÁRDENAS

Macroproceso: Servicio al cliente y canales

Código: (PR-041) Atención al cliente y canales vida individual

Descripción: Satisfacer oportuna y eficientemente las necesidades del cliente y canales brindando información clara y precisa, con buen trato y cortesía

Responsable: Tania Estrella

ACTIVIDADES/RESPONSABLE	RECEPCIONISTA	EJECUTIVO SERVICIO AL CLIENTE	ÁREA RESPONSABLE
Recepción del cliente	X		
Transferir requerimientos básicos	X		
Reproducir el Script de Atención telefónica		X	
Identificar la necesidad		X	
Confirmar/actualizar datos del cliente y registrar datos de req. En el mantis		X	
Cerrar la ocurrencia en el mantis		X	
Solicitar soporte de otra a área a través del mantis		X	
Hacer encuesta de satisfacción del cliente		X	
Informar la solución al cliente de acuerdo al tiempo establecido		X	
Elaborar informe mensual de atención de req. Y citas dentales		X	
Analizar req. Asignado mantis			X
Hacer análisis de causas			X
Definir plazo y registrar en mantis			x

FUENTE: ANDRÉS CÁRDENAS
ELABORADO: ANDRÉS CÁRDENAS

Macroproceso: Gestión Contable - Financiera

Código: (PR-123) Pagos

Descripción: Realizar pagos correctos y oportunos a proveedores, clientes y canales

Responsable: Sofia Tapia

ACTIVIDADES/RESPONSABLE	ASISTENTE DE CAJA EGRESOS/ASISTENTE CONTABLE DE COMISIONES/ASISTENTE CONTABLE DE NOMINA	ASISTENTE CAJA PAGOS/ASISTENTE CONTABLE DE COMISIONES/	COORDINADOR FINANCIERO
Ingresar factura al sise	X		
Generar autorización técnica	X		
Descontar anticipo en orden de pago	X		
Generar orden pago	X		
Generar orden de pago en sise		X	
Direccionar orden de pago		X	
Imprimir documentos de respaldo		X	
Custodiar documentos de pago		X	
Entregar pagos a proveedores		X	
Recibir documentos firmados por beneficiarios		X	
Revisar asignación correcta de cuenta			X
Revisar forma y % de retención correctamente aplicados			X
Validar cuentas contables y valores aplicados			X

FUENTE: ANDRÉS CÁRDENAS
ELABORADO: ANDRÉS CÁRDENAS

Concluido el análisis de los procesos que forman parte de los Macroprocesos de la compañía, se realiza una selección de los procesos críticos a considerar en el plan.

3.10. SELECCIÓN DE PROCESOS CRÍTICOS

Para la selección de los procesos críticos se solicita una valoración de impactos de los mismos con la siguiente escala:

Tabla 2 Valoración de impactos

Calificación	Criterio	Valor
Alto	El proceso es fundamental para el cumplimiento de los objetivos de la empresa	3
Medio	El proceso aporta de manera importante para el cumplimiento de los objetivos de la empresa	2
Bajo	El proceso aporta de una manera menor para el cumplimiento de los objetivos de la empresa	1
Nulo	No aporta para el cumplimiento de los objetivos de la empresa	0

FUENTE: ANDRÉS CÁRDENAS

ELABORADO: ANDRÉS CÁRDENAS

Tabla 1 Procesos Críticos de Equivida

MACROPROCESOS	CÓDIGO	PROCESO	IMPACTO EN LA EMPRESA	IMPACTO EN EL CLIENTE	TOTAL
Gestión Comercial	PR-021	Ventas Colectivo	3	1	4
Gestión Comercial	PR-022	Incremento de negocio y fidelización de los clientes	3	1	4
Gestión Comercial	PR-023	Ventas Masivas	3	1	4
Gestión Comercial	PR-024	Ventas Individuales - Fuerza de Ventas	3	1	4
Gestión de Contratos	PR-031	Administración de operaciones contractuales colectivo	3	3	6
Gestión de Contratos	PR-032	Movimientos y facturación colectivo	3	3	6
Gestión de contratos	PR-033	Recaudos	3	3	6
Gestión de Contratos	PR-034	Beneficios y prestaciones al cliente – siniestros	3	3	6
Gestión de Contratos	PR-035	Administración de contratos individuales	3	3	6
Servicio al cliente y canales	PR-041	Atención al cliente y canales vida individual	3	3	6
Gestión Contable - Financiera	PR-123	Pagos	3	3	6

FUENTE: ANDRÉS CÁRDENAS

ELABORADO: ANDRÉS CÁRDENAS

3.11. SISTEMAS QUE SOPORTAN LOS PROCESOS

A continuación se describen cada uno de los sistemas que soportan los procesos.

Tabla 2 Inventario de sistemas

Nombre del Sistema	Descripción	Critico	Tipo de Sistema	Responsable	Procesos
Data cleaning	Verificación de la validez de información básica del cliente	2	AIX 6.1 Power 6	Iván Noboa	PR-024 PR-035 PR-021
Cliente único	Plataforma para captura y mantenimiento de información consistente de clientes	2	AIX 6.1 Power 6	Kathy Flores	PR-024 PR-035 PR-021
GPC	Aplicación para la generación en línea de certificados de seguro.	2	Servidor: Microsoft Windows 2008 Server, IIS Cliente: Internet Explorer 7.0 o superior Internet Explorer 7.0 o superior	Javier Chicaiza	PR-021 PR-023 PR-031
BUEN VIAJE	Aplicación para la venta en línea de seguros de viaje.	2	Servidor: Microsoft Windows 2008 Server, IIS	Javier Chicaiza	PR-024

			Cliente: Internet Explorer 7.0 o superior Internet Explorer 7.0 o superior		PR-035 PR-021
BIORED	Aplicación para servicios dentales.	3	Servidor: Microsoft Windows 2008 Server, IIS Cliente: Internet Explorer 7.0 o superior Internet Explorer 7.0 o superior	Javier Chicaiza	PR-021 PR-022
VECTOR	Sistema de modelamiento, control y seguimiento de procesos.	1	Servidor: Microsoft Windows 2003 Server, IIS Cliente: Internet Explorer 7.0 o superior Internet Explorer 7.0 o superior	Javier Chicaiza	PR-021 PR-023 PR-024 PR-032 PR-035
INTRANET	Portal de comunicación interna	3	Servidor: Microsoft Windows 2003 Server, IIS Cliente: Internet Explorer 7.0 o superior Internet Explorer 7.0 o superior	Javier Chicaiza	PR-041
MANTIS	Sistema para seguimiento de tickets de servicio al cliente.	2	Apache	Javier Chicaiza	PR-041
ADAM	Sistema que administra la nómina de la compañía.	1	Servidor: Microsoft Windows 2003 Server, IIS	Javier Chicaiza	PR-123
BUXIS	Sistema de Talento Humano que administra la gestión organizativa, el desarrollo y capacitación del personal.	3	Microsoft	Andrés Cárdenas	N/A
MONITOR PLUS ACRM	Sistema para la prevención de lavado de activos basado en la administración de riesgos	3	Microsoft	Andrés Cárdenas	N/A

RISK CONTROL SERVICE	herramienta de control que tiene como objetivo minimizar el riesgo de establecer vínculos con posibles involucrados o señalados en actividades ilícitas como lavado de activos, narcotráfico o terrorismo,	2	Microsoft	Andrés Cárdenas	PR-035
SISE	Sistema Integrado de Seguros. Este sistema soporta el core del negocio y la parte administrativa financiera, tiene módulos de: Emisión/Facturación Individual y Colectivo, Reaseguros, Siniestros, Generación Intereses, Retiros y Préstamos, Caja Ingresos, Caja Egresos, Contabilidad, Cierres Mensuales, Consultas, Informática.	1	Servidor: AIX 6.1, Servidor Power 6. Cliente: Windows XP o 7.	Javier Chicaiza	PR-031 PR-032 PR-033 PR-034 PR-035 PR-041 PR-123
iSISE	Aplicación para la venta en línea de certificados de seguro.	3	Winserver para servidores de BD y App. El cliente solo necesita Internet Explorer de cualquier versión.	Isvel López \ Javier Chicaiza	PR-021 PR-023
BAIS	Aplicación para la venta en línea de certificados de seguro.	3	Servidor: Windows Server 2008, IIS 7. Cliente: Windows XP o 7.	Isvel López	PR-021
CRM	Sistema automatizado para el control de la fuerza de ventas individual	2	Linux, Apache	Andrea Bandera	PR-041
PORTAL WEB	Portal diseñado para la prestación de servicios online	2	Expression Engine	Andrea Bandera	PR-041

ACTIVOS FIJOS	Sistema automatizado para el control de los activos fijos de la compañía	3	Microsoft	Andrea Bandera	N/A
PIVOTAL	CRM para gestión de clientes	3	Microsoft	Andrea Bandera	PR-041 PR-021

FUENTE: ANDRÉS CÁRDENAS

ELABORADO: ANDRÉS CÁRDENAS

3.12. COMPONENTES TECNOLÓGICOS QUE SOPORTAN LOS PROCESOS

A continuación se describen cada uno de los componentes que soportan los procesos.

Tabla 3 Inventario Recursos Tecnológicos

TIPO DE COMPONENTE	DETALLE	MARCA	PR-031	PR-032	PR-033	PR-034	PR-035	PR-041	PR-123	CRITICO
MAQUINAS VIRTUALES	Active Directory Primario	VMware	x	x	x	x	x	x	x	☑
MAQUINAS VIRTUALES	Active Directory secundario	VMware								
MAQUINAS VIRTUALES	Antivirus Symantec Quito	VMware								
MAQUINAS VIRTUALES	Citrix (Virtualizador de escritorios)	VMware								

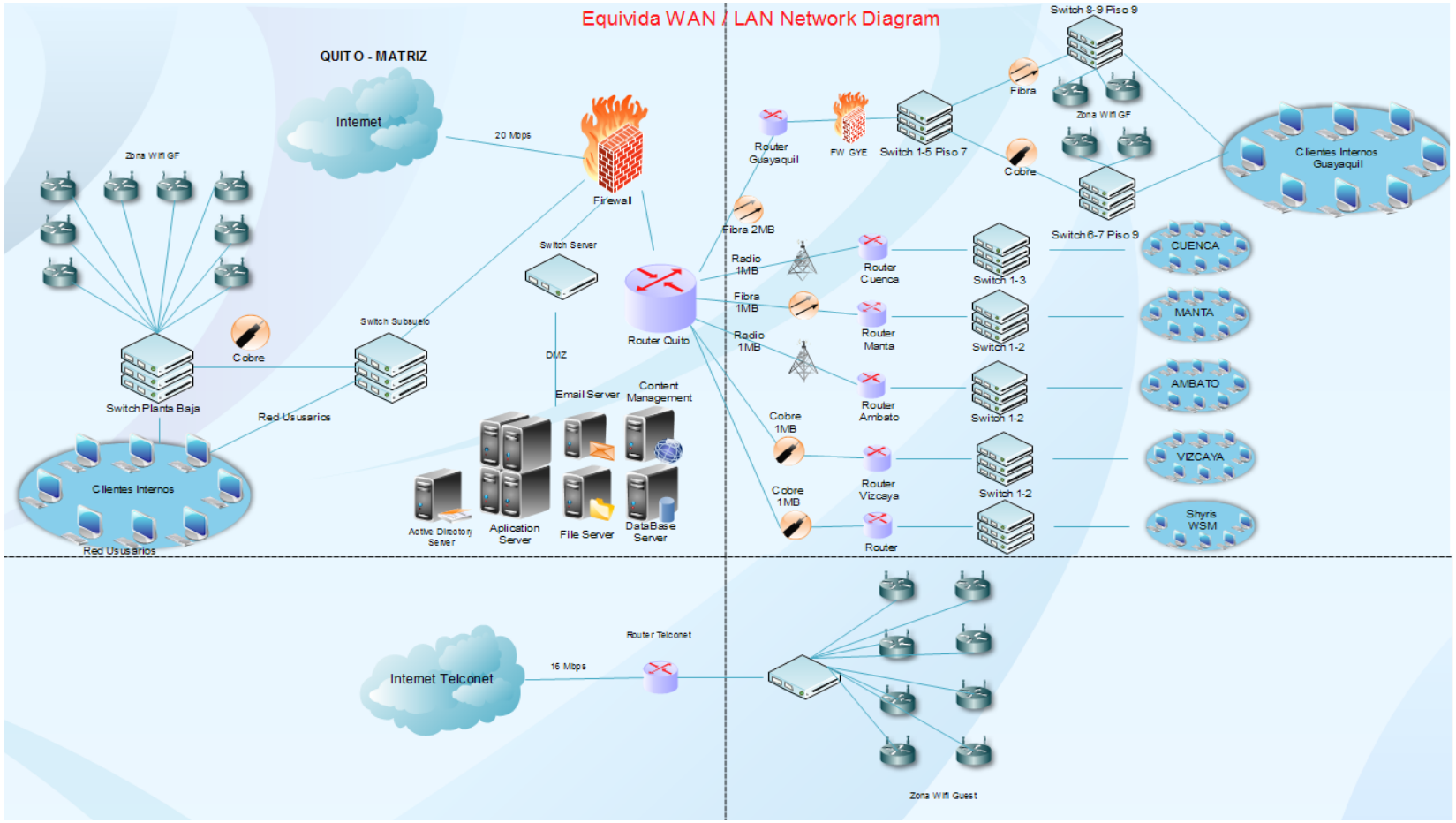
MAQUINAS VIRTUALES	Sistema Vector	VMware	x	x			x	x		☑
MAQUINAS VIRTUALES	Vcenter (administrador MV)	VMware	x	x	x	x	x	x	x	☑
MAQUINAS VIRTUALES	Sistema Loncherito (Control de almuerzos)	VMware								
MAQUINAS VIRTUALES	Sistema Belarc (Inventario de equipos)	VMware								
MAQUINAS VIRTUALES	Sistema Mantis (tickets de quejas)	VMware						x		☑
MAQUINAS VIRTUALES	Correo Electrónico	IBM	x	x	x	x	x	x	x	☑
MAQUINAS VIRTUALES	Proxy Quito	IBM								
MAQUINAS VIRTUALES	Sistema de Cumplimiento	IBM					x			☑
ENLACES	Enlaces	Internet	x	x	x	x	x	x	x	☑
Router	Router	Cisco	x	x	x	x	x	x	x	☑
ENLACES	Transciever Enlace	Cisco	x	x	x	x	x	x	x	☑
ENLACES	Transciever E1	Cisco	x	x	x	x	x	x	x	☑
COMUNICACIÓN	Videoconferencia	Polycom								
INFRAESTRUCTURA	Respaldos	IBM								
INFRAESTRUCTURA	Sistema Adam (Nomina Equivida)	IBM							x	☑
INFRAESTRUCTURA	Página Web Global	IBM				x		x		☑
INFRAESTRUCTURA	ERP (Producción SISE)	IBM	x	x	x	x	x	x	x	☑
INFRAESTRUCTURA	ERP (Desarrollo SISE)	IBM								
INFRAESTRUCTURA	Bus de Servicios (Sonic)	IBM	x	x				x		☑

INFRAESTRUCTURA	Sistema Data Quality	IBM								
INFRAESTRUCTURA	Sistema Biored Ventas Seguro Dental	HP	x	x				x		☑
RESPALDO	Storage DS5020	IBM								
RESPALDO	Tape Library TS3100	IBM								
SWITCH	Servidores Subsuelo	3Com	x	x	x	x	x	x	x	☑
SWITCH	LAN 1 Sub Subsuelo	3Com	x	x	x	x	x	x	x	☑
SWITCH	Core 1 Sub Subsuelo	3Com	x	x	x	x	x	x	x	☑
SWITCH	LAN 2 Sub Subsuelo	3Com	x	x	x	x	x	x	x	☑
SWITCH	LAN 1 Pb Planta Baja	3Com	x	x	x	x	x	x	x	☑
SWITCH	LAN 2 Pb Planta Baja	3Com	x	x	x	x	x	x	x	☑
SWITCH	LAN 3 Pb Planta Baja	3Com	x	x	x	x	x	x	x	☑
SWITCH	LAN 4 Pb Planta Baja	3Com	x	x	x	x	x	x	x	☑
SWITCH	LAN 5 Pb Planta Baja	3Com	x	x	x	x	x	x	x	☑
SWITCH	LAN 6 Pb Planta Baja	3Com	x	x	x	x	x	x	x	☑
INFRAESTRUCTURA	Acess Point	3Com	x	x	x	x	x	x	x	☑
INFRAESTRUCTURA	Firewall Quito	IBM								
CENTRAL TELEFÓNICA	Central Telef. Quito	Telesynergy			x	x		x	x	☑

FUENTE: ANDRÉS CÁRDENAS

ELABORADO: ANDRÉS CÁRDENAS

Ilustración 17 Diagrama de red de Equivida



3.13. TIEMPO MÁXIMO DE RECUPERACIÓN DE LOS PROCESOS

Necesidad de recuperación:

- Día 0: Recuperación inmediata
- Día 1-5: El proceso debe ser recuperado entre el primer día y el quinto día después de un incidente.
- Día 6-13: El proceso debe ser recuperado entre el sexto día y antes del treceavo día
- Más de 13: El proceso puede ser recuperado después de 13 días ocurrido el incidente

Tabla 4 Tiempo máximo de interrupción de los procesos

CÓDIGO	PROCESO	Necesidades de Recuperación	Criticidad	Observaciones
PR-021	Ventas Colectivo	9-13 días	1	El envío de ofertas de negocio colectivos en caso de crisis se puede enviar después de 7 días hábiles permitiendo generar la documentación en base a licitaciones anteriores sin necesidad del sistema
PR-022	Incremento de negocio y fidelización de los clientes	7-10 días	2	El objetivo de fidelizar los negocios colectivo nos obliga a cumplir ciertos aspectos de generación de contratos a tiempo, con lo cual se necesita la facturación acordada con el cliente
PR-023	Ventas Masivas	7-10 días	2	La generación de ventas a través de terceros se puede realizar por cotizadores con los que cuentan los bróker, independizando del sistema core del negocio.
PR-024	Ventas Individuales - Fuerza de Ventas	7-10 días	2	Al ser una venta individual es más factible la generación de proformas por medio del cotizador y mientras se restablece los sistemas, es proceso de venta debe pasar por unos pasos previos antes de la generación de la póliza
PR-025	Gestión Posventa Individual - Mantenimiento	12 días	2	La fidelización de los negocios individuales en caso de crisis se puede mantener al margen hasta entrar en operaciones normales
PR-031	Administración de operaciones contractuales colectivo	4-5 días	3	Se debe mantener los acuerdos de convenio con el cliente de tiempo y calidad en la facturación de las pólizas.
PR-032	Movimientos y facturación colectivo	4-5 días	3	Los sistemas que permiten la administración de recaudos deben estar habilitados lo más pronto posible porque rigen los convenios de tiempo con entidades bancarias
PR-033	Recaudos	4-5 días	3	Los cobros automáticos tienen que ser enviados en fechas ya establecidas por las entidades financieras, caso contrario había

				retrasos ocasionando pérdidas económicas y malestar en los clientes.
PR-034	Beneficios y prestaciones al cliente - siniestros	3 días	3	Como entidad regida por la SBS se tiene que cumplir con tiempos de entrega de prestaciones a beneficiarios en caso de siniestros.
PR-035	Administración de contratos individuales	4-5 días	3	Los seguros individuales y facturación deben de cumplir con estándares de tiempo y calidad
PR-041	Atención al cliente y canales vida individual	3 días	3	La atención al cliente asegurado ante todo debe ser oportuna y precisa por lo cual es indispensable contar con la herramientas que permitan esta gestión
PR-123	Pagos	3 días	3	Se mantiene acuerdos de servicio de pagos, por lo cual incumplirlos puede ocasionar demandas legales.

FUENTE: ANDRÉS CÁRDENAS

ELABORADO: ANDRÉS CÁRDENAS

3.14. ANÁLISIS DE RIESGOS

El propósito del Análisis de Riesgo es el de conocer los riesgos implicados para las instalaciones de EQUIVIDA y el potencial tiempo de caída de las funciones del negocio.

El análisis de estos peligros es muy importante en el desarrollo de un plan de Continuidad del Negocio, el cual es necesario para la recuperación después de una situación de desastre.

Los recursos, personal y tiempos necesarios pueden ser identificados después de que el impacto ha sido analizado. Los puntos claves del análisis son:

Entender la vulnerabilidad de que ocurra un desastre y establecer medidas preventivas para tratar de eliminar o minimizar la ocurrencia del desastre.

Proveer una localidad segura, no sujeta a los mimos peligros que las instalaciones de computación principales, para respaldar el activo en caso de alguna contingencia.

Considerando lo anterior, en primer lugar, debemos analizar el entorno o contesto donde opera el negocio a fin de identificar las amenazas potenciales que podrían causar interrupciones prolongadas en las operaciones.

Es así que se consideran las siguientes categorías de amenazas:

AMENAZAS RELACIONADAS A LA CONTINUIDAD DEL NEGOCIO

Tabla 5 Catálogo de amenazas

TIPO	AMENAZAS	POSIBLES
NATURALES	Inundaciones	x
	Incendios	x
	Terremotos	x
	Deslizamiento de tierra	x

	Fuego fortuito	x
POR EL HOMBRE	Incumplimiento legales	x
	Accesos no autorizados al edificio	x
	Robo de equipos	x
	Robo de datos / documentos	x
	Huelgas/manifestaciones	
	Bloqueos de vías prolongadas	x
	Ataques cibernéticos	x
TECNOLÓGICOS	Virus	x
	Denegación de servicio	x
	Accesos no autorizados	x
	Falla en los servicios de comunicación	x
	Explosión	x
	Incendio	x
	Pérdida de confidencialidad	x
	Fallo de suministro eléctrico	x
	Errores en los sistemas firewall	x

FUENTE: ANDRÉS CÁRDENAS

ELABORADO: ANDRÉS CÁRDENAS

Evaluación de la Probabilidad de Ocurrencia de la Amenaza

(Histórico vs. percepción de ocurrencia)

El objetivo de esta fase es valorar cada una de las amenazas a fin de estimar una Probabilidad de Ocurrencia, tomando como base información histórica del evento, el entorno o contexto y, la situación y condición de la instalación o sede en evaluación así como también el juicio del experto que conocen de manera específica la situación y condición de cada instalación, conocen el medio donde se desarrollan, conocen las condiciones externas que podría afectarles, viven el día a día del entorno donde se desarrollan y por lo

tanto tienen la percepción de las variables que presentan las amenazas cuando se materializan.

Tabla 6 Nivel de probabilidad de ocurrencia de la amenaza

AMENAZAS	Histórico / Ocurrencia Φ	Juicio Experto / Percepción Я	Nivel de Probabilidad de ocurrencia (p)
Inundaciones	Baja	Baja	(Φ) *(Я)
Incendios	Medio	Alto	(Φ) *(Я)
Terremotos	Nulo	Nulo	(Φ) *(Я)
Deslizamiento de tierra	Nulo	Nulo	(Φ) *(Я)
Fuego fortuito	Baja	Baja	(Φ) *(Я)
Accesos no autorizados al edificio	Media	Baja	(Φ) *(Я)
Robo de equipos	Alta	Media	(Φ) *(Я)
Robo de datos / documentos	Alta	Media	(Φ) *(Я)
Huelgas/manifestaciones	Baja	Media	(Φ) *(Я)
Bloqueos de vías prolongadas	Baja	Baja	(Φ) *(Я)
Ataques cibernéticos	Baja	Media	(Φ) *(Я)
Virus	Media	Media	(Φ) *(Я)
Denegación de servicio	Baja	Media	(Φ) *(Я)
Accesos no autorizados	Media	Media	(Φ) *(Я)
Falla en los servicios de comunicación	Alta	Media	(Φ) *(Я)
Explosión	Nulo	Baja	(Φ) *(Я)
Pérdida de confidencialidad	Media	Media	(Φ) *(Я)
Fallo de suministro eléctrico	Alta	Media	(Φ) *(Я)
Errores en los sistemas firewall	Media	Media	(Φ) *(Я)

FUENTE: ANDRÉS CÁRDENAS

ELABORADO: ANDRÉS CÁRDENAS

Nivel de Probabilidad de ocurrencia (p)	Interpretación
(Φ) *(Я)	Impensable no se cree que ocurra (Desestimar)
(Φ) *(Я)	Improbable, con probabilidad de ocurrencia muy baja

	(Desestimar)
(Φ) *(Я)	Posible, con probabilidad de ocurrencia intermedia (Sin prioridad)
(Φ) *(Я)	Probable, con probabilidad de ocurrencia alta (Prioridad)
(Φ) *(Я)	Casi seguro, con probabilidad de ocurrencia extrema (Urgente)

Las amenazas identificadas en esta fase nos sirven para considerarlos como los peores escenarios de desastre a ser considerados en el Plan de Continuidad del Negocio para el análisis de vulnerabilidades.

ANÁLISIS DE VULNERABILIDADES

En función de las Amenazas que hemos marcado como posibles, establecemos los escenarios en que una amenaza puede convertirse en un incidente de seguridad.

Tabla 7 Análisis de vulnerabilidades

ESCENARIOS	VULNERABILIDAD
Fuego inesperado por cortocircuito de cables encima del cielo raso	Material inflamable en todas las áreas de la compañía
Ingreso de personas extrañas al edificio y robo de equipos	No se cuenta con controles de acceso al edificio
Extracción de información confidencial a través de dispositivos portables	No existe políticas de desactivación de los puertos de los dispositivos
Código mal intencionado instalado en los exploradores Web para robo de credenciales	Ausencia de programas para detección de keylogger
Accesos a sistemas de información de clientes por personas inescrupulosas	Información de clientes en bases de datos no ofuscada
Indisponibilidad del internet por un fallo del proveedor.	No se cuenta con un proveedor secundario de internet
Informe de Roles de pagos en carpetas compartidas para toda la empresa	Carpetas compartidas a nivel de toda la empresa sin controles de autentificación
Interrupción de la energía eléctrica por más	No se cuenta con una planta eléctrica

de 5 horas	de alta capacidad
Mala configuración de los firewalls expuestos a internet.	Falta de expertos en seguridades de apliance.

FUENTE: ANDRÉS CÁRDENAS

ELABORADO: ANDRÉS CÁRDENAS

EVALUACIÓN DEL RIESGOS

Para las amenazas antes expuestas se calcula el riesgo.

Tabla 8 Evaluación de riesgos

DESCRIPCIÓN	PROBABILIDAD	IMPACTO	RIESGO
Incendio	Media	Alto	ALTO
Robo de equipos	Alta	Media	ALTO
Robo de datos / documentos	Alta	Media	ALTO
Virus	Media	Media	MEDIO
Accesos no autorizados	Media	Media	MEDIO
Falla en los servicios de comunicación	Alta	Media	ALTO
Pérdida de confidencialidad	Media	Media	MEDIO
Fallo de suministro eléctrico	Alta	Media	ALTO
Errores en los sistemas firewall	Media	Media	MEDIO

FUENTE: ANDRÉS CÁRDENAS

ELABORADO: ANDRÉS CÁRDENAS

RECOMENDACIONES – CONTRAMEDIDAS

Para gestionar los riesgos detectados y mitigarlos en la medida de lo posible, se propone la puesta en marcha de las siguientes contramedidas:

Tabla 9 Contramedidas de amenazas

DESCRIPCIÓN	CONTRAMEDIDAS
Incendio	Contar con un sistema de detección de humo Tener en cada área en un lugar visible extintores Mantener los materiales inflamables bajo supervisión.
Robo de equipos	Control de accesos de personas ajenas a la compañía a las oficinas internas. Cámaras de vigilancia Bloqueos y borrado de información remota Contratar una póliza de seguros contra robos de componentes tecnológicos.
Robo de datos / documentos	Encriptación y ofuscación de la información sensible de los repositorios Políticas de acceso y extracción de información por dispositivos digitales Políticas de respaldo para la información más crítica para la compañía. Contratar una empresa especializada en la administración y custodia de documentos físicos (ej. pólizas)
Virus	Gestión de los logs que arroja el antivirus. Quitar permisos de administradores en las pc´s Monitorear los sistemas que no pertenecen a la compañía
Accesos no autorizados	Establecer un control de acceso físico al lugar donde se encuentran los equipos con información clave para la compañía.
Falla en los servicios de comunicación	Contar con un proveedor alterno en casos de emergencia. Definir SLA´s ajustados a la realidad del negocio
Pérdida de confidencialidad	Establecer políticas y niveles de confidencialidad de los documentos.
Fallo de suministro eléctrico	Adquirir un sistema de energía ininterrumpida UPS más robusto. Contar con un sistema de protección de variación de voltaje (picos y caídas de tensión)
Errores en los sistemas firewall	Definir políticas de seguridad correspondientes a cada red Contar con diseño para la configuración de cada firewall Capacitar al personal técnico con las marcas específicas con las que se cuenta en la empresa.

FUENTE: ANDRÉS CÁRDENAS

ELABORADO: ANDRÉS CÁRDENAS

CAPÍTULO 4

4. ESTRATEGIA DE RECUPERACIÓN Y CONTINUIDAD

Una vez que se ha realizado la gestión de los riesgos detectados, se debe seleccionar una estrategia de recuperación de negocio que asegure la continuidad de los procesos que hemos considerado críticos en el Análisis de Impacto (Kosutic, 2012).

4.1. CONSIDERACIÓN PARA LA ESTRATEGIA DE RECUPERACIÓN

- Considerar un sitio alternativo para administrar la recuperación, tal que no sea afectado por el mismo desastre.
- Considerar que debe haber facilidades para que las personas claves que forma el equipo de recuperación, puedan llegar al sitio alternativo.
- Reducir los costos, re-localizando el sitio alternativo a uno menos costoso una vez que se tenga el control de la interrupción.
- Asegurar que las facilidades de recuperación de TI sean adecuadas, que tengan controles, protección, seguridad.
- Asegurar que los proveedores que proporcionan las facilidades de recuperación sean lo suficientemente confiables.
- Utilizar sistemas de reemplazo en las áreas donde sea posible.

4.2. CENTRO DE REUNIÓN ALTERNATIVO EN CASO DE DESASTRE

De acuerdo al tipo de desastre se tienen las siguientes prioridades de puntos de encuentro:

Si el sitio del desastre es accesible, reunirse en:

- Matriz Sala de reuniones Planta Baja

- Matriz Sala de reuniones Primer piso

Si el sitio es inaccesible, reunirse en:

- Oficinas Ed. Viscaya (Sucursal Equivida Quito)

4.3. ACUERDOS CON PROVEEDORES

El departamento de TI de Equivida ya tiene implementados acuerdos con proveedores (Telconet) para que proporcionen los recursos necesarios en caso de desastre con sus tiempos pre-acordados

Requerimientos Tecnológicos

El departamento de TI de Equivida ya tiene un plan de respaldos con el proveedor (Locker´s) el cuál envía los backups fuera de la matriz una vez por semana, y cuenta con back up diarios en un servidor externo a la Matriz.

Para la selección de estrategias se plantea varios escenarios con las amenazas consideradas más probables.

4.4. SELECCIÓN DE ESCENARIOS

Escenario 1:

Contingencia: Ocurrió un incendio en la matriz Equivida en la Planta Baja en el área de administración junto al área de Sistemas.

Amenaza materializada: Al empezar el incendio este no pudo ser controlado debido a la cantidad de material inflamable en el área de administración a pesar

de contar con 2 extintores por área, el fuego no pudo ser controlado, se produce la perdida de documentos físicos (pólizas) y el fuego avanzo al cielo raso con el cual se propaga llegando a destruir el cableado de red que comunica los datos desde los servidores a todas las estaciones de trabajo.

Inconvenientes detectados:

Al quemarse una cantidad considerable de papel y cielo raso en la Planta baja inhabilita por el humo el trabajo también en el piso superior de la compañía.

El 70% de comunicaciones en la compañía esta inhabilitada, hay estaciones de trabajo que tienen acceso a voz y datos pero no pueden ser identificadas en su totalidad.

Se pierden enlaces de voz con lo cual las estaciones del Servicio al cliente no pueden dar servicio.

Estrategias de continuidad:

Solicitar que se habilite los canales de comunicación entre el Ed. Viscaya al centro de respaldo contratado a Telconet.

Conectarse a los servidores de respaldo de Telconet desde el Ed. Viscaya

Empezar con la restauración de los últimos respaldos en los servidores contratados en caso de emergencia.

Levantar los sistemas prioritarios.

Conectarse por maquina remota a la central telefónica para direccionar las llamadas a las líneas del Ed. Viscaya.

El equipo de las unidades organizativas solicitar a las personas claves las pruebas de los sistemas.

Escenario 2:

Contingencia: En las remodelaciones de las oficinas ingreso un grupo de personas del proveedor de cielo raso para arreglar el techo y al otro día desaparecieron varias laptops del área Comercial.

Amenaza materializada:

Las oficinas de Equivida al tener un crecimiento de personal requieren de remodelaciones constantes en su infraestructura, con lo cual las áreas no cuentan divisiones de paneleria unas de otras, con lo cual el acceso a cualquier área es fácil

En el área comercial todo el personal trabaja con laptops los cuales no tienen ningún tipo de seguridad para evitar ser extraídas.

Inconvenientes detectados:

- El área comercial no tiene puertas para controlar el acceso
- Las laptops no tenían candados para atarla al escritorio
- El personal no fue consciente de la vulnerabilidad de robo de sus equipos.
- No se solicito una póliza de protección al proveedor del cielo raso.
- No se cuenta con cámaras de seguridad en el área.

Estrategias de continuidad:

- Aplicar la póliza que se mantiene con Tecniseguros para la reposición económica del robo.
- Solicitud al proveedor Binaria de la adquisición de laptops y aplicar el acuerdo de entrega de equipos portables en menos de 3 días.
- Entregar a las personas con actividades críticas las 4 laptops de respaldo que se tiene en Sistemas y permitir el acceso a los sistemas críticos a través de Escritorios Compartidos.
- Equipo de gestión de servicio técnico replicar los Sistemas Operativos y aplicaciones a todas las laptops.
- Levantar los respaldos automáticos de información que se tiene en el Storage a las laptops.

Escenario 3:

Contingencia: Por la mala planificación de suministro de energía Equivida se queda sin luz durante 3 días y la planta eléctrica propia solo soporta 5 horas cuando está a tope el combustible, pero como no existía mantenimiento está menos de la mitad de su capacidad.

Amenaza materializada: La empresa se quedará sin energía eléctrica por 3 días, con lo cual no podrá entregar ningún servicio.

Inconvenientes detectados:

- No hubo un análisis de consumo de energía durante el crecimiento de la empresa.
- No existen planes de mantenimiento a la planta eléctrica
- Se cuenta con una planta eléctrica que soportaba a la mitad de componentes con los cuales ahora cuenta la empresa.
- No se mantuvo comunicación con la EEQ para notificar la carga eléctrica nueva que necesitaba la compañía.

Estrategias de continuidad:

- Solicitar a servicios generales obtener combustible para los próximos días.
- Apagar todos los componentes hardware que no sean considerados para el soporte de los procesos críticos.
- Enviar a grupos de trabajo a la sucursal para apoyar la gestión de procesos no críticos.

- Habilitar los accesos remotos para la conexión de los empleados desde sus hogares, las personas que trabajaran físicamente en las empresas serán únicamente las necesarias para el servicio al cliente.
- Una vez que se ha seleccionado la estrategia de continuidad, se puede comenzar a construir el Plan de Continuidad definiendo la estructura y composición de los equipos y las acciones de cada uno de ellos.
- Dado que Equivida cuenta con personas específicas para las operaciones consideradas críticas, el número de equipos y su composición no será tan grande.

4.4.1 COMITÉ DE CRISIS

Gerente de Crisis	Nombre: Marta Tufiño Posición: Gerente General Teléfono: 0987968741 Correo: matufino@gmail.com
Miembros del Comité	María Isabel Quiroz Posición: Gerente de TI Teléfono: 0998120487 Correo: miquiroz20@hotmail.com Marco Vaca Posición: Project Manager Teléfono: 0922125482 Correo: marco.vacaec@hotmail.com Ximena Benavides Posición: Gerente Operaciones Teléfono: 0873759480 Correo: ximentbena@yahoo.com

Lugar de reunión: Oficinas Ed. Viscaya Sucursal Equivida-Quito

Una vez que se comunica un incidente, el Comité de Crisis debe reunirse y tomar decisiones para afrontar la situación. Deben estar continuamente informados de la situación y determinar si es necesario iniciar el Plan de Continuidad. En este caso, se comunicará a los responsables de los equipos del comienzo de las actividades que llevarán a restablecer los servicios en la Sucursal Viscaya.

4.4.2 EQUIPO DE RECUPERACIÓN

El equipo de recuperación es el encargado de poner en marcha todo el proceso de recuperación para restaurar los servicios en las Oficinas del a Sucursal Viscaya.

Para ello realizarán las siguientes actividades:

- Se trasladarán hasta las oficinas de la sucursal.
- Pondrán en marcha por orden de criticidad los sistemas: ERP Sise, Adam, Servidor correo, etc.
- Para la puesta en marcha de los sistemas, se tomará la última copia de seguridad de los sistemas que semanalmente se manda a Locker’s.

- En primera instancia se reutilizarán los equipos de las oficinas de Viscaya. Se contactará con la persona responsable de logística para que solicite a los proveedores todos los equipos necesarios en los plazos acordados (durante el desarrollo del plan), sirvan todo el material necesario (servidores, PC’s, impresoras, etc.)

  Una vez que se vayan restaurando los servicios, debe comprobarse su operatividad.

4.4.2 EQUIPO DE RECUPERACIÓN

Responsable del Equipo	**Nombre: Juan Pablo Eguiguren** **Posición: Director de TI** **Teléfono: 0847896403** **Correo: *jpeguiguren@gmail.com***
Miembros del Equipo	Javier Chicaiza Posición: Jefe de Aplicaciones Teléfono: 0976598302 Correo: javier3847ch@hotmail.com Andrés Cárdenas Posición: Analista de sistemas Teléfono: 098883693 Correo: andrescaleo@gmail.com Gustavo Ortiz Posición: Coordinador de Infraestructura Teléfono: 0855376442 Correo: xlgustavo@yahoo.com Paulina Oviedo Posición: Jefe de servicios Teléfono: 0878447985 Correo: pauli.oviedo32@yahoo.com Paulina Valenzuela Posición: Gestor de servicios Teléfono: 0944876490 Correo: pauvalen09@gmail.com

4.4.3 EQUIPO DE COORDINACIÓN LOGÍSTICA

Es responsable de todo lo relacionado con las necesidades logísticas. En función del tipo de incidente se encargará de:

Atender las necesidades logísticas de primera instancia tras la contingencia. (Transporte de personas, transporte de materiales, etc.)

Contactar con los proveedores para solicitar el material necesario que indiquen los responsables de la recuperación.

Gestionar el suministro de comida al personal involucrado.

Responsable del Equipo	**Nombre: Ana Echeverría** **Posición: Jefe Administrativa** **Teléfono: 0899568301** **Correo: *anitaeche@gmail.com***
Miembros del Equipo	Nombre: Ana Hinojosa Posición: Asistente administrativa Teléfono: 0978765028 Correo: *anitahinojosa37@hotmail.com* Nombre: Ítalo Paucar Posición: Mensajero Teléfono: 0864569013 Correo: *italito.pau@gmail.com*

4.4.4 EQUIPO DE RELACIONES PÚBLICAS

Es responsable de la comunicación externa e interna.

Según el incidente será el responsable de comunicar a clientes y proveedores el tiempo en el que los servicios serán restablecidos.

Estar informado de las decisiones que tome el Comité de Crisis

Responsable del Equipo	Nombre: Tania Estrella Posición: Coordinadora Servicio al Cliente Teléfono: 0899372015 Correo: tanitasiempre@hotmail.com
Miembros del Equipo	Nombre: Lorena Pazmiño Posición: Gerente Talento Humano Teléfono: 09746383448 Correo: lpazminop@hotmail.com Nombre: Emilia del Pino Posición: Jefe de Talento Humano Teléfono: 084882092 Correo: iemmypino@gmail.com

4.4.5 EQUIPO DE UNIDADES DEL NEGOCIO

Estos equipos estarán formados por las personas que trabajan con las aplicaciones críticas, y serán los encargados de gestionar a sus supervisados para realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas.

4.4.6 PROCEDIMIENTOS PARA LA CONTINUIDAD

4.4.6.1 PROCEDIMIENTO DE NOTIFICACIÓN DEL DESASTRE

Cualquier empleado de Equivida que sea consciente de un incidente grave que puede afectar a la empresa, debe comunicar a su jefe inmediato y este a su vez al comité de crisis para su respectiva evaluación.

4.4.6.2 PROCEDIMIENTO DE EJECUCIÓN DEL PLAN

Una vez notificado del incidente el Comité de crisis se reunirá en el punto de encuentro definido, se evaluará el grado del incidente y decidirá si el Plan de Continuidad del Negocio es puesto en marcha, en caso afirmativo se iniciará el procedimiento de ejecución del Plan.

En caso de que el Comité decida no activar el Plan de Continuidad porque la situación no lo amerite, será necesario documentar el mismo y gestionarlo para que no aumente su gravedad

4.4.6.3 PROCEDIMIENTO DE NOTIFICACIÓN DE EJECUCIÓN DEL PLAN

Se tendrá un árbol de notificación y llamadas para avisar a los diferentes equipos que se definieron en el plan.

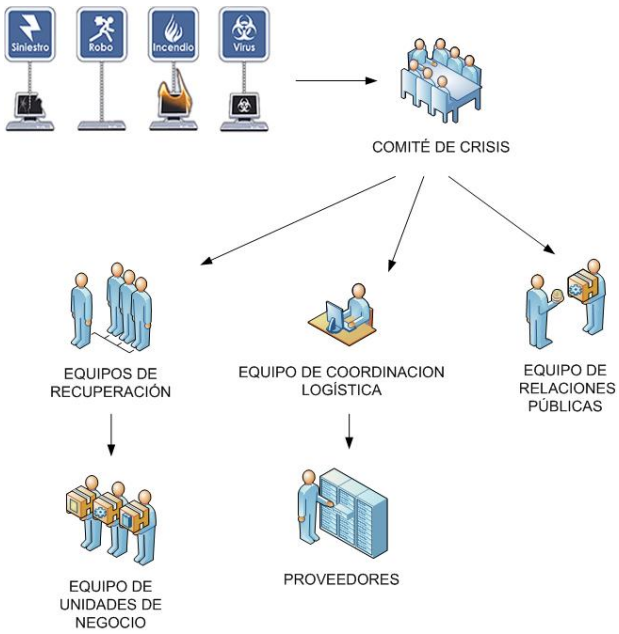


Ilustración 18 Procedimiento de ejecución del plan

PROCEDIMIENTOS PARA INCIDENTES DISRUPTIVOS

- Gestión de un incidente disruptivo
- Todos los empleados tienen la obligación de reportar incidentes
- Todos los empleados están obligados a informar cualquier incidente disruptivo de la siguiente manera:
- Todos los incidentes relacionados con tecnología de la información y de la comunicación son informados telefónicamente a la Jefatura de Sistemas
- Todos los demás incidentes son informados telefónicamente a la Jefatura de administración.

- Cualquier otro evento o vulnerabilidad del sistema que todavía no se hubiera convertido en un incidente disruptivo debe ser informado de la misma forma.
- Si un incidente demanda la intervención de la policía, de ambulancias o de los bomberos, la primera persona disponible debe llamar al ECU-911 y, desde allí, informar a la persona responsable de su unidad organizativa o al Gerente de crisis.
- En caso que ocurra un incidente, los empleados pueden comunicarse libremente sólo con sus familiares y con la policía, o los bomberos; mientras que cualquier otro tipo de comunicación se delega en el Comité de crisis.

GESTIÓN DE INCIDENTES DISRUPTIVOS

- La persona que recibe la información sobre el incidente debe evaluar si el incidente, o potencial incidente, es real o falso, y si es real, activa inmediatamente este plan respetando los siguientes pasos:
- Comenzar a controlar y erradicar el incidente de acuerdo a lo detallado en las siguientes secciones del presente documento.
- Informar a todas las personas responsables sobre la ocurrencia del incidente dentro de su área de responsabilidad.
- Notificar al comité de crisis, que debe evaluar si es necesario alertar a alguna de las partes interesadas.

- Controla el estado del incidente y, si es necesario, informa a quien lo reportó y a los demás empleados involucrados, acerca del progreso en la gestión del incidente.
- En caso que una persona no pueda controlar y/o erradicar el incidente, debe informarlo al Gerente de crisis. La información que se envía al Gerente de crisis debe incluir la naturaleza y alcance del incidente disruptivo, como también su potencial impacto.
- La persona responsable de erradicar el incidente debe registrar en el Registro de incidentes todas las acciones tomadas.

Gerente de crisis

El Gerente de crisis debe supervisar el progreso en la gestión del incidente y el período de interrupción de las actividades individuales y debe evaluar el tiempo necesario para solucionar el incidente.

Si el tiempo necesario para solucionar el incidente es mayor que el objetivo de tiempo de recuperación de una actividad particular, se debe activar el plan de recuperación para la actividad interrumpida. En ese caso, el Gerente de crisis debe notificárselo a todos los gerentes de recuperación, quienes activarán sus planes de recuperación.

Control y erradicación de un incidente

4.4.6.4 PROCEDIMIENTO DE EVACUACIÓN DEL EDIFICIO

(independientemente del tipo de incidente)

Se evacua el edificio y se dirige al personal hacia los puntos de encuentro especificados en la Lista de ubicaciones para continuidad del negocio.

Gerente de crisis	En caso que esté en riesgo la vida o la salud de las personas, emite una orden de evacuación. Si el Punto de encuentro 1 no está disponible, envía a alguien a señalizar la ubicación del Punto de encuentro 2 (señales de papel, flechas de dirección, banderas, señalización de vehículos, etc.). En caso de una amenaza maliciosa, decide la nueva ubicación del punto de encuentro (Punto de encuentro 3) y lo notifica a la persona responsable de ejecutar la evacuación.
Personas responsables de ejecutar la evacuación	Dirige la evacuación hacia el punto de encuentro. Verifica que todas las áreas estén vacías luego de la evacuación. En caso que alguien no haya podido salir del edificio, lo informa al 911.
Todos los empleados	Evacuan según los planes de evacuación para el edificio. Siguen las instrucciones suministradas por las personas

	responsables de dirigir la evacuación. Al evacuar, solamente llevan su bolso de mano y billetera, no llevan ningún otro elemento. Ayudan a evacuar a otras personas, si necesitan ayuda.
Gabinete de apoyo de crisis	Cuando la gente se ha reunido en el punto de encuentro, lleva un registro de todas las personas presentes y las que faltan.

Incendio

Se evacua el edificio de acuerdo con el plan de evacuación del edificio.

Gerente de crisis	En caso que esté en riesgo la vida o la salud de las personas, el Gerente de crisis emite una orden de evacuación. Escoge las medidas para disminuir el daño o salvar bienes, a menos que esto represente un riesgo para las personas.

Interrupción del suministro eléctrico

Gabinete de apoyo de crisis	Establece la causa de la interrupción; es originada por el cableado o por el distribuidor de electricidad.
Jefe de administración	Soluciona el problema junto con el distribuidor de electricidad.
Todos los empleados	Cumpliendo con los planes de recuperación, proceden con las formas alternativas para ejecutar actividades, sin el uso de electricidad.
Empleados del departamento de TI	Supervisan los dispositivos UPS y desconectan el sistema informático si es necesario.

Terremoto

Se evacua el edificio de acuerdo con el plan de evacuación del edificio.

Todos los empleados	Buscan refugio bajo el marco de una puerta, cerca de una pared interior de apoyo, o debajo de un escritorio. No corren hacia el exterior del edificio hasta que termine el terremoto. Una vez que el terremoto ha finalizado, intentan salvar a otras personas salvo que se haga más daño a la persona herida. En caso que se ordene la evacuación, proceden de acuerdo al plan de evacuación.
Gerente de crisis	En caso que esté en riesgo la vida o la salud de las personas, ordena la evacuación del edificio una vez que haya terminado el terremoto.
Gabinete de apoyo de crisis	Apaga todos los servicios: gas, electricidad, calefacción, ventilación, suministro de agua. Asegura el edificio y demás bienes.

Carta de amenaza

Todos los empleados	Si reciben una carta sospechosa, no la abren, la sostienen sólo por sus bordes externos. La colocan en un sobre vacío. Informa al Jefe de administración. Proceden según las instrucciones del Jefe de administración.
Gerente de crisis	Notifica a la policía a través del 911. Notifica al comité de crisis de la situación. Ejecuta las medidas impartidas por la policía.

Falla en las telecomunicaciones

Empleado del departamento de TI	Cualquier empleado recibe información sobre la falla. Si es necesario, coordina el proceso con proveedores de servicios de TI.
Empleados - usuarios de servicios de comunicación	Utilizan vías de comunicación alternativas.

Falla en el sistema de información

Empleado del departamento de TI	Cualquier empleado recibe información sobre el incidente. Si es necesario, coordina el proceso con proveedores de servicios de TI. Toma las medidas necesarias para evitar o controlar el incidente del sistema de información.
Gerente de crisis	Se asesora sobre todos los servicios importantes, evalúa la gravedad del incidente.
Todos los empleados	Si es posible, realizan procedimientos alternativos para llevar adelante las actividades.

Ataque de código malicioso

Empleado del departamento de TI	Cualquier empleado recibe información sobre el incidente. Si se trata de un código malicioso desconocido, notifica al Oficial de Seguridades de la información Notifica al fabricante del software antivirus. Si se ha identificado el origen externo del código malicioso,

	contacta a la persona responsable de TI de esa organización. Coordina la notificación a otros empleados; particularmente aquellos que intercambiaron mensajes con el sistema infectado. Si es necesario, coordina el proceso con proveedores de servicios de TI.
Todos los empleados	Desconectan físicamente de la red cualquier ordenador infectado, desactivan las redes inalámbricas, de Bluetooth, etc. No apagan los dispositivos de red y servidores; este es un trabajo de los empleados del departamento de TI.
Empleados del departamento de TI	Si el ordenador todavía no ha sido desconectado de la red, evalúa si lo desconecta para evitar mayor infección. Cierra su software (incluido el sistema operativo); para los servidores, evalúa si es necesario notificar primero a los usuarios del sistema. Consigue información sobre el tipo de código malicioso y sobre los pasos necesarios para su erradicación (desde Internet, de los proveedores). Procede de acuerdo a las instrucciones recibidas.

Violación de reglas internas o externas

Jefe de administración	El procedimiento se realiza de acuerdo a lo establecido en los procedimientos disciplinarios regulados por las leyes laborales y por la propia organización.

FASE DE TRANSICIÓN

4.4.7 PROCEDIMIENTO DE CONCENTRACIÓN Y TRASLADO DE MATERIAL Y PERSONAS

Notificados todos los equipos involucrados y activado el Plan, deberán acudir al centro de reunión indicado, además del traslado del personal al centro de recuperación hay que trasladar todo el material necesario para poner en marcha las actividades.

- Cintas de back up
- Material de oficina
- Documentación

Esto tiene que realizarlo el equipo de logística y documentar en el Plan de transporte.

Plan de transporte

En caso que se activen planes de recuperación, el transporte se organizará de la siguiente manera:

Tabla 10 Registro para el plan de transporte

Ubicación de partida	*Ubicación de destino*	*Quién o qué es transportado*	*Persona responsable de la coordinación*	*Medios de transporte*	*Transportista*

4.4.8 PROCEDIMIENTO DE PUESTA EN MARCHA DEL CENTRO DE RECUPERACIÓN

Una vez que el equipo de recuperación llegue al Centro de recuperación y que los materiales empiecen a llegar, pueden comenzar a instalar las aplicaciones en los equipos que se encuentran en esta oficina.

El equipo de recuperación solicitará al equipo de logística cualquier tipo de material extra que fuera necesario para la recuperación.

FASE DE RECUPERACIÓN

4.4.9 PROCEDIMIENTO DE RESTAURACIÓN

El orden de recuperación de las funciones se realizará según la criticidad los sistemas.

Los dos primeros sistemas deben recuperarse lo antes posible, en las 48 horas siguientes.

Para identificar los requerimientos de recuperación se pueden distinguir las siguientes áreas que deben ser recuperadas:

Área de trabajo: Área de trabajo u oficina alternativa para la administración de la crisis

Sistemas de IT e infraestructura: Se clasifica los recursos de TI en las siguientes categorías.

- Sistemas críticos TI
- Enlaces de datos
- Enlaces de voz
- Servidores
- Recursos
- Datos e información crítica

4.4.9.1 PROCEDIMIENTOS PARA LA RECUPERACIÓN DE INFORMACIÓN DESDE LOS BACKUP.

Dentro de las operaciones diarias en la realización de respaldos de la base de datos del sistema ERP, el departamento de sistemas genera los respaldos mediante los procesos batch los cuales se encargan de crear los archivos de backup, copiarlos a dispositivos de almacenamiento externos los cuales son: servidores alternos dentro de la misma infraestructura, discos duros en estado compartido y cintas magnéticas.

Objetivo

Establecer lineamientos para la obtención de respaldos de los datos de los sistemas críticos que se generan en cintas de respaldo para el envío a sitios externos de las oficinas.

Alcance

El procedimiento de restauración de Backup para los diferentes sistemas de información de la empresa como: Bases de datos, configuraciones y sistemas.

Desarrollo del procedimiento:

El departamento de sistemas es el encargado de coordinar el envío y recepción de las cintas magnéticas con el proveedor Lockers.

Para la solicitud del respaldo de una cinta magnética se tiene que solicitar a través del formulario: Solicitud de Cintas a Lockers

EMPRESA DE GESTIÓN DE RESPALDOS LOCKER´S		
NOMBRE DE LA EMPRESA:		FECHA DE SOLICITUD:
RESPONSABLE ENTREGA DOCUMENTOS:		HORA:
APROBADO POR:		
NOMBRE:		CARGO:
NRO. CINTA	DESCRIPCIÓN	CANTIDAD DE CINTAS/DOC.
Firma:		
CI:		
Dirección de entrega:		

Este documento se tiene que entregar a un motorizado de la compañía Locker’s para que este sea el encargado de devolver el paquete a la dirección solicitada en ese momento.

La cinta tiene que ser entregada al coordinador de Infraestructura o la persona encargada con esas funciones especificas.

Los servidores de respaldo se tiene que configurar con las mismas características que los originales para evitar cualquier tipo de incompatibilidad al tratar de recuperar la información.

La cinta será recuperada con los últimos datos de información, base de datos, sistemas.

Llenar el documento de recuperación de respaldos para controlar las actividades que se realizaron.

REGISTRO DE RECUPERACIÓN DESDE CINTAS (BACKUPS)		
CINTA RESTAURADA:		
FECHA:	***SOLICITADO POR:***	***APROBADO POR:***
SISTEMAS OPERATIVOS AFECTADOS:		
USUARIOS AFECTADOS:		
OBSERVACIONES:		

4.4.9.2 PROCEDIMIENTO DE DOCUMENTACIÓN Y REGISTRO DE CONFIGURACIONES PARA RECUPERACIÓN: SOFTWARE Y HARDWARE

Para la administración adecuada de la recuperación en sistemas de información.

Objetivo

Establecer lineamientos de registro de configuraciones de software y hardware de los diferentes sistemas de información, mediante la utilización de bitácoras asegurando el funcionamiento correcto y oportuno en escenarios de desastre que requieran la reconfiguración e instalación de los diferentes sistemas en otros sitios seleccionados para la reanudación de las actividades.

Alcance

El procedimiento de documentación y registro de configuraciones se registrará en incidentes que obliguen a instalar y configurar los sistemas en otros equipos que se encuentren fuera del lugar habitual de trabajo.

Desarrollo del procedimiento:

El departamento de sistemas es el encargado de coordinar la distribución e instalación de los sistemas en los equipos entregados provisionalmente para reanudar las actividades.

Por cada equipo configurado se guardará el registro del usuario y los sistemas instalados junto a la descripción del equipo.

El coordinador de infraestructura verificará que los equipos con los sistemas instalados tengan acceso a la información que necesiten para su respectivo funcionamiento

Se tendrá que llenar el documento de: documentación y registro de configuraciones.

El administrador de red comunica al encargado de tecnología y al responsable de la administración de datos que los canales de comunicación están listos para el acceso de todos los dispositivos.

4.4.9.3 PROCEDIMIENTO DE SOPORTE Y GESTIÓN

Una vez recuperados los sistemas, se avisará a los equipos de los departamentos que gestionan los sistemas (listado del equipo de Unidades de Negocio) para que realicen las comprobaciones necesarias que certifiquen que funcionen de manera correcta y pueda continuarse dando el servicio.

Además el Equipo de Seguridad deberá comprobar que existen las garantías de seguridad necesarias (confidencialidad, integridad, disponibilidad) antes de dar por terminada la fase de recuperación.

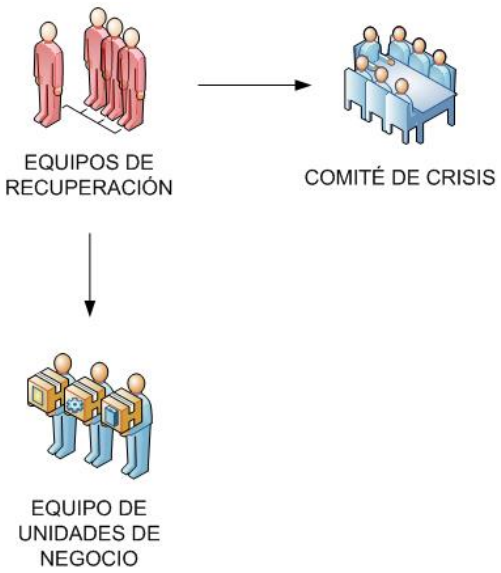


Ilustración 19 Procedimiento de soporte y gestión

FASE DE VUELTA A LA NORMALIDAD

Una vez restablecido los procesos críticos y solventados la contingencia, hay que definir las diferentes estrategias y acciones para recuperar la normalidad de todos los servicios de la compañía.

4.4.10 ANÁLISIS DEL IMPACTO, REGISTRO DE INCIDENTES (ANEXO IV)

Se realiza una valoración detallada de los equipos e instalaciones dañada. Para ello, el equipo de recuperación junto con el equipo de seguridad, realizarán un listado de los elementos que han sido dañados gravemente y son irrecuperables, así como de todo el material que se puede volver a utilizar. Esta evaluación deberá ser comunicada lo antes posible al equipo director para que determinen las acciones necesarias que lleven a la operación habitual lo antes posible.

Los incidentes se clasifican dentro de los siguientes tipos:

- Relacionados con la información (directamente relacionados con tecnología de la información y comunicación)
- No relacionados con la información (todos los demás incidentes)

ADQUISICIÓN DE NUEVO MATERIAL

Una vez realizada la evaluación del impacto, se determinará la necesidad de nuevo material. El Comité de Crisis contactará con el seguro de la compañía para conocer qué parte cubre el seguro y qué inversión tendrá que hacer la compañía en el material que no se pueda recuperar.

Contactar con los proveedores para que en el menor tiempo posible reponga todos los elementos dañados.

FIN DE LA CONTINGENCIA

Dependiendo de la gravedad del incidente, la vuelta a la normalidad de operación puede variar entre unos días (si no hay elementos clave afectados) e incluso meses (si hay elementos clave afectados). Lo importante es que durante el transcurso de este tiempo de vuelta a la normalidad, se siga dando servicio a los clientes y trabajadores por parte de la compañía y que la incidencia afecte lo menos posible al negocio.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- El desarrollo del Plan permitió definir objetivamente los procesos críticos de la compañía que sirvió además de apoyo a la toma de decisiones en otros ámbitos.
- El desarrollo de un Plan de Continuidad permite una consolidación de intereses entre la Alta Dirección y las diferentes Unidades organizativas al constatar que diferentes áreas apoyan a procesos idénticos.
- Es importante contar con asesoría especializada y software apropiado que facilite el desarrollo del estudio y garantice calidad a los resultados

RECOMENDACIONES

- Dar continuidad al plan con revisiones de los procesos, personas y componentes involucrados a través de talleres al menos una vez al año para generar conciencia de la utilidad del Plan y se pueda aportar mejoras al mismo.

- Difundir el Plan de Continuidad a los nuevos colaboradores que ingresan a la compañía, para hacerles participe del mismo y fortalecer los Equipos que componen el plan.
- Replicar el Plan de Continuidad a las distintas sucursales del Ecuador para contar con mayor resiliencia a cualquier incidente.
- Implementar un Sistema de Gestión de Seguridad de la Información que vaya a la par con un Sistema de Gestión de la Continuidad para darle el respaldo respectivo a todas las funciones del negocio y con eso mayor valor al negocio.

Bibliografía

Borrmart. (2012). *La necesidad de implantación de un Plan de Continuidad del Negocio.*

Carrasco, M. (29 de 10 de 2012). *Administracíon electrónica*. Obtenido de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Gallardo, P. C. (2011). *Análisis de Riesgos Informáticos y elaboración de un Plan de Contingencia TI.* Quito.

Gaspar, M. J. (2012). *El Plan de Continuidad del Negocio.* Madrid: McGraw-Hill.

Juaquin, E. (03 de 07 de 2010). *Gobierno de seguridades*. Obtenido de www.gobiernoenlinea.gov.co/

Kosutic, D. (02 de 2012). *Estándares Iso 22301*. Recuperado el 15 de 03 de 2013, de http://www.iso27001standard.com/ique-es-iso-22301

Lenner, S. (s.f.). *www.continuityplantemplates.com.* Recuperado el 12 de 11 de 2012, de http://www.continuityplantemplates.com/business-impact-assessment-tool

María Gallardo, P. J. (2011). *Análisis de riesgos informáticos y elaboración de un plan de contingencia T.I. para la empresa eléctrica Quito S.A.* Quito: Escuela Politécnica Nacional.

Moran, M. (2011). *Elaboración del Plan de Continuidad del Negocio para la Empresa Compteco compra por teléfono consorcio comercial S.A.* Sangolquí : Escuela Politécnica del Ejercito.

Pino, L. d. (2009). *Guía de Desarrollo de un Plan de Continuidad del Negocio.* Madrid: Universidad Politécnica de Madrid.

Solana, M. (2001). *Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información.* Lima: Instituto Nacional de Estadística e Informática.

Quito, 16 de Febrero del 2012

Señores:

Escuela Politécnica del Ejército

Presente:

AUSPICIO

Equivida S.A , Seguros para Personas, mediante el Departamento de Innovación y Desarrollo Tecnológico , tiene el agrado de Auspiciar la Tesis del Sr. Estudiante Cárdenas Pallo Andrés Leonardo, cédula de identidad No. 1720524451, que tiene por tema DESARROLLO DEL PLAN DE CONTINUIDAD DEL NEGOCIO (BCP)el mismo que tiene por objetivo un entregable del Plan de Continuidad del Negocio para Equivida S.A, que son de vital importancia para nuestra empresa y el desarrollo continuo e imprescindible de la misma.

Agradeciendo la atención prestada a la presente, me suscribo.

Atentamente,

Ing. María Isabel Quiroz

Gerente de Innovación y Desarrollo Tecnológico

Quito, 14 de Noviembre del 2013

Señores:

Escuela Politécnica del Ejército

Presente:

ACEPTACIÓN

Equivida S.A, Seguros para Personas, mediante el Departamento de Innovación y Desarrollo Tecnológico, da a conocer la aceptación del entregable de la Tesis del Sr. Estudiante Cárdenas Pallo Andrés Leonardo, cédula de identidad No. 1720524451, el cuál es el Plan de Continuidad del Negocio para Equivida para el período 2012-2015.

Agradeciendo la atención prestada a la presente, me suscribo.

Atentamente,

Ing. María Isabel Quiroz

Gerente de Innovación y Desarrollo Tecnológico

Biografía

Nombre: Andrés Leonardo Cárdenas Pallo

Nacionalidad: Ecuatoriana

Lugar de nacimiento: Quito

Fecha de nacimiento: 28 de Julio de 1985

Instrucción Primaria

Nombre: Pensionado San Vicente

Período: 1992-1997

Instrucción Secundaria

Nombre: Colegio Experimental Juan Pío Montúfar

Período: 1998-2003

Certificaciones

Implementador Buxis TTHH

SOA Architect Certified

Sistema de Gestión de la Seguridad 27001

Itil Foundation

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADO POR

_____

Andrés Leonardo Cárdenas Pallo

DIRECTOR DE LA CARRERA

_____

Ing. Mauricio Campaña

Sangolquí, Noviembre del 2013