



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN
Y TRANSFERENCIA DE TECNOLOGÍA
CENTRO DE POSGRADOS**

CARRERA DE MAESTRÍA EN GERENCIA DE SISTEMAS

**TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL
TÍTULO DE MAGISTER EN GERENCIA DE SISTEMAS**

**TEMA “DESARROLLO DE UN PLAN DE CONTINUIDAD DEL
NEGOCIO PARA EL DEPARTAMENTO DE TECNOLOGÍA DE
YELLOWPEPPER”**

AUTOR: SALINAS CARRANZA, ANGELA JESSENIA

DIRECTOR: ING. PÁLIZ, VICTOR MSc

SANGOLQUÍ

2016



**VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA
DE TECNOLOGÍA**

CENTRO DE POSGRADOS

CARRERA DE MAESTRÍA EN GERENCIA DE SISTEMAS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO PARA EL DEPARTAMENTO DE TECNOLOGÍA DE YELLOWPEPPER" realizado por la señora **Angela Jessenia Salinas Carranza**, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a la señora **Angela Jessenia Salinas Carranza** para que lo sustente públicamente

Sangolquí, 1 de Julio del 2015



ING. VICTOR PALIZ MSc
DIRECTOR



**VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA
DE TECNOLOGÍA**

CENTRO DE POSGRADOS

CARRERA DE MAestrÍA EN GERENCIA DE SISTEMAS

AUTORÍA DE RESPONSABILIDAD

Yo, **Angela Jessenia Salinas Carranza**, con cédula de identidad N° 0703583062, declaro que este trabajo de titulación **"DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO PARA EL DEPARTAMENTO DE TECNOLOGÍA DE YELLOWPEPPER"** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 25 de mayo del 2016



ING. ANGELA JESSENIA SALINAS

0703583062



**VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA
DE TECNOLOGÍA**

CENTRO DE POSGRADOS

CARRERA DE MAestrÍA EN GERENCIA DE SISTEMAS

AUTORIZACIÓN

Yo, **Angela Jessenia Salinas Carranza**, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación "DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO PARA EL DEPARTAMENTO DE TECNOLOGÍA DE YELLOWPEPPER" cuyo contenido, ideas y criterios son de mi autoría y responsabilidad

Sangolquí, 25 de mayo del 2016



ING. ANGELA JESSENI SALINAS

0703583062

DEDICATORIA

La creación de este proyecto está dedicada a mi mejor amigo, DIOS, mi esposo e hija y mis padres, quienes representan la base de mi existir. A Dios por ser mi guía y luz durante mí diario andar, a mi amado esposo Javier e hija Danna por creer en mí, siendo mi apoyo en todo momento. A mis queridos padres quienes me formaron y enseñaron entre otras cosas a ser perseverante y luchadora, a todos ellos, con todo mi amor y admiración les dedico este proyecto.

Angela Jessenia Salinas Carranza

AGRADECIMIENTO

El desarrollo de este proyecto no es más que el resultado del conocimiento adquirido en Yellowpepper y del granito de arena aportado por todas las personas que formaron y forman parte de esta prestigiosa empresa. A todos ellos mi más sincero agradecimiento

Angela Jessenia Salinas Carranza

ÍNDICE

ÍNDICE	vii
ÍNDICE DE TABLAS.....	xi
ÍNDICE DE FIGURAS.....	xii
RESUMEN.....	xiii
CAPITULO 1.....	1
1.1 Planteamiento del problema	1
A. Descripción del problema.....	1
B. Preguntas de Investigación	1
1.2 Objetivos.....	2
A. Objetivo General	2
B. Objetivos Específicos	2
1.3 Metodología.....	3
CAPITULO 2.....	5
ANÁLISIS DE LA EMPRESA.....	5
2.1 Descripción de la Empresa.....	5
A. ¿Quién es Yellowpepper?	5
B. Visión General.....	5
C. Estructura de Yellowpepper	6
2.2 Departamento de TI.....	7
A. Esquema organizacional del departamento de TI	7
B. Roles y responsabilidades	8

C.	Infraestructura técnica.....	15
D.	Seguridades	15
E.	Arquitectura lógica.....	16
F.	Arquitectura física.....	16
G.	Aplicaciones	18
CAPITULO 3.....		20
ANÁLISIS DE IMPACTO		20
3.1	Política.....	20
3.2	Alcance.....	20
3.3	Suposiciones	20
3.4	Identificaciones de funciones y procesos	21
3.5	Evaluación del Impacto Financiero.....	23
3.5	Evaluación del Impacto Operacional	25
3.6	Identificación de Procesos Críticos del Negocio.....	27
3.8	Identificación del MTD	28
3.9	Determinación del RTO y WRT	30
3.10	Análisis del daño que causa la interrupción de un proceso.....	31
3.11	Conclusiones.....	33
CAPITULO 4.....		35
ANÁLISIS DE RIESGOS		35
4.1	Identificación de Riesgos.....	35
4.2	Análisis de Riesgos	38
4.3	Evaluación de Riesgos	42
4.4	Tratamiento de Riesgos	44

4.5	Conclusiones y recomendaciones	47
A.	Conclusiones.....	47
B.	Recomendaciones.....	47
CAPITULO 5.....		48
5.1	Criterios para declaración de desastre	48
5.2	Plan de comunicación	49
5.3	Estrategias de recuperación	50
5.4	Requerimientos estratégicos para la recuperación de la plataforma	51
5.5	Identificar las opciones de recuperación	51
5.6	Evaluación de opciones aplicables.....	54
A.	Recurso: Instalaciones	55
A.	Recurso: Infraestructura.....	55
B.	Recurso: Sistemas de producción.....	55
C.	Recurso: Información	56
5.7	Análisis costo/beneficio de las estrategias de recuperación.....	56
5.8	Selección de la estrategia	57
5.9	Declaración de desastre.....	61
CAPITULO 6.....		62
6.1	Estructura del equipo PCN	62
6.2	Equipos y responsabilidades.....	63
A.	Comité de crisis	63
B.	Equipo de recuperación	65
F.	Equipo de las unidades de negocio.....	66
G.	Logística.....	66

H. Relaciones públicas	67
6.3 Desarrollo de procedimientos	67
A. Plan de respuesta ante una emergencia	68
B. Plan de Gestión de Crisis	68
C. Planes de recuperación y restauración	68
CAPITULO 7.....	70
MANTENIMIENTO DEL PLAN DE CONTINUIDAD DEL NEGOCIO.....	70
7.1 Ejecución de pruebas.....	70
7.2 Cronograma de mantenimiento del PCN.....	71
BIBLIOGRAFIA.....	73
GLOSARIO.....	75

ÍNDICE DE TABLAS

Tabla 1 Funciones y procesos de yellowpepper	21
Tabla 2 Escala para medir el impacto financiero	23
Tabla 3 Evaluación del impacto financiero.....	23
Tabla 4 Categorías para evaluación del impacto operacional	25
Tabla 5 Niveles de impacto operacional	25
Tabla 6 Impacto operacional.....	26
Tabla 7 Procesos críticos del negocio	28
Tabla 8 Procesos críticos del negocio	29
Tabla 9 Escala de equivalencia para definición de MTD	29
Tabla 10 Definición del MTD.....	30
Tabla 11 Determinación de RTO y WRT	30
Tabla 12 Consecuencias de la interrupción de los servicios.....	32
Tabla 13 Identificación de riesgos.....	35
Tabla 14 Análisis de riesgo	40
Tabla 15 Evaluación del riesgo.....	43
Tabla 16 Alternativas de manejo de negocio	44
Tabla 17 Criterios para declaración de desastres.....	48

ÍNDICE DE FIGURAS

Figura 1 Prceso de gestión del riesgo según la norma an/nzs 4360:2004	3
Figura 2 Organigrama del departamento de ti de yellowpepper	7
Figura 3 Diagrama de redes y servidores de yellowpepper	18
Figura 4 Catriz de priorización	39
Figura 5 Criterios de evaluación de riesgo.....	43
Figura 6 Plan de crisis	49
Figura 7 Organización de equipos en declaración de desastre	63

RESUMEN

En la actualidad Yellowpepper opera en 7 países de la Región Andina y Central, con un promedio de 25 millones de transacciones mensuales, y sus servicios son utilizados por al menos 5.5 millones de usuarios. Por su continuo crecimiento y por la naturaleza de sus operaciones el área de Tecnología de Yellowpepper ha visto de vital importancia contar con un Plan de Continuidad de los Servicios Financieros Móviles. El presente proyecto de tesis detalla el desarrollo del Plan de Continuidad de Negocio para el área de Tecnología de la empresa Yellowpepper utilizando las mejores prácticas descritas en el estándar BS 25999. El proyecto inicia con el análisis de Yellowpepper en donde se conoce su visión, misión, líneas de negocio, y estructura de la misma, se realiza un análisis de riesgos en donde se identifica los riesgos que afronta Yellowpepper, emitiendo recomendaciones para su mitigación. Por otro lado, se realiza un análisis de impacto del negocio en donde se identifica las áreas y procesos críticos del negocio, y los tiempos máximos tolerables de interrupción que pueden enfrentar los procesos críticos de Yellowpepper para el desarrollo de la estrategia de recuperación más adecuada, se crean equipos para durante y después de la contingencia, así como procedimientos y planes para el reestableciendo de operaciones de Yellowpepper.

Palabras Claves

PCN

BCP

BIA

CONTINUIDAD

BS25999

ABSTRACT

Nowadays Yellowpepper operates in 7 countries of the Andean and Central Region, with an average of 25 million monthly transactions, and its services are used by at least 5.5 million users. For its continued growth and the nature of its operations area, it has been vital to have a Business Continuity Plan. This project details the development of a business continuity plan for the area Yellowpepper Technology using the best practices described in the BS 25999 standard. The project starts with Yellowpepper analysis then threat and risk assessments are made. On the other hand, a business impact analysis where areas and critical business processes are identified, and the maximum period of time that a given business process can be inoperative before Yellow Pepper's survival is at risk. Business continuity strategy are developed, equipment during and after the contingency and procedures and plans for reestablishing of operations of the Yellowpepper are created.

Keywords

PCN

BCP

BIA

CONTINUIDAD

BS25999

DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO PARA EL DEPARTAMENTO DE TECNOLOGÍA DE YELLOWPEPPER

Hoy en día, la exposición al riesgo es una realidad en todas las empresas siendo importante hacer pedagogía sobre la continuidad de negocio en las mismas. A pesar de que en nuestra cultura latinoamericana hemos sido hábiles a la hora de responder ante eventos inesperados y hemos sido muy creativos a la hora de ofrecer soluciones de último minuto, se torna importante que las organizaciones sin considerar su tamaño, adopten un sistema de gestión de continuidad de negocio el cual tiene como propósito comprometer esfuerzos y poner en práctica procedimientos de continuidad que resguarden el cuidado de las personas, activos de información y procesos críticos del negocio, contra eventos de desastres o fallas mayores y de las posibles consecuencias que de ellos deriven, producto de la no disponibilidad de los recursos de la organización y/o los componentes necesarios para la prestación de sus servicios críticos.

“El 90% de las empresas que tienen pérdidas significativas de datos desaparecen en un plazo de tres años, según Disaster Recovery Institute International” (Infraestructura, s.f.). La continuidad del negocio no simplemente se relaciona con fenómenos físicos como incendios o fallos tecnológicos, sino que se extiende de tal forma que la reputación y el valor del accionista son elementos clave. En consecuencia, las organizaciones deberían desarrollar e implementar lo que se conoce como Plan de Continuidad de Negocio (BCP) y Plan de Recuperación de Desastres (DRP). El Plan de Continuidad de Negocio (BCP) es un plan que sirve para mantener la funcionalidad de una organización, a un nivel mínimo aceptable durante una contingencia. Esto implica que un Plan de Continuidad de Negocio (BCP) debe contemplar todas las medidas preventivas y de recuperación para cuando se produzca una contingencia que afecte al negocio.

Plan de Continuidad del Negocio (BCP) “es el conjunto de procedimientos e información documentados que se desarrolla, compila y mantiene preparado para su uso en caso de producirse un incidente, para permitir a una Organización seguir desempeñando sus actividades críticas a un nivel aceptable predefinido” (BS 25999-1, 2006). El análisis del impacto del negocio conocido comúnmente como Business Impact Analysis (BIA) y el análisis de riesgos son la base para el desarrollo de un plan de continuidad del negocio. El BIA permite determinar y entender qué procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto, mientras que el análisis de riesgos permite conocer los riesgos a los que está expuesto para su posterior tratamiento.

CAPITULO 1

1.1 Planteamiento del problema

A. Descripción del problema

Los servicios financieros móviles que ofrece Yellowpepper están conectados con ciertas entidades financieras y también con operadoras móviles de celular procesando más de 25 millones de transacciones cada mes. Estos servicios operan las 24 horas, los 7 días de la semana y los 365 días al año ininterrumpidamente, por lo que es de vital importancia contar con un Plan de Continuidad del Negocio para la empresa que permitirá responder ante los incidentes o interrupciones de negocio, con el fin de permitir a la organización continuar ejerciendo sus actividades.

B. Preguntas de Investigación

- ¿Tiene el Departamento de Tecnología de Yellowpepper un Plan de Continuidad del Negocio para los Servicios Financieros Móviles que ofrece a sus Clientes?
- ¿Cuál es el tiempo máximo de recuperación del servicio en caso de producirse un incidente grave que afecte la continuidad de las actividades de Yellowpepper?
- ¿Cuáles son las mejores prácticas basadas en el estándar BS 25999 para la elaboración de un Plan de Continuidad del Negocio con el cual la empresa Yellowpepper pueda garantizar a sus clientes que sus servicios financieros móviles tendrán una alta disponibilidad?
- ¿Cuáles son los servicios financieros móviles de Yellowpepper considerados más críticos en caso de producirse un incidente?

- ¿Cuáles son los indicadores de indisponibilidad que el Departamento de Tecnología de la empresa Yellowpepper debe considerar para declarar que se ha producido una interrupción del servicio?

1.2 Objetivos

A. Objetivo General

Desarrollar un Plan de Continuidad del Negocio que dé respuesta a posibles incidentes que pudieran poner en peligro la continuidad de las actividades críticas de la empresa Yellowpepper, usando el estándar BS 25999.

B. Objetivos Específicos

- Levantar información que permita entender el funcionamiento a la empresa Yellowpepper.
- Analizar los impactos financieros y operacionales ante un desastre en la empresa.
- Identificar las posibles amenazas potenciales de interrupciones de la empresa Yellowpepper y los respectivos riesgos.
- Desarrollar estrategias de continuidad del negocio, que satisfaga los requerimientos de recuperación identificados en el análisis de impacto y en los escenarios de amenazas.
- Elaborar el plan de continuidad de negocio, el cual es un informe que contendrá los procedimientos y lineamientos concretos para la recuperación y el restablecimiento de los recursos dañados y de los procesos cuyo desempeño se ha interrumpido.
- Evaluar el Plan de Continuidad del Negocio Propuesto

1.3 Metodología

El análisis de Riesgo será realizado bajo los lineamientos del estándar Australiano/Neozelandés AS/NZS 4360:2004. Este estándar está compuesto por cinco partes interrelacionadas, tal como se observa en la **Figura 1**, todas ellas mediadas por procesos de comunicación y consulta y monitoreo y revisión.

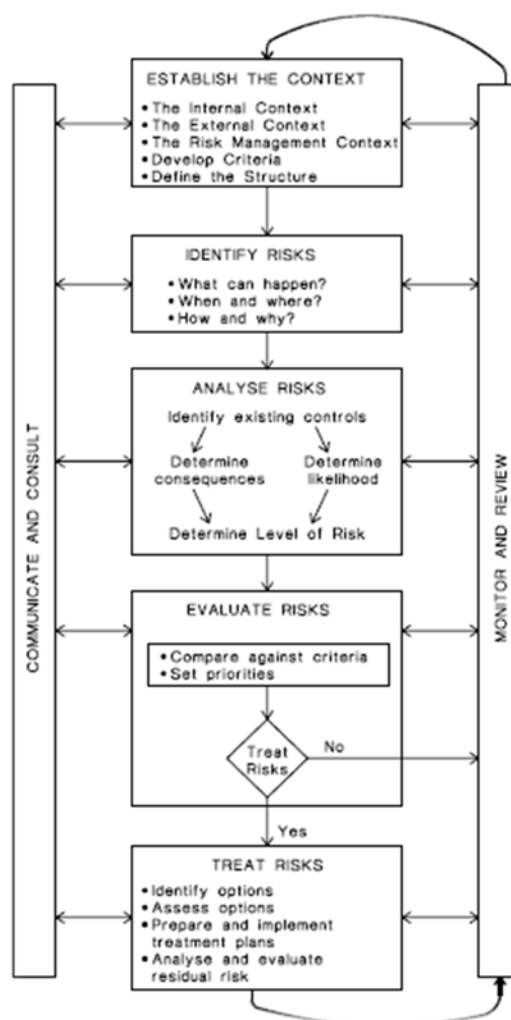


Figura 1 Proceso de gestión del riesgo según la norma AN/NZS 4360:2004

FUENTE: (Norma AN/NZS 4360, 2004)

Para el análisis de impacto del negocio, se ha seguido los lineamientos del libro Business Continuity Planning Methodology 2004, autores libro Akhtar Syed & Afsar Syed, el cual propone los siguientes aspectos a ser determinados para el análisis de impacto del negocio:

- Política, alcance y suposiciones
- Identificaciones de funciones y procesos
- Evaluación del impacto financiero
- Evaluación del impacto operacional
- Identificación de procesos críticos del negocio
- Identificación de MID
- Determinación del Recovery Time Objective (RTO) y Work Recovery Time (WRT)
- Análisis del daño que causa la interrupción de un proceso

La obtención de datos necesitados, se lo realizó a través de una combinación de reuniones y encuestas, las cuales fueron realizadas a los Gerentes de cada departamento de Yellowpepper. El formato de estas encuestas se encuentra en el Anexo 1 del documento.

Finalmente, la metodología a emplearse para el desarrollo del presente proyecto será basada en el ESTANDAR BS 25999, el mismo que comprende las siguientes etapas:

- Entendimiento de la organización
- Determinación de la estrategia de continuidad del negocio
- Desarrollo e implantación de una respuesta de GCN
- Prueba mantenimiento y revisión

CAPITULO 2

ANÁLISIS DE LA EMPRESA

2.1 Descripción de la Empresa

A. ¿Quién es Yellowpepper?

Yellowpepper es una empresa que ofrece el canal móvil a instituciones financieras a través de una sofisticada infraestructura tecnológica llamada **YEPEX**.

Yepex se encuentra en el centro del ecosistema de la red de servicios financieros móviles como un propulsor y conector de instituciones financieras, operadoras de telefonía móvil, empresas, consumidores y gobierno. Fue creado en el 2004 y tiene presencia en 7 países de la región:

- Colombia
- Ecuador
- Guatemala
- Mexico
- Peru
- Panama
- Estados Unidos

Actualmente está integrada a más de 40 instituciones financieras, posee más de 5 millones de usuarios y procesa más de 25 millones de transacciones por mes.

B. Visión General

Yepex provee productos de Emisión & Aceptación para alcanzar su visión de crear la red de pagos móviles líder en América Latina.

Líneas de Negocio

Yellowpepper cuenta con 2 líneas de negocios que son soportadas por la organización, siendo estas:

- **BANCA MÓVIL:** YellowPepper es el enlace entre la Institución Financiera y sus clientes a través del canal móvil (SMS, USSD, Smartphone).
- **SWITCH TRANSACCIONAL:** Provee servicios financieros a clientes no bancarizados empoderándolos hacia la inclusión financiera.

C. Estructura de Yellowpepper

El Comité Ejecutivo de Yellowpepper se encuentra ubicado en la ciudad de Miami y la matriz en la ciudad de Quito. Yellowpepper cuenta con 2 tipos de personal:

Personal local: Colombia, Ecuador, Guatemala, México, Perú, Panamá y Estados Unidos cuenta con personal local y este solo trabaja para el país al que pertenece. Generalmente estos cargos son: de gerente general, contadores, comerciales, limpieza y secretaria.

Personal global: Estas personas dan soporte a toda la organización. El 80% del mismo trabaja desde las oficinas de Quito-Ecuador. Estas áreas son:

- Financiera
- Soporte
- Consultoría y pruebas
- Proyectos
- Operaciones e Infraestructura
- Desarrollo

2.2 Departamento de TI

Dado que, Yellowpepper basa sus servicios en tecnología, depende en gran medida del departamento de tecnología. El Departamento de TI se encarga de que la infraestructura y sistemas a su cargo ofrezcan los niveles necesarios de disponibilidad y estabilidad y proporciona todos los servicios necesarios para garantizar el trabajo diario de toda la organización. El departamento de tecnología de Yellowpepper se encuentra ubicado en la ciudad de Quito-Ecuador y cuenta con 26 personas.

A. Esquema organizacional del departamento de TI

El Organigrama del departamento de TI de Yellowpepper se muestra en la Figura 2.

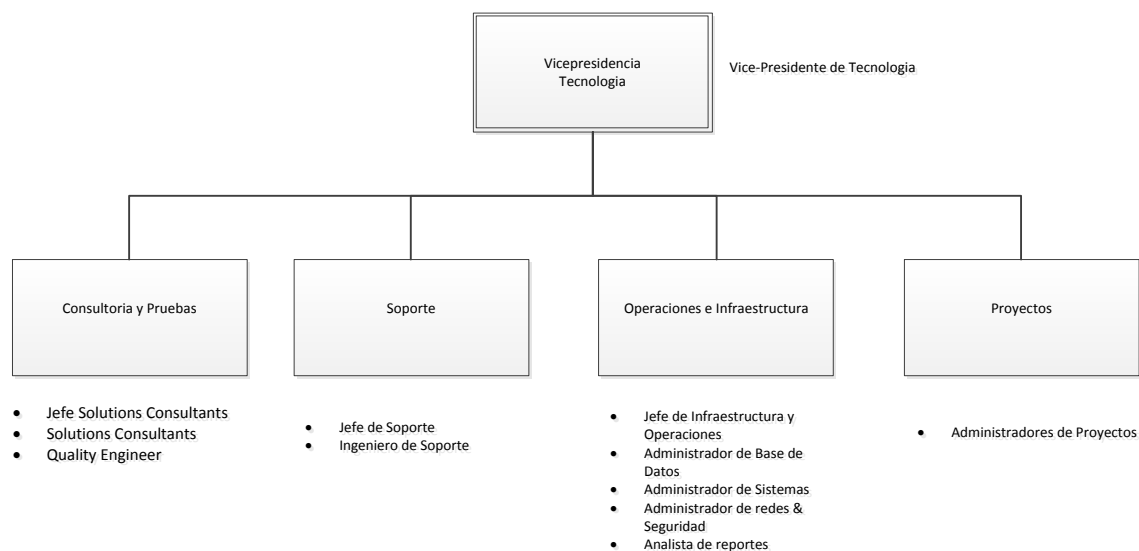


Figura 2 Organigrama del departamento de TI de Yellowpepper

Fuente: (Yellowpepper)

El departamento de TI está encabezado por un Vicepresidente de Tecnología el cual reside en la ciudad de Miami Florida y está conformado por 4 secciones:

- Proyectos
- Consultoría y Pruebas
- Soporte
- Operaciones e Infraestructura

B. Roles y responsabilidades

A continuación, se describen las funciones de cada sección, así como los roles y responsabilidades del personal que forma parte de cada sección:

C. Proyectos

Es la encargada de la definición, planificación y seguimiento del portafolio de proyectos. Está compuesto por 2 administradores de proyectos uno en Ecuador y otro en Perú, entre sus responsabilidades están:

- Definir los proyectos que serán aprobados y priorizados por el Comité Ejecutivo
- Programar de fechas de ejecución, pruebas y liberación de los mismos
- Dar seguimiento de los proyectos y realizar ajustes de tiempos en los mismos
- Reportar al Comité Ejecutivo del avance de los proyectos
- Reportar al área comercial del avance de sus proyectos

D. Consultoría y Pruebas

Es la encargada de la ejecución del desarrollo y pruebas de los proyectos aprobados y priorizados por el Comité Ejecutivo. Esta sección es liderada por un jefe de consultares. A continuación, se explica cómo está integrada esta sección:

- **Jefe de Consultores:** Radica en la ciudad de Quito/Ecuador, sus funciones son:
 - Asignar los proyectos aprobados por el Comité Ejecutivo de acuerdo a las prioridades dadas a los consultores

- Balancear el trabajo de los consultores
- Asignar ingenieros de pruebas a los proyectos aprobados y asignados a los consultores
- Dar seguimiento de los desarrollos en curso y resolver conflictos o cambios de prioridades de las soluciones tecnológicas
- **Consultores:** Formado por 5 personas, 2 en Ecuador, una en Colombia, otro en Perú y el último en México. Sus responsabilidades son:
 - Guiar a clientes a formular requerimientos, asesorar sobre alternativas y las implicaciones que llevan las modificaciones nuevas o ya revisadas
 - Mantener un contacto continuo con los clientes para identificar problemas y mejoras.
 - Crear la documentación técnica
 - Proveer análisis técnicos y diagnóstico de problemas
 - Coordinar con desarrolladores, control de calidad y soporte en producción para probar e implementar mejoras y soluciones.
 - Realizar implementaciones de nuevas instalaciones de clientes
- **Ingenieros de Pruebas:** Formado por 3 personas en Ecuador, sus tareas son:
 - Desarrollar casos de pruebas por proyecto asignado
 - Ejecutar las pruebas para garantizar que las aplicaciones desarrolladas se implementan con éxito
 - Reportar los errores y mejoras encontradas durante la ejecución de las pruebas para que sean resueltos por el equipo de desarrollo

E. Soporte

Es el punto único de contacto para usuarios internos y externos y es la encargada de brindar el soporte 7x24 a las soluciones que se encuentran en producción, en casos que se presenten inconvenientes durante su ejecución. Está compuesta por:

- **Jefe de Soporte:** Sus responsabilidades son:
 - Definir la estrategia del Equipo de soporte
 - Investigar y aplicar nuevas técnicas y metodologías de la gestión de la ayuda / manejo de incidentes
 - Evaluar el desempeño de los miembros del Equipo de soporte
 - Incentivar y planificar la formación constante del equipo, así como la normalización de conocimiento a través de los miembros del equipo
 - Ejecutar las actividades de monitoreo y escalamiento de incidentes
 - Mantener la Guía de procesos de Escalada (español e inglés), así como velar por el cumplimiento de los indicadores clave de rendimiento especificados
 - Comprender, conocer y cumplir con el Service-Level Agreement (SLA) con todos los clientes
 - Convertirse en una parte activa de los debates del SLA con los clientes.
 - Coordinar agilizar la entrega de los informes de conciliación (diaria y mensual)
 - Entregar Key Performance Indicator (KPIs) de rendimiento cuando sea necesario
 - Realizar los informes de incidentes e informes de análisis de causa raíz cuando un problema es presentado en producción

- Utilizar ITIL como la guía básica para los procedimientos de apoyo, así como las normas ISO de investigación y la ejecución de los procesos para la mejora del Equipo de soporte
- Trabajar activamente con el equipo de consultores y el equipo de base de datos con el fin de garantizar el tiempo de actividad en las aplicaciones
- Apoyar al departamento de ventas en cualquier país de la operación para lograr resultados positivos en las investigaciones y la ejecución de la conectividad / configuración / seguridad de cumplimiento / etc
- **Ingeniero de Soporte:** Son 6 personas en Ecuador, sus tareas son:
 - Monitorear el desempeño de las soluciones tecnológicas en producción
 - Brindar el soporte nivel 1 en caso de presentarse un incidente.
 - Escalar a nivel 2 si el incidente no puede ser resuelto de manera inmediata
 - Generar conciliaciones mensuales con los clientes
 - Ayudar a los usuarios a solucionar sus problemas y responder a las solicitudes de información en los distintos ámbitos de las TI (hardware, software, telecomunicaciones e infraestructura)
 - Ofrecer toda una serie de servicios que los usuarios pueden solicitar cuando sea necesario (instalación, traslado o desinstalación de equipos y software, distribución de derechos de acceso, archivado y restauración de datos, etc.)
 - Configurar equipos del cliente para conectarse a Internet a través del router (clientes de acceso telefónico / DSL solamente) módem / DSL
 - Obtener conocimiento general del sistema operativo y las aplicaciones que están en producción

- Ser parte de cualquier otro proyecto que el departamento de TI necesite.

F. Operaciones e Infraestructura

Esta área es la encargada del mantenimiento y actualización de la infraestructura tecnológica que posee Yellowpepper, los cuales son hardware, software y comunicaciones. A continuación, se describen los integrantes de esta área con sus respectivas funciones.

- **Jefe de Infraestructura y Operaciones**

- Liderar el área de infraestructura y Operaciones
- Asignar las tareas operativas a cada uno de sus elementos
- Garantizar la disponibilidad diaria de los sistemas y se encarga de implementar los procedimientos técnicos necesarios cuando se retoma la actividad después de un fallo del sistema

- **Administrador de Base de Datos**

- Analizar el negocio e identificar las necesidades de servicio al cliente
- Elaborar la documentación técnica de los diseños de base de datos y otros servicios pertinentes a su cargo
- Evaluar nuevas herramientas que podrían formar parte de la cartera de tecnología de la empresa, en especial para el almacenamiento de datos e inteligencia de negocios.
- Estar actualizado con las nuevas tecnologías relacionadas con las técnicas de almacenamiento, almacenamiento de datos, mantenimiento de bases de datos, monitoreo de bases de datos, copias de seguridad, etc
- Ser un soporte para consultores y equipo de operaciones
- Compartir el conocimiento con el equipo de TI

- Obtener las certificaciones necesarias para cumplir con las expectativas
- Responsable de convertirse en parte activa de mejora y ejecución de planes de acción
- Convertirse en un experto en seguridad y los aspectos de mejora para la aplicación, el usuario y el acceso operativo a base de datos
- **Administrador de Sistemas:** Sus responsabilidades son:
 - Convertirse en parte activa y un especialista de la infraestructura Yellowpepper
 - Entregar lista de materiales para los usuarios externos cuando sea necesario
 - Investigar y evaluar nuevas herramientas para supervisar los servidores, sistemas operativos, aplicaciones, etc
 - Cumplir con los requisitos de seguridad internas y externas
 - Trabajar activamente con el Gerente de Operaciones para garantizar y velar por el tiempo de actividad
 - Comprender, conocer y velar por el cumplimiento de los SLAs.
 - Diseñar, mantener, ejecutar y dirigir los procedimientos de mantenimiento del servidor.
 - Diseñar, mantener, ejecutar y dirigir las políticas de seguridad, es decir: administración de contraseñas, el uso de servidores, etc.
 - Mantener actualizado el inventario de activos
 - Mantener actualizada la creación de redes y diseño de hardware
 - Mantener actualizado el inventario de contraseña y cifrado (compartido con el Director de Tecnología)

- Instalar nuevo hardware y asegurarse de que se alcanzan los objetivos de la instalación
- Coordinar los accesos al centro de datos de Yellowpepper.
- Investigar y evaluar las mejores estrategias cuando vienen nuevos requerimientos de infraestructura a lo largo del camino.
- **Administrador de red y seguridad:** Sus responsabilidades son:
 - Mantener operativo la red en la empresa
 - Dar mantenimiento a la infraestructura de red
 - Implementar las comunicaciones seguras Virtual Private Network (VPNs) entre el cliente y Yellowpepper
 - Configurar los elementos de comunicación.
 - Implementar políticas de seguridad para evitar intrusiones o ataques
 - Configurar, mantener, monitorear los principales Firewalls y balanceadores de carga de Yellowpepper.
- **Analista de reportes:** Sus responsabilidades son:
 - Crear procedimientos (manuales / automáticos) para ofrecer estadísticas e información al Comité Ejecutivo de Yellowpepper.
 - Ser un apoyo para el Database Administrator (DBA) para análisis y ejecución de mejoras en los procedimientos internos y externos para mantener el tiempo de actividad de la infraestructura organizativa.
 - Ser apoyo para el DBA a la hora de evaluar nuevas herramientas
 - Apoyar a consultores, operaciones y equipo de soporte para el análisis de secuencias de comandos (scripts) y la ejecución de los mismos

- Recomendar enfoques para hacer frente a los problemas de rendimiento, así como estrategias de Inteligencia de Información y Negocios
- Convertirse en una parte activa en el diseño, mantenimiento y ejecución de las bases de datos.

C. Infraestructura técnica

Los servidores y equipos de comunicación de Yellowpepper se encuentran alojados en el centro de cómputo ubicado en el Network Access Point (NAP) de las Américas en Miami, Florida, USA, los cuales son administrados por el área de operaciones e infraestructura ubicada en la ciudad de Quito Ecuador. En dichos servidores se encuentran instaladas todas las aplicaciones de Yellowpepper.

D. Seguridades

En el NAP se cuenta con las siguientes seguridades:

- Seguridad física
- Seguridad personal

La seguridad física se encuentra compuesta por ciertos elementos que permiten mantener un estándar de seguridad interna, estos elementos son, correcta separación entre redes eléctricas y redes de comunicaciones mediante canaletas separadas por una distancia determinada que impide que existan interferencias en las comunicaciones. Adicionalmente encontramos correctamente distribuidos los extintores de incendios en todas las áreas del edificio. Las puertas de ingreso están compuestas de aleaciones especiales.

La seguridad personal es manejada por recurso humano, ya que para que una persona ingrese a las instalaciones debe pasar por dos filtros de seguridad, el primero efectúa una revisión minuciosa de todo lo que la persona ingresa al edificio, luego se llega a una sección en el cual se encuentra otro guardia de seguridad el mismo que se encarga de autorizar el ingreso al área de servidores,

caso contrario se podrá ingresar con escolta y sin derecho a uso de llaves. Todos los armarios tienen llave, la misma que es entregada por el guardia de seguridad.

E. Arquitectura lógica

Yellowpepper cuenta con 2 plataformas, la una llamada SMS Metropolis y la otra llamada Mobile Everywhere (ME). SMS Metropolis actúa como un enrutador, el cual re direcciona todas las solicitudes SMS a las diferentes aplicaciones para que puedan ser procesadas. Así mismo Mobile Everywhere (ME) recepta y enruta todas las solicitudes Smartphone a las diferentes aplicaciones para que puedan ser procesadas. Estas aplicaciones envían dichas solicitudes a cada institución financiera para que puedan ser procesadas.

F. Arquitectura física

En el NAP de las américas se encuentra todo el hardware y software necesitado para que los servicios de Yellowpepper puedan operar, los mismos se encuentran distribuidos en 26 servidores de la siguiente manera:

Plataforma Metropolis

Ambiente de producción:

- 6 Servidores de aplicaciones web
- 5 servidores de bases de datos

Ambiente de pruebas:

- 2 Servidores de base de datos
- 2 Servidores de aplicaciones

Plataforma ME

Ambiente de producción

- 2 servidores para base de datos
- 2 servidores para aplicación.

Ambiente de pruebas

- 1 servidor para base de datos
- 1 servidor para aplicación.

Otros

- 1 servidor para File Transfer Protocol (FTP)
- 2 servidores para active directory
- 1 servidor para la aplicación Applications and Products (SAP)
- 4 equipos de comunicación.

Los servidores usados para la plataforma ME utilizan como sistema Operativo Linux mientras que los servidores de la plataforma Metropolis tienen como sistema operativo Windows. Ambas plataformas usan Structured Query Language (SQL) como base de datos. En el Anexo 3 se muestra el detalle de cada servidor. La seguridad y acceso lógico a la red de Yellowpepper es controlada a través de un firewall. Todos los clientes de Yellowpepper se conectan a dicho firewall a través de canales seguros como son las VPNs. En la Figura 3, muestra el diagrama de redes y servidores de Yellowpepper.

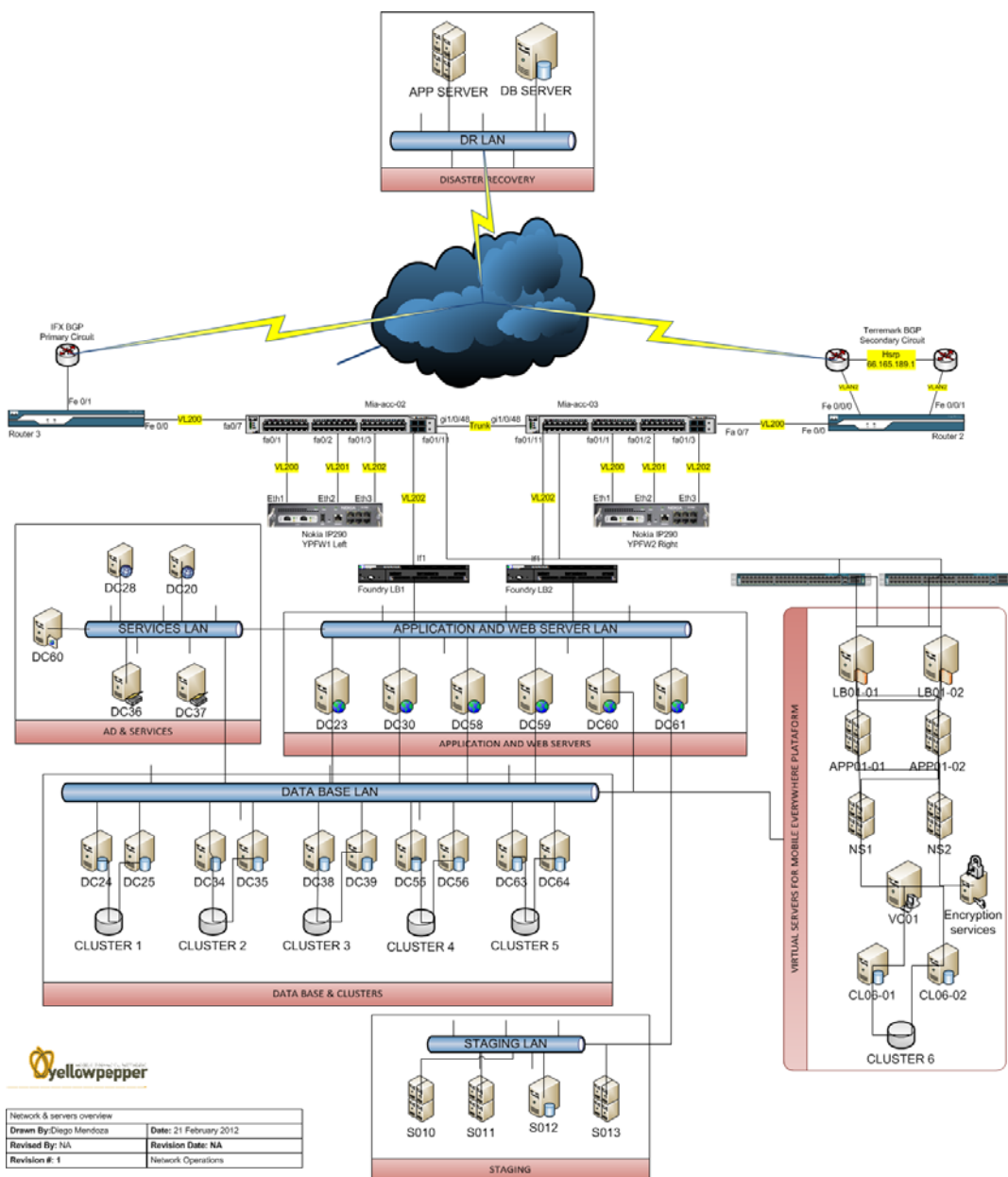


Figura 3 Diagrama de redes y servidores de Yellowpepper

Fuente: (Yellowpepper)

G. Aplicaciones

Yellowpepper cuenta con 2 tipos de aplicaciones:

- Aplicaciones internas
- Aplicaciones externas

Las aplicaciones internas son las usadas por Yellowpepper, entre las principales tenemos:

- Aplicación SAP
- Aplicación de Monitoreo
- Microsoft Reporting Services
- Nagios EventLog Agent
- LiveVault Backup

Las aplicaciones externas son las que Yellowpepper desarrolla para sus clientes y son usadas por ellos. Estas son 86 aplicaciones. En el Anexo 2 se detallan estas aplicaciones en donde # de usuarios representa el número de usuarios que usa dicha aplicación, #Transacciones/Mes representa el número de transacciones que transacciona dicha aplicación en un mes y servidor instalado representa en que servidor se encuentra instalada dicha aplicación.

CAPITULO 3

ANÁLISIS DE IMPACTO

El propósito del análisis de impacto en el negocio (BIA) es identificar qué áreas y procesos del negocio son esenciales para la supervivencia de Yellowpepper. El BIA identificará la rapidez con la que las áreas/procesos críticos dentro del departamento de tecnología tienen que regresar a la normalidad después de una situación de desastre.

3.1 Política

Se aplicará el BIA en los procesos del negocio para determinar la criticidad de cada uno de los procesos en Yellowpepper y determinar cuales es el impacto que representa para la organización si uno de ellos fuese interrumpido. Se identificará el tiempo que pasará una infraestructura antes de estar disponible (RTO) y cuanto la organización está dispuesta a perder en cantidad de datos (RPO) y los procesos claves del negocio.

3.2 Alcance

El BIA estará enfocado a los elementos del departamento de tecnología que soportan los procesos críticos de Yellowpepper. Tener en cuenta que el BIA no abordara las soluciones de recuperación.

3.3 Suposiciones

El BIA será desarrollado pensando en el peor de los escenarios, para lo cual se tomarán como base las siguientes suposiciones:

- No se podrá acceder al centro de datos por el lapso de 1 hora
- La infraestructura física que soporta cada proceso, ha sido destruida junto con todos los registros y equipamiento
- La interrupción ocurre en horas pico
- Durante la interrupción, el personal clave no se encuentra disponible
- No se cuenta con la logística necesaria durante la interrupción

3.4 Identificaciones de funciones y procesos

Para la identificación de funciones y procesos de negocio de Yellowpepper se ha tomado como base Yellowpepper Ecuador. Tener presente que el departamento de tecnología da soporte a toda la organización. A continuación, se detallarán las funciones y procesos de Yellowpepper, tomando como premisa que:


- **Funciones:** Departamentos o áreas que conforman la organización. Ejemplo: Soporte, Contabilidad, Comercial, etc.
- **Procesos:** Actividades que son realizadas en cada departamento. Ejemplo, atención a clientes en soporte, facturación en contabilidad.

Tabla 1

Funciones y procesos de Yellowpepper

FUNCIÓN	PROCESO
Comercial	Analizar mercado en busca de clientes
	Contactar clientes identificados
	Presentación de las líneas de Productos a los Clientes
	Negociación de servicios nuevos o existentes
	Establecimiento de las reglas del negocio
	Busqueda de potenciales clients
	Ofrecer y vender los productos y servicios
Contabilidad	Manejo Recursos Humanos
	Manejo Asientos Contables

Continúa 

	Adminstración Tributaria
	Inventario
	Facturación
	Cuentas por cobrar
	Cuentas por pagar
	Clientes
Financiero	Coordinar las tareas de Presupuesto
	Asesoramiento a la Alta Dirección en temas contables
	Mantener control sobre los registros de Activos/Pasivos/Ingresos/Egresos
	Garantizar la preparación de los Estados Financieros
	Ejecutar conciliaciones Bancarias
	Realizar informes del estado de los recursos de la empresa
Operaciones	Administración de servidores y equipos de comunicación
	Mantenimiento de Hardware
	Mantenimiento de Software
	Administración de base de datos
	Mantenimiento de comunicaciones
	Obtención de Backups
	Adquisición de equipos
	Mantenimiento de aplicaciones
Soporte	Soporte a usuarios 7x24
	Monitoreo de las aplicaciones
	Mantenimiento de las computadoras de la oficina
	Manejo de Incidentes y recuperación del servicio
	Cumplimientos de los Acuerdos de Niveles de Servicio
Consultores	Definición y Diseño de Soluciones Tecnológicas de los Clientes
	Seguimiento y Evaluación de las Aplicaciones Desarrolladas
	Elaboración de la Documentación Técnica de las Soluciones
	Asesoramiento a las áreas comerciales sobre las soluciones tecnológicas
	Apoyo al área de soporte en la solución de incidentes
Control de Calidad	Diseño de las matrices de pruebas
	Crear matrices de pruebas sobre las soluciones tecnológicas 

Reportar errores y mejoras al Equipo de Desarrollo
Mantenimiento de reportes, registros de pruebas de las soluciones certificadas

Fuente: (Yellowpepper)

3.5 Evaluación del Impacto Financiero

En esta etapa se evaluará el impacto financiero tomando como base las suposiciones indicadas anteriormente. En la tabla 2 se definen los rangos utilizados en pérdidas por día de ganancias.

Tabla 2

Escala para medir el impacto financiero

Impacto	Nivel	Rango de perdida financiera (diaria)
0	Normal	No hay pérdidas, 0 días
1	Baja	Entre 0.01 a 100.00
2	Medio	Entre \$100.01 a \$1000.00
3	Alto	Entre \$1000.01 a \$3538.00


Fuente: (Yellowpepper)

En la tabla 3 se muestra el análisis realizado.

Tabla 3

Evaluación del impacto financiero

FUNCIÓN	PROCESO	Impacto Financiero
Comercial	Analizar mercado en busca de clientes	0
	Contactar clientes identificados	0
	Presentación de las líneas de Productos a los Clientes	0
	Negociación de servicios nuevos o existentes	1
	Establecimiento de las reglas del negocio	0 Continua ➔

	Busqueda de Potenciales Clientes	0	
	Ofrecer y vender los productos y servicios	0	
Contabilidad	Manejo Recursos Humanos	0	
	Manejo Asientos Contables	2	
	Adminstración Tributaria	0	
	Inventario	1	
	Facturación	3	
	Cuentas por cobrar	3	
	Cuentas por pagar	3	
	Clientes	1	
	Operaciones	Administración de servidores y equipos de comunicación	3
Mantenimiento de Hardware		2	
Mantenimiento de Software		2	
Administración de base de datos		2	
Mantenimiento de comunicaciones		3	
Obtención de Backups		2	
Adquisición de equipos		2	
Mantenimiento de aplicaciones		2	
Soporte	Soporte a usuarios 7x24	3	
	Monitoreo de las aplicaciones	2	
	Mantenimiento de las computadoras de la oficina	1	
	Manejo de Incidentes y recuperación del servicio	3	
	Cumplimientos de los Acuerdos de Niveles de Servicio	3	
Consultores	Definición y Diseño de Soluciones Tecnológicas de los Clientes	0	
	Seguimiento y Evaluación de las Aplicaciones Desarrolladas	2	
	Elaboración de la Documentación Técnica de las Soluciones	0	
	Asesoramiento a las áreas comerciales sobre las soluciones tecnológicas	1	
	Apoyo al área de soporte en la solución de incidentes	2	
Control de Calidad	Diseño de las matrices de pruebas	0	Continúa 

Crear matrices de pruebas sobre las soluciones tecnológicas	0
Reportar issues al Equipo de Desarrollo	1
Mantenimiento de reportes, registros de pruebas de las soluciones certificadas	1

3.5 Evaluación del Impacto Operacional

Para el impacto operacional se han tomado en cuenta las siguientes categorías:

Tabla 4

Categorías para evaluación del impacto operacional

CATEGORIA	IDENTIFICACIÓN	DESCRIPCIÓN
Imagen/Credibilidad	I	Imagen del servicio de Yellowpepper
Financiero	F	Flujo de caja de Yellowpepper
Operacional	O	Operativa de Yellowpepper

Además, es medido en base a la tabla 5.

Tabla 5

Niveles de Impacto operacional

Categoría	Identificación	Descripción
Imagen/Credibilidad	I	Imagen del servicio de Yellowpepper
Financiero	F	Flujo de caja de Yellowpepper
Operacional	O	Operativa de Yellowpepper

En la tabla 6, se ilustran los resultados del impacto operacional.

Tabla 6
Impacto operacional

FUNCIÓN	PROCESO	Categoría del Impacto		
		I	F	O
Comercial	Analizar mercado en busca de clientes	0	0	0
	Contactar clientes identificados	0	1	0
	Presentación de las líneas de Productos a los Clientes	0	1	0
	Negociación de servicios nuevos o existentes	0	2	0
	Establecimiento de las reglas del negocio	0	0	0
	Busqueda de Potenciales Clientes	0	1	0
	Ofrecer y vender los productos y servicios	0	1	0
Contabilidad	Manejo Recursos Humanos	0	0	0
	Manejo Asientos Contables	0	2	0
	Administración Tributaria	2	2	0
	Inventario	0	1	1
	Facturación	1	3	2
	Cuentas por cobrar	1	3	1
	Cuentas por pagar	1	3	1
Financiero	Coordinar las tareas de Presupuesto	0	0	0
	Asesoramiento a la Alta Dirección en temas contables	0	0	0
	Mantener control sobre los registros de Activos/Pasivos/Ingresos/Egresos	0	0	0
	Garantizar la preparación de los Estados Financieros	0	0	0
	Operaciones	Administración de servidores y equipos de comunicación	0	3
Mantenimiento de Hardware		2	3	3
Mantenimiento de Software		2	3	3
Administración de base de datos		2	3	3

Continúa 

	Mantenimiento de comunicaciones	2	3	2
	Obtención de Backups	1	3	3
	Adquisición de equipos	0	0	1
	Mantenimiento de aplicaciones	3	3	3
Soporte	Soporte a usuarios 7x24	3	0	2
	Monitoreo de las aplicaciones	1	0	2
	Mantenimiento de las computadoras de la oficina	0	0	2
	Manejo de Incidentes y recuperación del servicio	2	0	0
	Cumplimientos de los Acuerdos de Niveles de Servicio	2	0	0
Consultores	Definición y Diseño de Soluciones Tecnológicas de los Clientes	0	0	0
	Seguimiento y Evaluación de las Aplicaciones Desarrolladas	0	0	0
	Elaboración de la Documentación Técnica de las Soluciones	0	0	0
	Asesoramiento a las áreas comerciales sobre las soluciones tecnológicas	0	0	0
	Apoyo al área de soporte en la solución de incidentes	1	2	3
Control de Calidad	Diseño de las matrices de pruebas	0	0	0
	Crear matrices de pruebas sobre las soluciones tecnológicas	0	0	0
	Reportar issues al Equipo de Desarrollo	0	0	0
	Mantenimiento de reportes, registros de pruebas de las soluciones certificadas	0	0	0

3.6 Identificación de Procesos Críticos del Negocio

La identificación de los procesos críticos del negocio se la ha realizado analizando el impacto operacional y financiero realizado, tomando como base las siguientes premisas:

- Un proceso es crítico si el impacto financiero tiene un valor 2 o 3.

- Un proceso es crítico si el impacto operacional tiene al menos dos valores “Altos”
- Un proceso es crítico si el impacto operacional tiene un valor Alto y un Medio.

En la tabla 7 se muestran los resultados.

Tabla 7

Procesos críticos del negocio

FUNCIÓN	PROCESOS CRITICOS	Impacto Financiero	Categoría del Impacto			Total Puntos
			I	F	O	
Contabilidad	Facturación	3	1	3	2	9
	Cuentas por cobrar	3	1	3	1	8
	Cuentas por pagar	3	1	3	1	8
Operaciones	Administración de servidores y equipos de comunicación	3	0	3	3	9
	Mantenimiento de Hardware	2	2	3	3	10
	Mantenimiento de Software	2	2	3	3	10
	Administración de base de datos	2	2	3	3	10
	Mantenimiento de comunicaciones	3	2	3	2	10
	Obtención de Backups	2	1	3	3	9
	Mantenimiento de aplicaciones	3	3	3	3	12
Soporte	Soporte a usuarios 7x24	3	3	0	2	8
Consultores	Apoyo al área de soporte en la solución de incidentes	2	1	2	3	8

3.8 Identificación del MTD

El MTD indica el tiempo máximo que un proceso del negocio puede estar no operacional. La estimación del MTD está basada en el valor total de puntos

obtenidos por proceso crítico. La escala de tiempos que se usa para dar valores del MTD a cada proceso del negocio es la siguiente:

Tabla 8

Procesos críticos del negocio

Escala	Descripción
A	De 1 a 2 horas
B	De 3 a 4 horas
C	De 5 a 6 horas
D	De 6 horas a 48 horas
E	De 49 horas a 72 horas
F	De 73 horas en adelante

A continuación, la escala de equivalencias para definición de MTD:

Tabla 9

Escala de equivalencia para definición de MTD

Total de puntos Financiero + Operacional	MTD
12	A
10	B
9	C
8	D
7	E
5	F

Los valores de MTD de cada proceso crítico se describen en la tabla 10.

Tabla 10**Definición del MTD**

FUNCIÓN	PROCESO	MTD
Contabilidad	Facturación	E
	Cuentas por cobrar	D
	Cuentas por pagar	D
Operaciones	Administración de servidores y equipos de comunicación	C
	Mantenimiento de Hardware	B
	Mantenimiento de Software	B
	Administración de base de datos	B
	Mantenimiento de comunicaciones	B
	Obtención de Backups	C
	Mantenimiento de aplicaciones	A
Soporte	Soporte a usuarios 7x24	D
Consultores	Apoyo al área de soporte en la solución de incidentes	D

3.9 Determinación del RTO y WRT

El RTO indica el tiempo disponible para recuperar sistemas y/o recursos que han sufrido una alteración. Y WRT es el tiempo disponible para recuperar los datos perdidos una vez que los sistemas están reparados dentro del MTD. (Alexander, 2007).

Tabla 11**Determinación de RTO y WRT**

FUNCIÓN	PROCESO	APLICACIONES CRITICAS DEL SISTEMA DE TI	RTO (horas)	WRT (horas)
Contabilidad	Facturación	Aplicación SAP	2	4
	Cuentas por cobrar	Aplicación SAP	2	4 Continua

	Cuentas por pagar	Aplicación SAP	2	4
Operaciones	Administración de servidores y equipos de comunicación	Window server	1	1
		Remote Desktop connection.	1	1
	Mantenimiento de Aplicaciones	Aplicaciones Smartphones	1	1
		SMS Metropolis	1	1
		Aplicaciones SMS	1	1
		Billeteras Móviles	1	1
		Remote Desktop connection.	1	1
		Procesadores	1	1
		Aplicación de envíos	1	1
		Aplicación de monitoreo	1	1
	Administración de base de datos	SQL Server	1	1
		Remote Desktop connection.	1	2
	Mantenimiento de comunicaciones	Check point	1	2
	Obtención de Backups	SQL Server	1	2
Mantenimiento de software	Remote Desktop connection.	1	1	
Mantenimiento de hardware	Remote Desktop connection.	1	1	
Soporte	Soporte a usuarios 7x24	Jira	1	2
Consultores	Apoyo al área de soporte en la solución de incidentes	Jira	1	2
		Remote Desktop connection.	1	1

3.10 Análisis del daño que causa la interrupción de un proceso

Es importante determinar las consecuencias de la interrupción de un sistema, recurso o servicio soportado por el departamento de TI con el fin de conocer el

posible impacto que tendría el negocio en caso de la paralización de operaciones.

Tabla 12

Consecuencias de la interrupción de los servicios

Servicio de TI	Consecuencia
Aplicación SAP	Si se interrumpe el sistema SAP, se detiene la facturación, cuentas por cobrar, cuentas por pagar y administración de clientes. SAP es el ERP de la empresa, formando parte del core del negocio
Window server	El mal funcionamiento de Windows Server en los servidores provoca que los servicio que forman parte del core de la empresa dejen de funcionar.
Remote Desktop connection.	El mal funcionamiento de Remote Desktop connection provoca que el equipo de operaciones no pueda acceder a los servidores.
Aplicaciones Smartphones	La interrupción de las aplicaciones Smartphone provoca que los clientes de Yellowpepper no puedan utilizar las aplicaciones BlackBerry, iPhone y Android.
SMS Metropolis	La interrupción de la plataforma SMS Metropolis provoca que las aplicaciones SMS no puedan procesar las transacciones generadas por los clientes ni los clientes podrán recibir notificaciones vía SMS.
Aplicaciones SMS	La interrupción de las aplicaciones SMS provoca que los clientes de Yellowpepper no puedan transaccionar a través del canal de SMS
Billeteras Móviles	La interrupción de las billeteras móviles provoca que los clientes no puedan realizar transacciones.
Procesadores de recargas	La interrupción de los procesadores de recarga provoca que los clientes no puedan comprar tiempo aire.

Continúa 

Aplicación de envíos	La interrupción de la aplicación de envíos provoca que nuestros clientes no puedan enviar notificaciones a los usuarios finales
Aplicación Billing	La interrupción de la aplicación Billings no permite generar facturas al cliente final.
SQL Server	La interrupción de SQL Server provoca que los usuarios no puedan generar ninguna transacción.
Check point	La interrupción de Check Point provoca que no se puedan administrar las VPN que actualmente mantenemos con nuestros clientes ni la configuración de nuevas. Además, los servidores no podrán ser accedidos por el equipo de operaciones.
Jira	La interrupción de Jira provoca que no se puedan manejar los incidentes.

3.11 Conclusiones

El análisis de impacto del negocio en Yellowpepper realizado permitió concluir:

- Las áreas críticas del negocio son:
 - Soporte
 - Operaciones
 - Contabilidad
 - Consultores
- Los procesos críticos de Yellowpepper son:

FUNCIÓN	PROCESO
Contabilidad	Facturación
	Cuentas por cobrar
	Cuentas por pagar
Operaciones	Administración de servidores y equipos de comunicación
	Mantenimiento de Hardware
	Mantenimiento de Software
	Administración de base de datos
	Mantenimiento de comunicaciones

Continúa 

	Obtención de Backups
	Mantenimiento de aplicaciones
Soporte	Soporte a usuarios 7x24
Consultores	Apoyo al área de soporte en la solución de incidentes

- Los tiempos máximos tolerables de interrupción (MTD) que pueden enfrentar los procesos críticos de Yellowpepper son:

FUNCIÓN	PROCESO	MTD
Contabilidad	Facturación	49-72 horas
	Cuentas por cobrar	6-48 horas
	Cuentas por pagar	6-48 horas
Operaciones	Administración de servidores y equipos de comunicación	5 -6 horas
	Mantenimiento de Hardware	3-4 horas
	Mantenimiento de Software	3-4 horas
	Administración de base de datos	3-4 horas
	Mantenimiento de comunicaciones	3-4 horas
	Obtención de Backups	5 -6 horas
	Mantenimiento de aplicaciones	1-2 horas
Soporte	Soporte a usuarios 7x24	6-48 horas
Consultores	Apoyo al área de soporte en la solución de incidentes	6-48 horas

CAPITULO 4

ANÁLISIS DE RIESGOS

Los elementos que soportan los procesos críticos de Yellowpepper se encuentran en el departamento de tecnología. Es importante mencionar que una interrupción en el área de tecnología afectaría considerablemente a toda la empresa, ocasionando pérdidas. El análisis de riesgos evaluará a estos elementos que soportan a los procesos críticos de Yellowpepper y los diversos riesgos tanto internos como externos que pueden les pueda afectar.

4.1 Identificación de Riesgos

En la tabla 13 se presentan los potenciales riesgos que podrían afectar a los procesos críticos de Yellowpepper, estos incluyen los riesgos que están y los que no están bajo el control de Yellowpepper.

Tabla 13

Identificación de riesgos

#	Tipo de Riesgo	Riesgo	Descripción	Posibles consecuencias
1	Externo	Inundaciones	Ingreso de agua en el centro de datos	Daño total de los servidores o equipos de comunicación provocando la caída de los servicios de Yellowpepper.
2	Externo	Terremotos	Terremotos en la ciudad donde se encuentra el centro de datos	Daño total de los servidores o equipos de comunicación provocando la caída de los servicios de Yellowpepper



3	Externo	Tormentas eléctricas	Tormentas eléctricas donde se encuentra el centro de datos	Daño total de los servidores o equipos de comunicación provocando la caída de los servicios de Yellowpepper
4	Externo	Huracanes	Huracanes en el centro de datos	Daño total de los servidores o equipos de comunicación provocando la caída de los servicios de Yellowpepper
5	Externo	Incendios	Fuego en el centro de datos.	Daño total de los servidores o equipos de comunicación provocando la caída de los servicios de Yellowpepper
6	Externo	Explosiones	Explosiones en el centro de datos	Daño total de los servidores o equipos de comunicación provocando la caída de los servicios de Yellowpepper
7	Interno-Externo	Destrucción intencional de datos	Falta de las respectivas seguridades físicas en el centro de datos	Daño total de los servidores, aplicaciones o equipos de comunicación provocando la caída de los servicios de Yellowpepper
8	Interno-Externo	Sabotage	Daño intencional provocado por una persona interna o externa	Daño total o parcial de los servidores, aplicaciones o equipos de comunicación provocando la caída de los servicios de Yellowpepper
9	Interno-Externo	Robo de equipos.	Robo de hardware.	Mal funcionamiento de los servidores, aplicaciones o equipos de comunicación provocando la caída de los servicios de Yellowpepper
10	Interno	Persona NO capacitada	Daño no intencional de los servicios de YP.	Mal funcionamiento de las aplicaciones provocando la caída de los servicios de Yellowpepper



11	Interno- Externo	Falla de Firewall	Servidores susceptible ataques.	La infraestructura mal configurada y sin parchear puede pasar desapercibida, dejándolo susceptible a los ataques de virus, software malicioso y ataques de Internet.
12	Interno	Falla de los equipos de ventilación en el Data center.	Falla de los equipos de ventilación en el Data center.	Daño total o parcial de los servidores y equipos de comunicación provocando el mal funcionamiento de los servicios de Yellowpepper.
13	Interno- Externo	Corte de energía	Cortes de energía en centro de datos	Falla eléctrica provocando la inoperatividad de los equipos de comunicación y servidores de Yellowpepper.
14	Interno	Saturación de los servidores	Ausencia de monitoreo en línea de capacidad y rendimiento de los servidores	La sobrecarga de tráfico-información provoca el mal funcionamiento de los servicios de Yellowpepper.
15	Externo	Falla del servicio de internet	Falla del servicio de internet en el centro de datos	Provoca la caída de los servicios de Yellowpepper.
16	Interno	Ausencia de procesos formalizados para gestión de cambios en producción	Falta de procesos formalizados de Gestión de cambios en aplicaciones e infraestructura en producción no siguen siempre un proceso estructurado de	Sin un proceso formalizado de gestión de cambios, la disponibilidad e integridad de las aplicaciones puede verse en peligro como resultado de pruebas inadecuadas, evaluación de riesgos, y la falta de comunicación a las partes afectadas.



				evaluación de riesgos, las pruebas pre / post implementación y aprobación formal.
17	Información	Perdida de información confidencial	de	Perdida de información para los procesos críticos del negocio.
				de
				Perdida de información
				de información
				para puede provocar pérdidas para la empresa y el mal funcionamiento de los servicios de la empresa.

4.2 Análisis de Riesgos

Una vez identificados los riesgos, el siguiente paso es analizar los mismos, para lo cual se calculará la magnitud de cada riesgo. La magnitud de un riesgo es obtenida a través de la probabilidad de ocurrencia por el impacto que puede causar dicho riesgo, teniendo la siguiente formula:

$$\text{Magnitud} = \text{Probabilidad} \times \text{Impacto}$$

Donde la probabilidad es la frecuencia que podría presentar el riesgo y el impacto es la forma en la cual el riesgo podría afectar los resultados del proceso. Las escalas que se usarán para obtener la probabilidad como el impacto son:

Probabilidad	Descripción
Alto	Es muy factible que el riesgo se presente
Media	Es factible que el riesgo se presente
Baja	Es muy poco factible que el riesgo se presente

Impacto	Descripción
Alto	Afecta en alto grado la disponibilidad del servicio
Medio	Afecta en grado medio la disponibilidad del servicio
Baja	Afecta en grado bajo la disponibilidad del servicio

La Matriz de Priorización es presentada en la Figura 4, con la cual se clasificarán los riesgos de acuerdo a su Magnitud, donde:

Magnitud A: Nivel Alto de riesgo

Magnitud B: Nivel Medio de riesgo

Magnitud C: Nivel Bajo de riesgo

Probabilidad	ALTA	B	A	A
	MEDIA	B	B	A
	BAJA	C	B	B
		BAJO	MEDIA	ALTO
		Impacto		

Figura 4 Matriz de priorización

Fuente: (Universidad Tecnológica de Pereira, 2010)

En la tabla 14 se presenta información sobre la magnitud de los riesgos analizados, la cual será de suma importancia para la etapa de evaluación, en donde serán priorizados o clasificados según los criterios definidos.

Tabla 14
Análisis de Riesgo

#	Tipo- Riesgo	Riesgo	Control existente	Probabilidad	Impacto	Magnitud
1	Externo	Inundaciones	Los servidores están instalados en un rack sobre un piso elevado.	Baja	Alto	B
2	Externo	Terremotos	-	Baja	Alto	B
3	Externo	Tormentas eléctricas	Inclinación del techo diseñada para ayudar a canalizar el exceso de agua de una tormenta con una intensidad que sólo se vería cada 100 años, asistida por 18 desagües en la azotea.	Baja	Medio	B
4	Externo	Huracanes	EL NAP de las Américas está diseñado para soportar un huracán de categoría 5 con aproximadamente 9 mil toneladas de lastre de hormigón. Paneles exteriores de hormigón reforzados con acero de 18 cm de grosor.	Media	Alto	A
5	Externo	Incendios	Extintores y alarmas de incendios. Seguro contra incendios	Baja	Alto	B

Continúa 

			Se cuenta con material aislante dentro del centro de datos.			
6	Externo	Explosiones	Extintores y alarmas de incendios. Se cuenta con material aislante dentro del centro de datos.	Baja	Alto	B
7	Interno- Externo	Destrucción intencional de datos	Respaldos diarios de las bases de datos	Media	Alto	A
8	Interno- Externo	Sabotaje	Seguridad durante las 24 horas del día, todos los días del año. El personal de seguridad supervisa todas las cámaras de seguridad, vigila los puntos de acceso de entrada y salida del edificio y controla el acceso con llave electrónica a ascensores, pisos y áreas del techo.	Media	Alto	A
9	Interno- Externo	Robo de equipos.	Seguridad durante las 24 horas del día, todos los días del año. El personal de seguridad supervisa todas las cámaras de seguridad, vigila los puntos de acceso de entrada y salida del edificio y controla el acceso con llave electrónica a	Baja	Alto	B

Continúa


				ascensores, pisos y áreas del techo.			
10	Interno	Persona NO capacitada	Sin control		Media	Alto	A
11	Interno	Falla firewall	Diariamente se realizan respaldos de las Base de datos		Media	Alto	A
12	Interno	Falla de los equipos de ventilación en el Data center.	Mantenimientos mensuales.		Baja	Baja	C
13	Interno-Externo	Corte de energía	Se cuenta con una planta de energía Alterna		Baja	Alto	B
14	Interno	Saturación de los servidores	Se dispone de un load balancer que distribuye la carga entre los servidores.		Media	Alto	A
15	Externo	Falla del servicio de internet	Se disponen de enlaces de Backup		Baja	Alto	B
16	Interno	Perdida de información confidencial	Sin control		Media	Alto	A

4.3 Evaluación de Riesgos

El objetivo de la evaluación de riesgos es tomar decisiones basadas en los resultados del análisis de riesgos, identificar cuáles deben ser tratados y la prioridad para su tratamiento. Como base usaremos la tabla mostrada en la Figura 5 para establecer criterios de evaluación de cada riesgo:

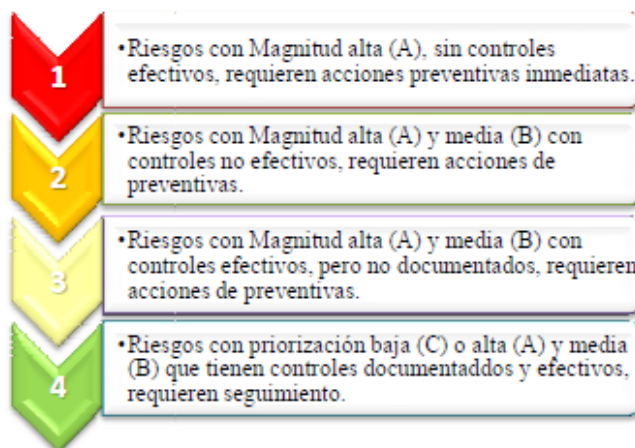


Figura 5 Criterios de evaluación de riesgo

Fuente:

(http://www.utp.edu.co/php/controlInterno/docsFTP/ADMINISTRACION_DE_RIESGOS172.ppt)

En la tabla 15 se muestra los resultados luego de la evaluación de cada riesgo, en la cual se establece la prioridad de cada riesgo y la determinación del tratamiento:

Tabla 15

Evaluación del riesgo

#	Riesgo	Criterio	Tratar riesgo
1	Inundaciones	4	NO
2	Terremotos	2	SI
3	Tormentas eléctricas	4	NO
4	Huracanes	2	SI
5	Incendios	4	NO
6	Explosiones	4	NO
7	Destrucción intencional de datos	1	SI
8	Sabotage	2	SI
9	Robo de equipos	4	NO
10	Persona NO capacitada	1	SI
11	Falla firewall	1	SI Continua →

12	Falla de los equipos de ventilación en el Data center.	4	NO
13	Corte de energía	4	NO
14	Saturación de los servidores	2	SI
15	Falla del servicio de internet	4	NO
16	Perdida de información confidencial	1	SI

4.4 Tratamiento de Riesgos

El tratamiento del riesgo implica la identificación de opciones para el tratamiento de los riesgos, la evaluación de estas opciones, la preparación los planes de tratamiento y la ejecución de los mismos. (AS/NZS, 2004).

Las opciones hacen referencia a como se pretende afrontar el riesgo disponiendo de las siguientes alternativas:

Tabla 16

Alternativas de manejo de negocio

Control del riesgo	Descripción
Reducir Probabilidad	Bajar la cantidad de veces que se presenta el riesgo en un periodo de tiempo
Reducir Impacto	Mitigar las consecuencias negativas cuando se presenta el riesgo.
Transferir el riesgo	Traspasar el riesgo a otra compañía (contrato de outsourcing, póliza de seguro)
Compartir el riesgo	Consiste en intentar extender el riesgo de un área en concreto, a diferentes secciones, con el fin de impedir la perdida de todo negocio
Evitar el riesgo	Si prestar un servicio supone un gran riesgo, el servicio se deja de entregar

Fuente: (AS/NZS 4360 Risk management, 2004).

En esta sección se identificarán y recomendarán las alternativas para modificar el riesgo mas no se implementarán, quedará a criterio de Yellowpepper la implementación de los mismos.

RIESGOS:

- Terremoto
- Huracanes

Observaciones:

Hace algunos meses atrás, Yellowpepper estuvo trabajando en la implementación de un plan de recuperación ante desastres, los equipos se adquirieron y configuraron, sin embargo, las pruebas realizadas no fueron exitosas. Debido a otros proyectos, este proyecto quedó inconcluso.

Recomendaciones:

Retomar el proyecto de plan de recuperación ante desastres para reducir el impacto ante un desastre natural.

RIESGOS:

- Destrucción intencional de datos,
- Perdida de información confidencial
- Sabotage

Observaciones:

- No existe un proceso formal de terminación de contrato de un empleado en donde se realice la eliminación del acceso físico y lógico a los sistemas de Yellowpepper. A menos que el acceso se retire inmediatamente después de la salida, los ex empleados pueden continuar accediendo a los datos de la empresa.
- Actualmente los consultores, el equipo de operaciones, gerente de soporte y operaciones tienen acceso a las bases de datos de la empresa.

Recomendaciones:

- Contar con un proceso de terminación de contrato del empleado en donde todos sus accesos sean deshabilitados para reducir la probabilidad de los riesgos.
- Limitar el acceso a las bases de datos así para reducir la probabilidad de los riesgos.

RIESGO: Persona no capacitada.

Observaciones:

Se observó que no existen procesos formales para realizar cambio en el ambiente de producción. Toda el área de tecnología tiene acceso al mismo y puede realizar cambios sin previo aviso.

Recomendaciones:

- Implementar procesos formalizados para gestión de cambios en producción para reducir la probabilidad del riesgo.
- Limitar el acceso al ambiente de producción para reducir la probabilidad del riesgo.

RIESGO: Falla firewall

Observaciones:

Yellowpepper cuenta con un firewall para evitar la exposición a terceros de información confidencial y controlar los accesos externos no autorizados a la red interna de la empresa a través del enlace de internet. No se realizan análisis de vulnerabilidad al firewall.

Recomendaciones:

- Realizar análisis de vulnerabilidad una vez por año para reducir la probabilidad del riesgo.
- Contar con un firewall más e implementar redundancia entre ellos para reducir la probabilidad del riesgo.

4.5 Conclusiones y recomendaciones

A. Conclusiones

- Luego de realizar el análisis de riesgo se concluyó que el centro de datos de Yellowpepper cuenta con las seguridades físicas necesarias para ser frente ante riegos que podrían paralizar las actividades de la empresa, sin embargo, existen algunas debilidades en la seguridad lógica, para lo cual se emitieron recomendaciones para su mejora.
- Yellowpepper cuenta con profesionales capacitados y especializados para hacer frente ante eventos inesperados.
- El estándar Australiano / Neozelandés AS/NZS 4360:2004 permitió tener una mayor comprensión de los riesgos en los procesos administrativos en general.

B. Recomendaciones

- Retomar el proyecto de Disaster Recovery que Yellowpepper inició pero que no pudo ser concluido debido a otras prioridades.
- Realizar análisis de vulnerabilidad al menos una vez por año en los servidores de Yellowpepper.
- Contar con un firewall más en el centro de datos e implementar redundancia entre ellos para permitir la confidencialidad e integridad la información.
- Implementar procesos formalizados para gestión de cambios en producción lo que permitirá reducir la probabilidad del riesgo.
- Limitar el acceso de usuarios al ambiente de producción.

CAPITULO 5

5.1 Criterios para declaración de desastre

Es importante identificar condiciones que califiquen para la declaración de desastre, estas proveerán una guía de lineamientos para la toma de decisiones de cuando se debe activar el plan de continuidad que conlleva a la activación del centro de datos alterno, por lo cual se han establecido algunos criterios los cuales se presentan en la tabla 17.

Tabla 17

Criterios para declaración de desastres

Pérdida de personas clave	
Administradores y gerentes	Todos
Expertos en cuestiones operativas	Equipo de operaciones, completo
Número de fatalidades	1 o más
Número de lesiones graves	5 o más
Personal no disponible debido a circunstancias personales: (familia afectada, casa perdida, etc.)	10 o más
Pérdida de tecnología clave	
Internet, teléfono y medio de comunicación	Internet
Archivos y bases de datos	25%
Infraestructura y cableado	45%
Virus, denegación de servicio	60%
Pérdida de uso del centro de datos	
Porcentaje de pérdida del centro de datos	45%
Días inhabilitados para uso del centro de datos	12 horas o más
Pérdida de servicios de terceros (Energía, internet, etc.)	Cualquiera
Contaminación	Si es grave
Incapacidad de ingreso al centro de datos (Daño en calles, inundaciones, huracanes, etc.)	Si la condición es grave

5.2 Plan de comunicación

El plan de comunicación de la unidad sigue básicamente el proceso que se indica en la Figura 6.

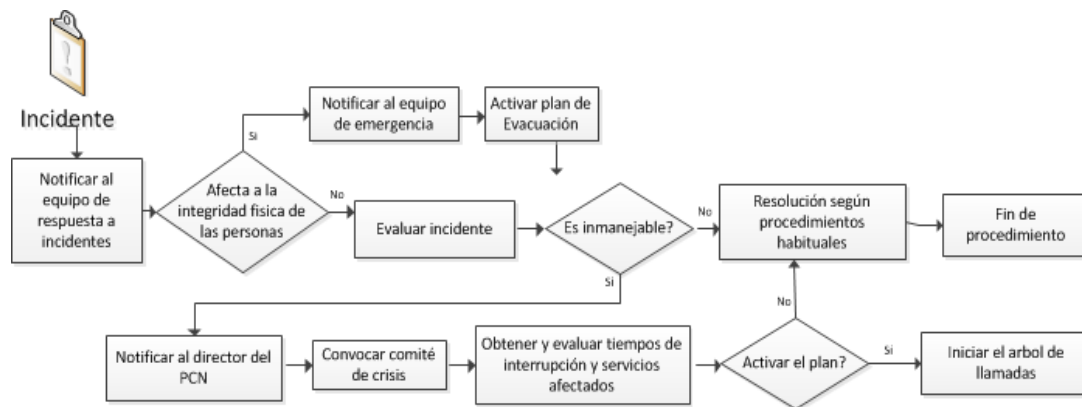


Figura 6 Plan de crisis

Las situaciones inmanejables deben ser comunicadas de inmediato al CEO de la compañía. Estas situaciones son:

- Cualquier fatalidad relacionada con el negocio
- Una empresa o negocio no relacionado amenaza la salud o puede afectar el funcionamiento de la empresa a través de la ausencia significativa o la distracción mental de trabajo (también conocido como un "evento de pandemia")
- Ley de terrorismo o intento de acto terrorista
- El secuestro o intento de secuestro de un empleado
- Bombardeos, secuestros, asesinatos que ocurran en las zonas donde opera compañía o sus empleados
- Actos reales o intentos de espionaje comprobados
- Potencial interrupciones en el negocio debido a la pérdida de instalaciones, empleados, proveedores clave, y / o de TI

- Informe nacional de medios o la investigación generada por un incidente que afecta a la compañía
- Revolución, guerra, conflicto armado o de policía, acciones en lugares donde la compañía opera
- Amenaza inminente o real de un desastre natural en o cerca de un lugar donde opera la compañía (incendios, terremotos, inundaciones, tormentas severas, tornados, huracanes)
- Demostración activista en las instalaciones de la compañía
- Falla regional de telecomunicaciones
- Incidentes ambientales y de transporte que resulta en daño al público, el medio ambiente y la continuidad del negocio

5.3 Estrategias de recuperación

En base a los resultados del BIA y del análisis de riesgos, se desarrollan estrategias para identificar mecanismos que permitan a la organización proteger y recuperar las actividades críticas sobre la base de la tolerancia al riesgo de la organización y dentro de los objetivos de tiempo de recuperación definidos. Estas estrategias permiten establecer una estructura de respuesta a incidentes y gestión, gestionar las relaciones con los principales interesados y las partes externas y recuperar las actividades críticas del negocio. En esta etapa se desarrollan los siguientes puntos:

- Identificar los requerimientos estratégicos para la recuperación de la plataforma de TI
- Identificar las opciones de recuperación
- Evaluación de opciones aplicables
- Análisis costo/beneficio de las estrategias de recuperación
- Consideraciones para las estrategias de recuperación

5.4 Requerimientos estratégicos para la recuperación de la plataforma

A continuación, se lista los recursos críticos sobre los cuales se van a diseñar las estrategias de recuperación:

- **Instalaciones:** Área alternativa en donde será recuperada la plataforma de TI.
- **Sistemas de Producción:** Aplicaciones que serán recuperadas.
- **Infraestructura:** Infraestructura que necesita ser recuperada. Se considera solo la infraestructura que se encuentra en el centro de datos de Yellowpepper.
- **Información crítica:** Información a ser respaldada en un sitio alternativo. En este recurso se tomará en cuenta información que no es almacenada en base de datos como manuales, documentos técnicos, etc. No se ha tomado en cuenta la información que es almacenada en base de datos ya que actualmente existe un procedimiento establecido para respaldos.

5.5 Identificar las opciones de recuperación

Los métodos de adquisición de los recursos pueden ser:


- **Bajo demanda:** Los recursos son adquiridos e instalados luego de haber ocurrido el desastre.
- **Pre-establecidas:** Los recursos son adquiridos e instalados antes de que ocurra un desastre y su uso es única y exclusivamente para propósitos de recuperación.
- **Pre-acordadas:** Se establecen acuerdos con los proveedores los cuales garantizaran la entrega de los recursos dentro de un periodo convenido luego de que ocurra un desastre.

A continuación, se listan las opciones de recuperación que se tendrían por recurso crítico:

Recurso: Instalaciones

Categoría	Opción de recuperación	Descripción
Instalación propia	Instalación alternativa propia de Yellowpepper	Un centro de datos propio de Yellowpepper debidamente adecuado.
Instalación comercial	Instalación alternativa arrendada	Un centro de datos físico arrendado a un proveedor.
	Instalaciones en la nube	Un centro de datos lógico arrendado a un proveedor
Método de adquisición	Bajo demanda	La instalación es adquirida cuando ocurre el desastre, según las necesidades del momento.
	Pre-establecido	La instalación es adquirida y preparada exclusivamente para este propósito antes de que ocurra el desastre
	Pre-acordada	La instalación es adquirida a un proveedor que garantice la disponibilidad de la instalación en un periodo de tiempo convenido entre ambas partes a partir del desastre.

Recurso: Infraestructura


Categoría	Opción de recuperación	Descripción
Infraestructura propia	Infraestructura alternativa propia de Yellowpepper	Infraestructura propia de Yellowpepper debidamente adecuado.
Infraestructura comercial	Infraestructura alternativa arrendada	Infraestructura física arrendada a un proveedor.
	Infraestructura lógica (en la nube)	Infraestructura lógica arrendado a un proveedor
Método de adquisición	Bajo demanda	La infraestructura es adquirida cuando ocurre el desastre, según las necesidades del momento. Continúa 

Pre-establecido	La infraestructura es adquirida y preparada exclusivamente para este propósito antes de que ocurra el desastre
Pre-acordada	La infraestructura es adquirida a un proveedor que garantice la disponibilidad de la misma en un periodo de tiempo convenido entre ambas partes a partir del desastre.

Recurso: Sistemas de producción

Categoría	Opción de recuperación	Descripción
Método de adquisición	Bajo demanda	Las aplicaciones son instaladas cuando ocurre el desastre, según las necesidades del momento.
	Pre-establecido	Las aplicaciones son instaladas exclusivamente para este propósito antes de que ocurra el desastre
	Pre-acordada	Las aplicaciones son instaladas por un proveedor que garantice la disponibilidad de las mismas en un periodo de tiempo convenido entre ambas partes a partir del desastre.

Recurso: Información

Categoría	Opción de recuperación	Descripción
Sitio alternativo de almacenamiento	Sitio físico propio de Yellowpepper	Sitio de almacenamiento físico externo propio de Yellowpepper con las respectivas seguridades.
	Sitio físico arrendado	Sitio de almacenamiento físico externo, arrendado por un proveedor que ofrece las seguridades necesarias. Continúa 

	Sitio en la nube	Sitios de almacenamiento virtual accedido a través de internet con las respectivas seguridades.
Frecuencia de los respaldos	Diaria	Información respaldada una vez al día
	Semanal	Información respaldada una vez a la semana
	Mensual	Información respaldada una vez al mes
	Anual	Información respaldada una vez al año

5.6 Evaluación de opciones aplicables

Es necesario evaluar las opciones de recuperación en donde se analiza la aplicabilidad de cada opción y la prioridad de implementación de la misma en base a costos y factibilidad de Yellowpepper. Para evaluar la aplicabilidad se usan las siguientes opciones:

- Adecuado
- Recomendable
- No recomendable
- No aplica

Para evaluar la prioridad de implementación, se usan los siguientes niveles de prioridad:

- Prioridad alta
- Prioridad media
- Prioridad baja
- Prioridad nula

A continuación, se presenta la evaluación de las opciones de recuperación.


A. Recurso: Instalaciones

Categoría	Opción de recuperación	Aplicación	Prioridad de implementación
Instalación propia	Instalación alternativa propia de Yellowpepper	No Recomendable	4
Instalación comercial	Instalación alternativa arrendada	Recomendable	2
	Instalaciones en la nube	Adecuada	1
Método de adquisición	Bajo demanda	No Recomendable	4
	Pre-establecido	Adecuado	2
	Pre-acordada	Recomendable	3

A. Recurso: Infraestructura

Categoría	Opción de recuperación	Aplicación	Prioridad de implementación
Infraestructura propia	Infraestructura alternativa propia de Yellowpepper	No recomendable	4
Infraestructura comercial	Infraestructura alternativa arrendada	Recomendable	2
	Infraestructura en la nube	Adecuado	1
Método de adquisición	Bajo demanda	No recomendable	4
	Pre-establecido	Adecuado	1
	Pre-acordada	No recomendable	4

B. Recurso: Sistemas de producción

Categoría	Opción de recuperación	Aplicación	Prioridad de implementación
Método de adquisición	Bajo demanda	No recomendable	4
	Pre-establecido	Adecuado	1
	Pre-acordada	No recomendable	4 Continua 

C. Recurso: Información

Categoría	Opción de recuperación	Aplicación	Prioridad de implementación
Sitio alternativo de almacenamiento	Sitio físico propio de Yellowpepper	No recomendable	4
	Sitio físico arrendado	Recomendable	2
	Sitio en la nube	Adecuado	1
Frecuencia de los respaldos	Diaria	Adecuada	1
	Semanal	Recomendable	3
	Mensual	No recomendable	4
	Anual	No aplica	4

5.7 Análisis costo/beneficio de las estrategias de recuperación.

Evaluadas las opciones de recuperación para el centro de datos e información de Yellowpepper, procederemos a evaluar los costos. El objetivo de esta evaluación es escoger la opción que más se acople a las necesidades de la empresa. Las opciones que más se acoplan a las necesidades de la empresa para son:

- Arrendar un centro de físico
- Arrendar un centro de datos en la nube

A continuación, se muestra un resumen de la Evaluación de Costos.

OPCION DE RECUPERACIÓN	COSTO
Arrendar un centro de datos físico	\$ 756,060.19
Arrendar un centro de datos en la nube	\$ 487,398.00

5.8 Selección de la estrategia

Luego de realizar el análisis costo-beneficio de las estrategias que más se acoplan a las necesidades de la empresa, se llegó a la conclusión que la mejor opción es arrendar un centro de datos en la nube ya que la misma tiene una arquitectura orientada a servicios ahorrando en hardware. A continuación, las razones más relevantes que permitieron escoger dicha estrategia:

- Implementación es mucho más rápida y con menos riesgos: No existe hardware por comprar y mantener.
- Recursos escalables y configurables a medida: Es posible tener los servidores con los recursos que se necesite en el momento. Se podría reconfigurar los servidores Cloud y disponer de más recursos en caso que se necesite.
- Reducción de costos: La posibilidad de configuración de recursos, unido al menor costo de mantenimiento de una infraestructura en la nube, hacen que los servicios en la nube sean más económicos que los de hosting tradicional. Esto permite tener un Servidor Dedicado a menor precio.
- Resiliencia y redundancia: No hay posibilidades de fallas de hardware. La información está mucho más segura en un servidor de la nube comparado con un servidor dedicado ya que, incluso en caso de pérdida catastrófica de datos en su almacenamiento, el riesgo es mucho menor que en un servidor dedicado.

A continuación, se detalla la estrategia seleccionada:

Terremark configurará, implementará, desarrollará, provisionará y probará los recursos computacionales, recursos de almacenamiento, recursos de red (“infrastructure”) servicios de soporte y la aplicación utilizada para manejar Infrastructure (“aplicación Inficenter”). Infrastructure y la aplicación de

Infinicenter serán usados por Terremark para proveer los Servicios de Nube Empresarial a Yellowpepper.

Localización de la Solución

Solución	Localización
Nube	Terremark – Culpeper
Dispositivos de Red dedicados	Terremark - Culpeper

Costos:

A continuación, se muestra los costos sumarizados:

Total de cargos no recurrentes	\$2,295.00
Implementación de Servicios	\$2,295.00
Total de cargos Mensuales Recurrentes	\$8,753.00
Servicios Mensuales – Hosting	\$4,128.00
Servicios Mensuales – Red	\$3,125.00
Servicios Mensuales – Seguridad	\$0
Servicios Mensuales – Almacenamiento	\$1,500.00

Detalle de Precios del Servicio de Nube Empresarial

Servicios Mensuales de Hosting			
Descripción	Cant.	Precio	Exceso
Recursos Computacionales	1	\$4,128.00	\$4,128.00
Total			\$4,128.00
Servicios Mensuales de Red			
Descripción	Cant.	Precio	Exceso
Conectividad - Ancho de Banda Comprometido	1	\$125.00	\$125.00
Recursos de Red	1	\$0.00	\$0.00
Total			\$125.00
Servicios Mensuales de Seguridad			
Descripción	Cant.	Precio	Exceso

Recursos Computacionales	1	\$0.00	\$0.00
Total			\$0.00
Servicios Mensuales de Almacenamiento			
Descripción	Cant.	Precio	Exceso
Capacidad de Almacenamiento	1	\$1,500.00	\$1,500.00
Total			\$1,500.00

Dispositivos de red dedicados

Implementación de Servicios			
Descripción	Cant.	Precio	Exceso
OnNet IFC - Cat 6	1	\$295.00	\$295.00
OnNet IFC – Conexión	1	\$2,000.00	\$2,000.00
Total			\$2,295.00
Servicios Mensuales de Red			
Descripción	Cant.	Precio	Exceso
On-Net Conexión	1	\$3,000.00	\$3,000.00
Total			\$3,000.00


Detalle de los servicios de nube empresarial

Ancho de Banda

Conectividad - Ancho de Banda Comprometido	
Cantidad	1
Ancho de Banda	5 Mbps

Ambiente de la Nube

Recursos computacionales	
Cantidad	1
Manejo de Recursos	12 x Manejo de Recursos de Nube Empresarial - 1Ghz, 2GB MEM
CPU	12 GHz
Recursos de Memoria	24GB

Continua 	
Recursos de Red	
Cantidad	1
Recursos de Red	Utilidad de Load Balancer de Nube Empresarial HA
Recursos de IP Publica	5 x Ips Publicas
Recursos de IP Privada	Ips privadas (DMZ/27)
Recursos de IP Privada	Ips privadas (Int/28)
Seguridad	
Cantidad	1
Recursos de Seguridad	Utilidad de Firewall de Nube Empresarial HA
Recursos de Seguridad	2 x software de VPN Cliente de Nube Empresarial
Almacenamiento	
Cantidad	1
Recursos de Fibra de Almacenamiento	2000 GB

Dispositivos dedicados de red

Cableado entre unidades

Onnet IFC - Cat5	
Cantidad	1
IFC –Impl	CAT5, UTP - Setup

Onnet MIA to NCR

Conexión Onnet	
Cantidad	1
Servicio Una sola vez	2 x On-Net Conexión rápida
Ancho de Banda	100 Mbps

5.9 Declaración de desastre

Los siguientes empleados o colaboradores de Yellowpepper, están autorizados para declarar un desastre de los sistemas de información desplegados en el NAP, además de emitir una señal de normalización y reanudación de actividades y la posterior declaración de fin de aplicación del presente plan.

Nombre	Cargo
CEO de la compañía	CEO de la compañía
Director de Tecnología	Director de Tecnología
Director de Tecnología	Vicepresidente de la compañía

CAPITULO 6

6.1 Estructura del equipo PCN

Equipo	Función	Asignación
Comité de crisis	Líder de equipo	CEO de la compañía
Comité de crisis	Líder suplente y Miembro	Director de Tecnología
Comité de crisis	Miembro	Vicepresidente de la compañía
Comité de crisis	Miembro	Gerente de RRHH
Comité de crisis	Miembro	Controller
Logística	Líder de equipo	Gerente de RRHH
Logística	Miembro	Business Analyst
Logística	Miembro	Contador
Relaciones públicas	Líder de equipo	Relaciones Públicas
Relaciones públicas	Miembro	Coordinador de soporte
Unidades de negocio	Lider Equipo	Director de Tecnología
Unidades de negocio	Miembro	Administrador SAP
Unidades de negocio	Miembro	Director de proyectos
Unidades de negocio	Miembro	Control de calidad
Recuperación	Lider Equipo	Director de operaciones
Recuperación	Miembro	Administrador de redes
Recuperación	Miembro	Administrador de Base de datos
Recuperación	Miembro	Administrador de sistemas

La Figura 7 muestra cómo se deben organizar los equipos una vez declarado un desastre.

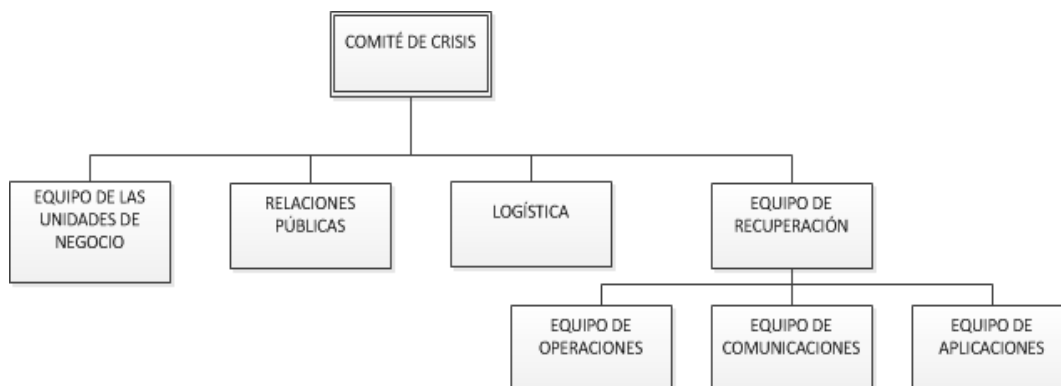


Figura 7 Organización de equipos en declaración de desastre

6.2 Equipos y responsabilidades

Se han creado equipos de trabajo en algunos casos y en otros solo personas debido al tamaño de la empresa, que intervendrán en la ejecución del plan.

A. Comité de crisis

El Comité de crisis es el responsable de la activación del plan de continuidad de negocio y dirigir las acciones durante la contingencia y recuperación. Toma las decisiones “clave” durante un incidente, además que mantiene informado de la situación a los accionistas de la compañía. Las principales tareas y responsabilidades de este comité son:

- 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.

El Líder del equipo es el responsable por la coordinación general del proceso.

Las responsabilidades incluyen:

- Asegurar que todos los miembros del comité se pongan en contacto y se comuniquen según sea necesario.
- Asegurar que todas las cuestiones de respuesta, como se identifica en los planes durante la activación, se publiquen y consten en el registro de seguimiento.
- Asegurar que todas las actividades de gestión de crisis y comunicaciones sean consistentes con las políticas de la compañía y las regulaciones gubernamentales
- Asegurar que las políticas y procedimientos del comité estén claramente definidas y que los miembros del equipo están capacitados
- Asegurar que los nuevos miembros del comité de crisis reciban capacitación sobre las funciones y responsabilidades.
- Mantener una lista de todos los contactos clave.
- Coordinar y difundir el calendario de las reuniones del grupo

Los miembros del grupo evalúan las consecuencias globales del incidente y en representación de sus respectivas áreas funcionales en respuesta al incidente.

Esto incluye:

- Dar prioridad a las responsabilidades del comité de crisis además de las responsabilidades funcionales del día a día
- Familiarizarse con sus roles individuales, responsabilidades y procedimientos generales del comité de crisis.
- Contribuir funcionalmente a los esfuerzos de respuesta ante un incidente
- Participar en el proceso de revisión posterior de un incidente
- Participar en la formación de gestión de crisis

B. Equipo de recuperación

Su función consiste en establecer los sistemas necesarios para la recuperación. Esto incluye todas las aplicaciones, comunicaciones y datos y cualquier otro elemento necesario para la restauración de un servicio. El líder del equipo de recuperación informa al comité de crisis acerca de la interrupción en el servicio y el avance en la recuperación. Este equipo está compuesto por un líder el cual es el director de operaciones y soporte el cual coordina y gestiona las actividades con sus miembros que se describen a continuación:

C. Equipo de Comunicaciones

Se encarga de las acciones de recuperación de la red comunicaciones.

Algunas de sus responsabilidades son las siguientes:

- Desarrollar y documentar las configuraciones de las comunicaciones de datos.
- Determinar el daño en la red de comunicaciones y asegurar la provisión del equipo de reemplazo.
- Coordinar la instalación del software del sistema operativo que permita la restauración de las comunicaciones.
- Ordenar e instalar el hardware necesario para establecer comunicaciones.
- Coordinar con entes externos para restaurar el servicio y ordenar las comunicaciones.
- Probar que las comunicaciones se hayan establecido adecuadamente.

D. Equipo de Operaciones

Este equipo de trabajo se encarga de la restauración de las operaciones de las plataformas críticas.

Entre sus responsabilidades están las siguientes:

- Asegurar la disponibilidad de los respaldos necesarios en la recuperación.
- Restaurar archivos y sistema operativo en el sitio de recuperación.
- Elaborar calendarios de operaciones en el sitio de recuperación.

- En caso necesario, coordinar actividades necesarias para restaurar las facilidades en el sitio principal o en el sitio alternativo.
- Ordenar e instalar el hardware necesario para el procesamiento normal en el sitio permanente.

E. Equipo de Aplicaciones

Este equipo se encarga de la restauración de las aplicaciones que residen en los servidores. Entre sus responsabilidades están las siguientes:

- Coordinar la recuperación de las aplicaciones en los servidores del centro de datos principal o alternativo.
- Reconstruir el ambiente de operación de las aplicaciones que residen en los servidores.
- Soportar el esfuerzo de los usuarios para actualizar los datos de la aplicación.
- En caso necesario, desarrollar un plan de trabajo detallado para moverse del sitio-alterno al sitio principal.

F. Equipo de las unidades de negocio

Está conformado por personas que interactúan con las aplicaciones críticas. Serán los encargados de realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas y comenzar a funcionar. Este equipo es responsable de:

- Verificar la operatividad de las aplicaciones a través de la ejecución de un conjunto de pruebas.
- Crear y mantener los escenarios de prueba actualizados
- Informar a la operatividad de las aplicaciones.

G. Logística

Responsable de proveer los medios necesarios para contribuir a la reactivación de la actividad normal. Las responsabilidades del equipo son:

- Solicitar al comité de crisis la provisión de recursos que se utilizaran durante la contingencia

- Contactar y coordinar las actividades a realizar con policía, bomberos y servicios médicos en caso de ser necesario
- Proveer transporte para equipos, personas y suministros al lugar de recuperación.
- Proveer dirección y números de teléfonos del centro Alterno
- Coordinar pagos de facturas
- Contacto con proveedores
- Proveer suministro de oficina y comida

Este equipo debe trabajar conjuntamente con los demás, con el fin de asegurar que todas las necesidades logísticas sean cubiertas.

H. Relaciones públicas

Responsable de las comunicaciones con clientes, accionistas y medios de comunicación canalizando la información que se realiza al exterior desde un solo punto. Sus funciones principales son:

- Elaboración de comunicados para la prensa.
- Comunicación con los clientes

Las tareas a realizar son:

- Si el tipo de incidente lo requiere, emitir un comunicado oficial a clientes y proveedores en el que se indique que se restablecerán los servicios lo antes posible.
- Atender a los clientes para proporcionarles información sobre el incidente con el fin de no genera pánico.

6.3 Desarrollo de procedimientos

Se han desarrollado procedimientos en base a los siguientes planes:

A. Plan de respuesta ante una emergencia

Incluye eventos que involucren grandes desastres en el centro de datos y crisis ante una amenaza no pandémica. Yellowpepper ha considerado potenciales situaciones de emergencia que puedan surgir en el centro de datos, ubicado en el NAP de las Américas. Cada situación se aborda más adelante, y esboza la respuesta ante una situación y las necesidades de servicios de emergencia (por ejemplo, bomberos, ambulancias, policía, etc.).

B. Plan de Gestión de Crisis

Estos procedimientos se ejecutan inmediatamente de haber sucedido un incidente que interrumpa las actividades críticas en la organización. Permitirán confirmar el tipo de incidente y su criticidad, tomar el control de la situación y mitigar el impacto que dicho incidente pueda provocar.

- Procedimiento de respuesta inicial
- Procedimiento de verificación del incidente
- Procedimiento de evaluación de daños
- Procedimiento de notificación de ejecución del plan

C. Planes de recuperación y restauración

Esta sección contiene los *planes de recuperación* tanto de la tecnología, los servicios y las instalaciones de la infraestructura que dan soporte a los procesos críticos del negocio que han de ser activados en caso de una crisis. Este estado no se considera un ESTADO NORMAL de desempeño y desarrollo de las actividades de la empresa.

Adicionalmente están los *planes de restauración*, que son planes para restaurar la infraestructura de la tecnología y la instalación a un ESTADO NORMAL de operación, ya sea por retorno a las oficinas o por el establecimiento de un nuevo lugar para desempeñar las tareas y procesos. La responsabilidad

de declarar un ESTADO DE NORMALIDAD depende de los altos funcionarios de la compañía.

Los planes de recuperación implementados, fueron:

- Plan de recuperación de Contabilidad
- Plan de recuperación de Operaciones
- Plan de recuperación de soporte
- Plan de recuperación de Consultores

Las acciones de restauración implementadas fueron:

- Acciones de restauración de Contabilidad
- Acciones de restauración de Operaciones
- Acciones de restauración de soporte
- Acciones de restauración de Consultores

CAPITULO 7

MANTENIMIENTO DEL PLAN DE CONTINUIDAD DEL NEGOCIO

El Plan de Continuidad de Negocio (PCN) es un documento que debe ser actualizado periódicamente con el fin de reflejar en él los cambios organizativos y de negocio que se presentan durante el pasar del tiempo y puedan ocasionar variaciones dentro de las prioridades establecidas en los riesgos. El comité de crisis es el responsable de la difusión, mantenimiento y pruebas periódicas del presente plan. Dentro de sus responsabilidades están:

- Promover una cultura de continuidad de negocio dentro de la empresa
- Permanente monitoreo de los procesos
- Documentar los cambios
- Coordinar y monitorear las pruebas del plan de continuidad
- Evaluar los resultados
- Optimizar las actividades que tuvieron algún grado de dificultad.
- Reforzar los procesos que funcionan normalmente

7.1 Ejecución de pruebas

Desarrollado e implantado el plan de continuidad de negocio, es recomendable que sea probado periódicamente debido a los siguientes motivos:

- Frecuentemente se descubren nuevas mejoras y eficiencias que mejoran el plan al ser aplicadas.
- Los procesos de negocio, el entorno tecnológico y multitud de componentes adicionales pueden cambiar durante el tiempo provocando que los planes de continuidad de negocio dejen de estar actualizados.

- Evaluar de forma más veraz la capacidad de respuesta de la empresa ante un desastre (tiempos de respuesta, capacidad de los responsables implicados e idoneidad de los procedimientos desarrollados).

El comité de crisis planificará las pruebas, su duración y alcance, los participantes (incluidos proveedores de servicios), los elementos del plan que serán evaluados (personas, comunicaciones, sistemas, procedimientos) y la secuencia de pasos a emprender durante su ejecución. Las pruebas deben simular situaciones próximas a la realidad y deben ser planificadas de forma que la exposición de las actividades de la organización ante los riesgos sea mínima. Debido a que la empresa no podrá paralizar completamente su producción, las pruebas serán realizadas en áreas y momentos específicos que no paralizen la entrega del servicio.

7.2 Cronograma de mantenimiento del PCN

Actividad del plan de mantenimiento	Responsabilidad	Frecuencia
Mantener un directorio que contenga los documentos PCN en el servidor de archivos. Las subcarpetas deben ser: <ul style="list-style-type: none"> ✓ Análisis de Impacto al Negocio (BIA) ✓ Operaciones ✓ Financiera ✓ Plan de Respuesta a las Crisis (CRP) ✓ Plan de Respuesta a Emergencias Instalaciones ✓ Plan de Operaciones de Seguridad ✓ Plan de Respuesta ✓ Plan de Comunicaciones ✓ Planes de Recuperación y Restauración ✓ Plan de Recuperación de Desastres (Disaster Recovery Plan) 	Director de Soporte y Operaciones	Actividad del día a día

Continúa 

<p>✓ Planes de restauración de actividades (para procesos esenciales definidos por BIA)</p>		
<p>Realizar revisiones de los planes para evaluar la exactitud de la información. Los propietarios de los procesos son los responsables de mantener los planes de reanudación al día. Cuando se producen cambios en los procesos, evaluar si el cambio propuesto y/o proyectadas impactará el PCN. Si es así es convocar a un comité para cambiarlo y actualizarlo.</p>	<p>CEO, coordinadores y dueños de procesos</p>	<p>Anual</p>
<p>Revisar los planes de recuperación por área. Actualizarlos si es necesario.</p>	<p>Gerentes de área</p>	<p>Bianual</p>
<p>Realizar ejercicios de validación de:</p> <ul style="list-style-type: none"> • Ejercicios de Evacuación y Refugio • Prueba de llamadas • Simulación de crisis 	<p>Director de Soporte y Operaciones</p>	<p>Bianual</p>
<p>Llevar a cabo ejercicios de prueba que permitan simular una reconstrucción de los servidores necesarios para reanudar rápidamente los procesos de negocio esenciales. Medir los resultados según lo acordado en el RTO y RPO</p>	<p>Gerentes de área</p>	<p>Anual</p>
<p>Llevar a cabo ejercicios de entrenamiento de sus equipos para proporcionar a los colaboradores de las prácticas que necesitan aprender para llevar a cabo eficazmente las tareas y procedimientos de reanudación, con el fin de prepararlos para una aplicación real</p>	<p>Director de Soporte y Operaciones Gerentes de área</p>	<p>Anual</p>

BIBLIOGRAFIA

- (s.f.). Obtenido de http://www.utp.edu.co/php/controlInterno/docsFTP/ADMINISTRACION_DE_RIESGOS172.ppt.
- (2010). Obtenido de Universidad Tecnologica de Pereira: http://www.utp.edu.co/php/controlInterno/docsFTP/ADMINISTRACION_DE_RIESGOS172.ppt
- Alexander, A. G. (2007). *Diseño de un sistema de gestión de seguridad de información*. Bogota: Alfaomega Colombiana S.A.
- Anonimo. (03 de 02 de 2011). *Banca Movil, negocio en expansion*. Recuperado el 15 de 08 de 2012, de [ww.Universo.com](http://www.eluniverso.com): <http://www.eluniverso.com/2011/02/03/1/1356/banca-movil-negocio-expansion.html>
- AS/NZS. (2004). *Risk management* (Tercera edición 2004 ed.). Standards Australia/Standards New Zealand.
- AS/NZS 4360 Risk management. (2004).
- British, B. (28 de Febrero de 2006). *Business continuity management - Part 1: code of practice*. BSI. Obtenido de Wikipedia: http://es.wikipedia.org/wiki/Plan_de_continuidad_del_negocio
- BS 25999-1. (2006).
- DAlvarez. (15 de 02 de 2012). *Boletin de Prensa*. Recuperado el 15 de 08 de 2012, de INEC: http://www.inec.gob.ec/sitio_tics/boletin.pdf
- Ferrer, R. (25 de 02 de 2009). Plan de Continuidad BS 26999.
- Infraestructura, S. e. (s.f.). *Asegure la continuidad de la empresa*. Obtenido de Plan de continuidad de negocio: <http://sistemas.trevenque.es/soluciones/recuperacion-de-datos-y-continuidad-de-negocio/>
- Norma AN/NZS 4360. (2004).

Sistemas e Infraestructuras. (s.f.). Obtenido de CCA Sistemas Grupo Trevenque:

<http://sistemas.trevenque.es/soluciones/recuperacion-de-datos-y-continuidad-de-negocio/>

Syed, A., & Syed , A. (s.f.). *Business Continuity Planning Methodology.* Sentryx Incorporated, 2004.

Yellowpepper. (s.f.). Documentación del departamento de operaciones.

GLOSARIO

BCP: Plan de continuidad del negocio.

DRP: Plan de Recuperación de Desastres.

MTD: Periodo máximo de tiempo de inactividad que puede tolerar la organización sin entrar en un colapso financiero y operacional.

RTO: Recovery Time Objective. Tiempo máximo permitido que un proceso puede estar caído como consecuencia de un evento catastrófico.

RPO: Recovery Point Objective. Define la pérdida de datos máxima tolerable que se acepta ante una situación de desastre.

WRT: Tiempo disponible para recuperar datos perdidos una vez que los sistemas estén reparados, dentro del MTD.