DECANATO DE INGENIERÍA E INFORMÁTICA

ESCUELA DE INFORMÁTICA

Plan de Continuidad de Negocio para el Área de TI del Centro de Procesamiento Transaccional, S.A. para el 2014.

Sustentantes:

Félix José Rodríguez Paulino 2006-0625

Arturo Tomas García Estrella 2007-2239

Iván Emmanuel Martínez Naranjo 2008-0248

Asesores:

Ing. Ramón Gómez

Monografía para Optar por el Título de:

Ingeniero en Sistemas de Información

Distrito Nacional, República Dominicana

Abril, 2014

Plan de Continuidad de Negocio para el Área de TI del Centro de Procesamiento Transaccional, S.A. para el 2013.

DEDICATORIAS

Principalmente a Dios, porque siempre esta cuando las ganas de seguir avanzando me faltan y a la vez me da la fuerza de seguir adelante en busca del éxito.

A mis padres, por ser mis guiadores, por enseñarme a persistir para conseguir mis metas, por su apoyo y sus orientaciones profesionales; muchas gracias, pues por ustedes he llegado a culminar otra meta más en mi vida.

También a mi bella hija, por ser la razón de mi vida y porque me ha dado las razones de seguir luchando por mis metas y crecer persona y profesionalmente.

Félix José Rodríguez Paulino.

Dedico este trabajo en primer lugar a Dios por darme la fortaleza en los momentos difíciles para seguir adelante, por ser todo poderoso y creador de todas las cosas.

De igual forma, a mi familia, a quienes le debo la vida y me han apoyado a lo largo de este reto universitario, por estar presentes en los momentos difíciles, por soportarme económicamente cuando lo he necesitado y por ayudarme en las asignaciones que eran prioritarias.

A mis amigos, quienes han compartido conmigo momentos inolvidables tanto dentro como fuera de la universidad. Les agradezco por ser mi soporte en los momentos difíciles.

Por último pero no menos importante, a mi novia, quien siempre se preocupó porque completara la universidad y me convirtiera en un exitoso profesional.

Arturo Tomas García Estrella.

En primer lugar quiero dedicar este trabajo de grado a papa Dios por darme salud para levantarme todos los días, la fuerza para luchar y no rendirme en los momentos difíciles y la sabiduría para enfrentar todos los obstáculos que se me presentan día a día, definitivamente gracias a él he logrado concluir mi carrera.

A mi padre Francisco Martínez, por siempre estar ahí brindándome su apoyo ante cualquier situación que se me presente, sin lugar a dudas ha sido la persona más influyente para mí en todos los sentidos y me llena de satisfacción poder dedicarle este trabajo.

A mi madre Aida Naranjo, que aunque no esté físicamente conmigo sé que desde el cielo me bendice y me guía para que todo salga bien, sé que este momento hubiera sido tan especial para ti como lo es para mí.

A mi hermana Tatiana Martínez, por su apoyo incondicional, por sus consejos y porque a pesar de nuestras diferencias siempre está dispuesta a escucharme y ayudarme en cualquier momento.

Iván Emmanuel Martínez Naranjo.

AGRADECIMIENTOS

A Dios, por servirme de guía y porque gracias a él pude levantarme y me ayudo a tomar las decisiones correctas en este arduo camino de la carrera.

A mis padres, Félix Ramón Rodríguez y María Altagracia Paulino, por instruirme por el camino sabio, y por su apoyo incondicional, ustedes son la principal inspiración para la culminación de mi carrera.

A mi novia Katherine Duran, por ser una persona incondicional y que ha estado presente incondicionalmente ante este arduo trabajo de grado.

A mis compañeros, Iván Martínez y Arturo García, gracias por tu apoyo y la dedicación para culminar esta, tan importante, meta. Espero que este sea el primero de muchos proyectos en los que podamos involucrarnos.

A nuestro asesor Ramón Gómez, por estar con nosotras desde el inicio de esta memoria, mediante su contribución, correcciones y recomendaciones, hoy podemos dar punto final a otra etapa de nuestras vidas.

Félix José Rodríguez Paulino.

A mi madre, Carmen Virginia Estrella de García, que fue mi soporto tanto económico como espiritual, siempre aconsejándome y tratando de que no dejara el camino correcto para llegar al éxito. Con su amor y entendimiento logró un cambio enorme en mi actitud y en mi forma de ver la vida.

A mi padre, Tomas Arturo García Freites, el cual ha sido un padre ejemplar, enseñándome que en la vida hay que sacrificarse para lograr tener estabilidad.

A mi hermana, Virginia Giselle García Estrella, quien ha aportado tanto en mi camino universitario ayudándome en las materias más difíciles y a mi hermano, Enrique Augusto García Estrella, por su compañía todos estos años.

A mi abuelo (que en paz descanse), Cesar Augusto Estrella Sadhalá, quien en su tiempo en la tierra logró que mi familia sea la más unida del mundo, quien inculco valores que jamás olvidaré y los cuales pasaré a mi familia más adelante.

A mi abuela. Ivelise Saldaña Rodríguez, quien siempre creyó en mí y me dio todo el cariño que las abuelas saben dar, consintiéndome cada vez que podía e incluso ayudándome económicamente en algunas cosas.

A mi novia, Carolina Torres Tavarez, quien siempre me ha apoyado y acompañado desde hace 4 años, ayudándome a ser mejor persona y soportando todo mi mal genio dándome amor y amistad.

Arturo Tomas García Estrella.

En primer lugar agradezco a Dios, por derramar tantas bendiciones sobre mí y haberme permitido cumplir uno de mis más grandes sueños, muchas gracias papa Dios porque gracias a ti pude culminar esta etapa de mi vida.

A mi padre Francisco Martínez, porque durante todos estos años ha sabido apoyarme para continuar y nunca renunciar a lo que realmente quiero, gracias por tu amor incondicional.

A mi hermana Tatiana Martínez, por alentarme en el transcurso de mi carrera a seguir luchando a pesar de los tropiezos para que sea alguien de bien.

A mis compañeros Félix Rodríguez y Arturo García por todos sus aportes durante el desarrollo de este gran proyecto, el cual desarrollamos con mucho esfuerzo, dedicación, enojos, risas y trasnochos el inicio de una nueva etapa.

Agradezco también a todos lo que directa e indirectamente nos brindaron su ayuda en este proyecto.

Iván Emmanuel Martínez Naranjo.

Tabla de Contenido

RESUMEN

En la actualidad, con el gran desarrollo de la tecnología, las empresas han basado sus operaciones en el uso de los sistemas de información, facilitando así su crecimiento.

Tomando en cuenta la dependencia que actualmente tienen las empresas de la tecnología, es de suma importancia disponer de un plan de recuperación ante desastres para de esta forma minimizar posibles pérdidas humanas, financieras y/o tecnológicas.

En este estudio se examinó el entorno tecnológico de la institución, como también los procesos operativos más críticos, los riesgos asociados y sus diferentes vulnerabilidades. Por tal razón se desarrolló un plan de recuperación ante desastres para el área de TI del Centro de Procesamiento Transaccional, S.A., el cual busca el aseguramiento de la continuidad de los procesos críticos del negocio.

INTRODUCCIÓN

Este trabajo de grado se desarrolla con el propósito de obtener el título de Ingeniero de Sistemas de Información y de igual forma, se busca colaborar con el Centro de Procesamiento Transaccional, S.A. para que disponga de un plan de recuperación ante desastres que cubra las operaciones criticas del negocio.

Actualmente el Centro de Procesamiento Transaccional, S.A. no dispone de adecuados procesos de recuperación en sus operaciones cotidianas para dar respuesta rápida ante cualquier eventualidad que ponga en riesgo la misma. Por tal razón, es de suma importancia el desarrollo de un adecuado plan de recuperación ante desastres que permita la evaluación de los procesos claves, el análisis de sus potenciales riesgos y el establecimiento de los controles necesarios con sus estrategias de recuperación y técnicas prácticas.

Con el desarrollo del plan de recuperación diseñado en este trabajo, se busca que el Centro de Procesamiento Transaccional, S.A. cuente con todos los procedimientos que den oportuna respuesta a cualquier eventualidad en sus actividades y operaciones diarias, protegiéndolos de los diferentes riesgos (estratégico, ambienta, mercado, financieros, operativos, de cumplimientos y tecnológicos) a que están asociadas las empresas.

Este trabajo está desarrollado con una estructura clara y apegándose a un nivel secuencial de los temas planteados, estos son:

Capítulo I – Antecedentes Históricos: En este capítulo se presentan todos los datos referentes al Centro de Procesamiento Transaccional, S.A., desde el organigrama o estructura de la empresa hasta la misión, visión y sus servicios ofrecidos.

Capítulo II – Conceptos Generales: Para este capítulo se tratan todas las definiciones y conceptos claves que soportaran nuestra investigación de grado.

Capítulo III – Gestión de Riesgo: En el capítulo de riesgo se revisarán todos los temas relacionados a la gestión de los riesgos en la empresa, como también los controles establecidos para la protección de los activos de la empresa.

Capítulo VI – Análisis de Impacto al Negocio (BIA): Para este capítulo se evaluarán todas las actividades, procesos y equipos de carácter crítico para el Centro de Procesamiento Transaccional, S.A.

Capítulo V – Estrategias del Plan: Para el capítulo referente a las estrategias del plan se revisarán todos los pasos a seguir mediante las informaciones obtenidas para de esta forma establecer los criterios claves de la continuidad del negocio.

Capítulo VI – Desarrollo del Plan de Recuperación: En este capítulo se establecerán las tareas de ámbito técnico para la ejecución de las estrategias del plan ante cualquier crisis o inadecuada gestión de los recursos tecnológicos.

Capítulo VII – Pruebas y Mantenimientos del Plan: Este capítulo mostrará las diferentes pruebas y los tipos de mantenimientos que se utilizaran para mantener el adecuado desarrollo de todos los procesos del plan.

Capítulo VIII – Plan de Manejo de Comunicación ante Incidentes y Crisis: En este capítulo se identifican todo lo relacionados al manejo de las tareas para una adecuada gestión en las comunicaciones y el manejo de crisis ante la ocurrencia de siniestros.

Capítulo IX – Programa de Capacitación, Concientización y Difusión del Plan: Aquí se manejan los temas relacionados a las metodologías y procedimientos para capacitar y dar difusión al plan, para así poder concientizar y cambiar la cultura de la organización.

Capítulo I

Antecedentes Históricos

1.1 Antecedentes Centro de Procesamiento Transaccional, S.A.

El Centro de Procesamiento Transaccional, S.A. fue iniciada para finales del 1999 con el patrocinio de un conjunto de entidades financieras y de servicios con el objetivo de agregar ventaja competitiva en el procesamiento de sus operaciones financieras, también obtener una mayor optimización de las inversiones de la industria y mejorar la calidad de los servicios, a través de una robusta y eficiente plataforma tecnológica.

Con el pasar de los años a este se unieron otras entidades financieras el cual unifico un diferentes servicios y productos, permitiendo manejar la Red ATH en la República Dominicana instalada en el país desde el año 96, ofreciendo los servicios de procesamiento a una amplia cartera de clientes los cuales fortalecieron de una forma amplia la estructura del Centro.

En mediados del año 2003 el Centro de Procesamiento Transaccional, S.A. lanza ciertos servicios transaccionales ACH el cual se acogió de una forma muy útil a las diferentes entidades del sector financiero, empresas y personas manejando la forma electrónica de pagos y cobros.

Para principios del 2007 sigue ampliando su catálogo de productos y servicios e incorpora la venta de pines de llamadas a través de los puntos de ventas, dinamizando sus líneas de negocios y logrando una amplia inserción en los comercios.

El Centro de Procesamiento Transaccional se ha consolidado como la principal entidad de apoyo al sector financiero, ofreciendo servicios a la industria, el comercio y el sector de servicios, y se ha convertido en la mayor empresa de transacciones electrónicas en la República Dominicana.

1.2 Comité Directivo

Todas las actividades del Centro de Procesamiento Transaccional, S.A. se maneja sus operaciones bajo un total clima de transparencia y apegado a sus más claros principios corporativos y gobernabilidad, guiándose de las mejores prácticas de la industria y apegándose a normas de protección de datos.

La Alta Gerencia del Centro, se ve guiado por las normativas del Comité Directivo los cuales tienen la responsabilidad moral y legal antes sus miembros accionistas y entidades asociadas, el velar por el cumplimiento de estas normas, las cuales deberán ser cumplidas por todos colaboradores de la Institución.

Este Comité está formado por funcionarios claves de los miembros accionistas, estas son reconocidas por una amplia moral y buen prestigio, garantizando la integridad e independencia en la objetividad de sus funciones como representante de alto nivel del Centro.

Dentro de sus funciones, el Comité dispone del tiempo para revisar y mantener alineado todos los temas referentes a la empresa estableciendo políticas y

procedimientos administrativas y operativas claras, cuyos lineamientos enmarquen el contexto del negocio.

1.3 Organigrama Institucional

El organigrama institucional del Centro de Procesamiento Transaccional, S.A. está conformado por un conjunto de funcionarios de alto nivel que integran la dirección administrativa de la misma. Ver organigrama:

Diagrama 1: Fuente Centro de Procesamiento Transaccional, S.A., 2014.

1.4 Organigrama Departamento de Tecnología de la Información

El área de tecnología se ve conformado por un sinnúmero de colaboradores los cuales gestionan el adecuado funcionamiento de las diferentes plataformas del Centro de Procesamiento Transaccional, S.A. Ver Organigrama:

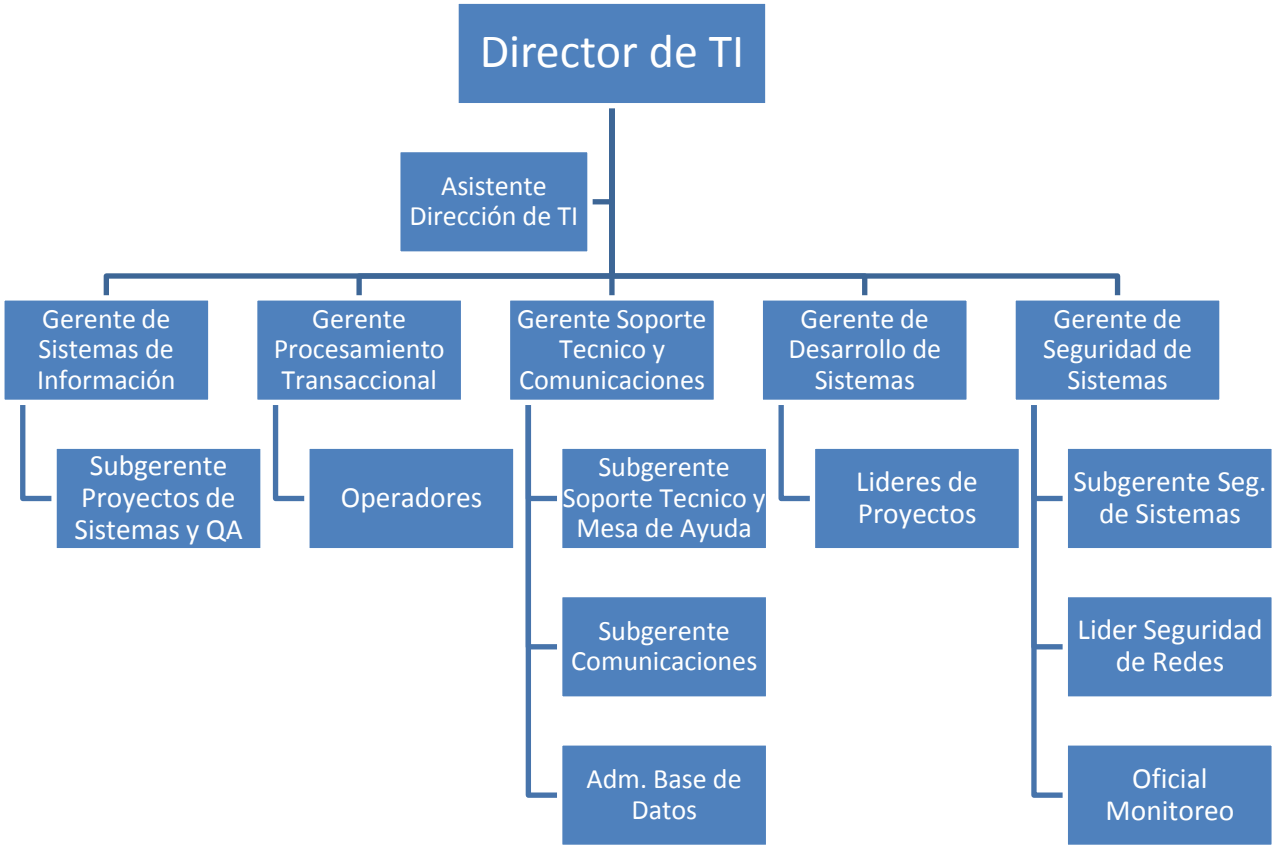


Diagrama 2: Fuente Centro de Procesamiento Transaccional, S.A., 2014.

1.5 Misión y Visión de la Empresa

Dentro de la **misión** del Centro de Procesamiento Transaccional, S.A. está la de ser una empresa con capacidad de identificar oportunidades y generar las soluciones a los usuarios que disponen de los diferentes productos y medios electrónicos brindando un consistente servicio, comprometidos con la calidad y la profesionalidad donde el cliente y el personal sean los recursos más importantes de la empresa, garantizando rentabilidad a sus accionistas.

El Centro de Procesamiento Transaccional, S.A. tiene como **visión** la de mantenerse como líderes del mercado en el procesamiento de transacciones y servicios al sistema financiero, convirtiendo los productos y servicios electrónicos en los medios preferidos de pago, manteniendo la vanguardia tecnológica y la calidad en el servicio.

1.6 Servicios Ofrecidos

El Centro de Procesamiento Transaccional, S.A. es una empresa dedicada a proveer servicios de pagos electrónicos y procesamiento de transaccional, mediante operaciones de redes de transferencias electrónicas de fondos.

Sus servicios se pueden agrupar en varios segmentos de negocios los cuales representan una amplia rentabilidad corporativa, dentro de estos están:

- Red de Cajeros Automáticos y Tarjetas de Débito ATH.

- Procesamiento de Tarjetas y Red de Terminales POS.
- Servicio de Transacciones Pre-Pago.
- Transferencias ACH.
- Distribución del Sistema Electrónico para Pago de Peajes.

Todas estas categorías de servicios proporcionan una amplia solución, de manera directa o indirecta a los diferentes sectores; el financiero, el comercial y el personal.

1.7 Situación Actual

El Centro de Procesamiento Transaccional, S.A. cuenta con una amplia estructura organizacional la cual es soportada por todos los procesos y equipos tecnológicos, estos recursos han evolucionado significativamente para poder estar a la vanguardia en la gestión de servicios con todos sus involucrados.

Actualmente dicha estructura tecnología cuenta de un amplio inventario de activos tecnológicos, dentro de estos están: Equipos Transaccionales (Transervers), Servidores Físico y Virtuales, Laptops y Desktop, la propia información de los clientes que se soportan bajo los esquemas de resguardo o backups, un amplio inventario de aplicaciones y otros más que ayudas directa e indirectamente del día a día operativo del Centro.

Revisando más detalladamente todos estos equipos de alto riesgo para las operaciones de la empresa, se identificó que ni se cuenta de un esquema bien estructurado de contingencia para reponer sus operaciones ante cualquier falla en los sistemas, desastres naturales o cualquier evento mal intencionado.

Esta situación de ausencias de un plan destinado para el restablecimiento de las operaciones del Centro de Procesamiento Transaccional, y tomando en cuenta que esta es una empresa de extremo apego a la tecnología, se identificó la necesidad del desarrollo de un plan de continuidad de negocio para el departamento de TI.

1.8 Infraestructura Actual de Tecnología de la Información

El Centro de Procesamiento Transaccional, S.A. cuenta con una estructura tecnológica que soportan todas las aplicaciones, las conexiones de datos, el servicio de telefonía, la seguridad de sistemas, el soporte técnico y demás áreas operativas, un detalla más claro de dicha estructura es la siguiente:

Distribución Equipos Front Office
Centro de Procesamiento Transaccional, S.A.

Localidad	Empleados	Estaciones (Desktop - Laptop)
Edificio Principal	230	206
Zonas:		
Norte	16	14
Este	4	4
Sur	3	3
Total	**253**	**227**

Tabla 1: Fuente Centro de Procesamiento Transaccional, S.A., 2014.

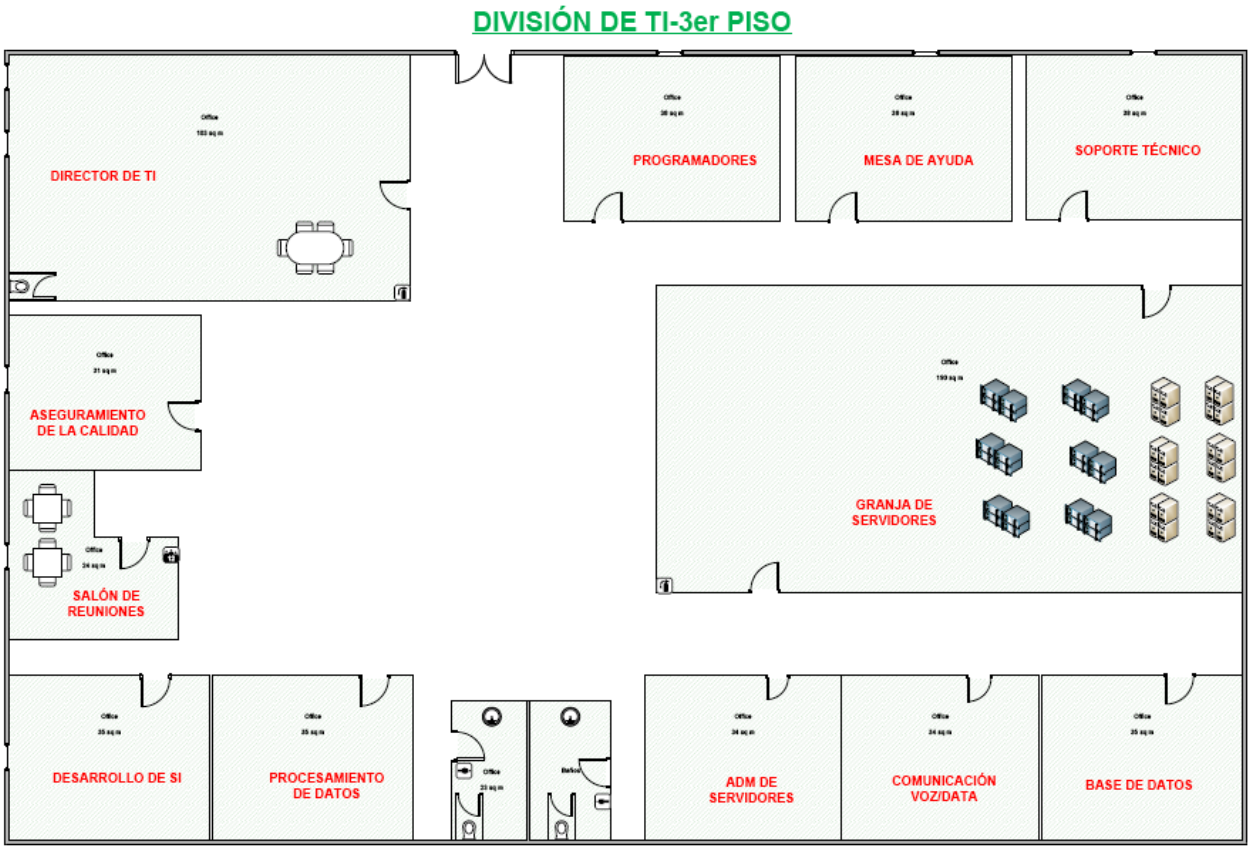
Dentro de los equipos BackOffice ubicados en el tercer piso del edificio principal del Centro de Procesamiento Transaccional, dentro de estos están:

Distribución Equipos Back Office
Centro de Procesamiento Transaccional, S.A.

Equipo	Cantidad
Servidores Windows	113
Oracle	95
Transervers	4
Switch	49
Otros	169
Total	**430**

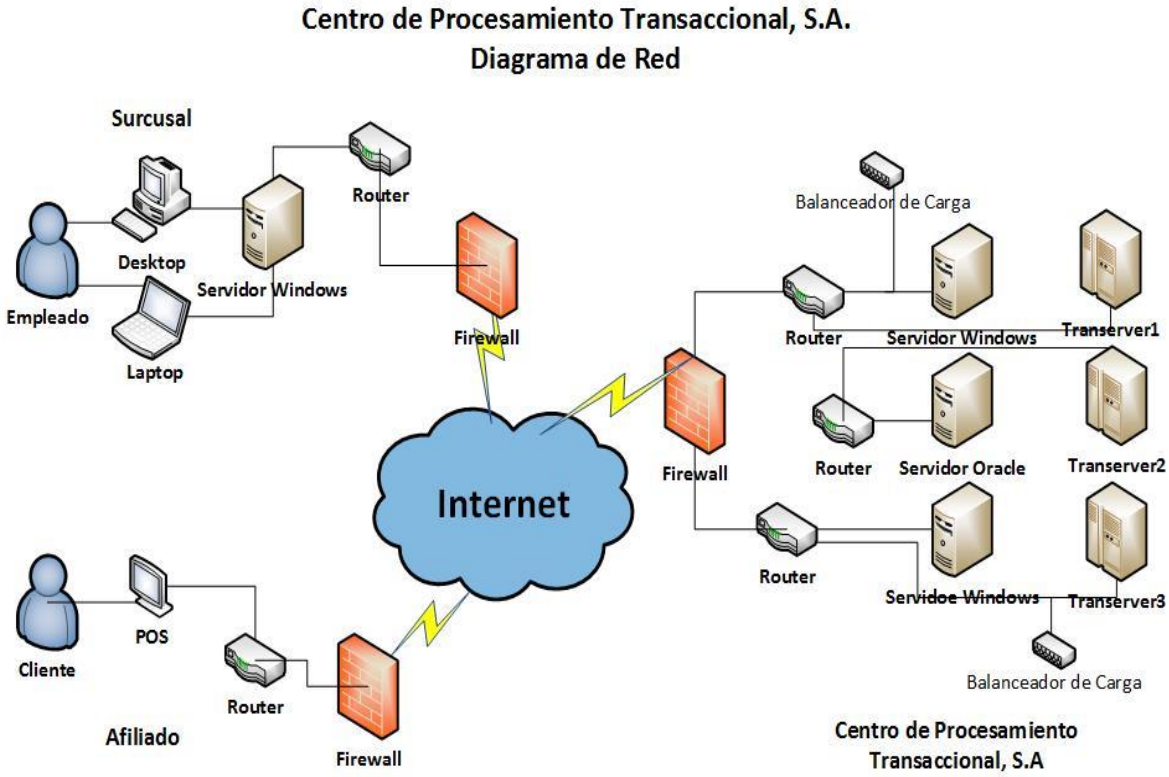
Tabla 2: Fuente suministrada por el Centro de Procesamiento Transaccional, S.A., 2014.

Actualmente la División de Tecnología está ubicado en el tercer piso del edificio principal y cuenta con el siguiente plano:



Gráfica 1: Fuente Centro de Procesamiento Transaccional, S.A., 2014.

EL Centro de Procesamiento Transaccional cuenta con una red distribuida entre las sucursales, sus clientes afiliados y el centro de procesamiento principal. Ver diagrama de red:



Gráfica 2: Fuente Centro de Procesamiento Transaccional, S.A., 2014.

Capítulo II

Conceptos Generales

2.1 Gobierno y Gestión de Tecnología de la Información

El gobierno de TI, uno de los ámbitos del gobierno corporativo, comprende el conjunto de tema tratados al considerar como se aplica la TI en la empresa.

Un gobierno corporativo efectivo concentra la pericia y experiencia individual y de grupo en áreas específicas, donde ellos puedan ser más efectivos. La tecnología de la información, considerada por mucho tiempo solo un facilitador de la estrategia de una organización, es ahora considerada como parte integral de esa estrategia. El gobierno de TI ayuda a alcanzar este factor crucial de éxito al desplegar de manera económica, eficiente y efectiva información segura y confiable, así como tecnología aplicada. Fundamentalmente, al gobierno de TI le incumben dos aspectos; que TI entregue valor al negocio y que los riesgos de TI sean gestionados[1].

La posibilidad de que una empresa disponga de una estructura institucional bien estructurada y con todos sus aspectos de gobernabilidad claros es poca, pero es menos común que el área de tecnología disponga de un gobierno de TI que pueda combinar sus esfuerzos para impulsar el desarrollo tecnológico y dar valor agregado.

El gobierno y la gestión están claramente diferenciados, ya que el gobierno permite que surja una situación en la que otros pueden gestionar sus tareas de forma eficaz. Como consecuencia, el Gobierno de TI y la Gestión de TI se deben trata como entidades independientes. La Gestión de Servicios de TI se puede

[1] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Gobierno de TI. *Manual de Preparación al Examen CISA 2012* (pp. 94). Estados Unidos de América: ISACA.

considerar parte de la Gestión de TI, por lo que el Gobierno de TI está dentro del dominio de la Gestión de la Información o de la empresa.

Aunque muchos marcos de trabajo están caracterizados como "marcos de Gobierno de TI", como COBIT o incluso ITIL, la mayor parte de ellos son en realidad marcos de gestión. Existen al menos un estándar para el Gobierno de TI[2].

2.2 Administración de la Continuidad del Negocio (Business Continuity Management, BCM).

Según el Instituto Británico para la Continuidad del Negocio (BCI, por sus siglas en ingles Business Continuiy Institute,), Business Continuity Management no es simplemente recuperación ante desastres, gestión de crisis, gestión de riesgos o recuperación tecnológica. No es simplemente una disciplina realizada por especialistas profesionales, sino un enfoque global de la actividad que integra un amplio espectro de actividades de gestión encaminadas al objetivo final de la organización[3].

[2] Bon Van, J., Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van der Veen, A. & Verheijen, T. (2008). Gobierno de TI. (Ed), *Fundamentos de la Gestión de Servicios de TI Basada en ITIL V3*. (pp. 10 – 11). Holanda: Van Haren Publishing. Recuperado de http://books.google.com.do/books?id=QHYs9yWDRsQC&pg=PA10&dq=gobierno+de+ti&hl=es&sa=X&ei=_lYaU4_XNYbQkQfwmoDYDQ&sqi=2&redir_esc=y#v=onepage&q=gobierno%20de%20ti&f=false

[3] Gaspar Martínez, J. (2004). Introducción. (Ed), *Planes de Contingencia - La Continuidad del Negocio en Las Organizaciones*. (pp XXVII). Madrid: Ediciones Díaz de Santos, S.A. Recuperado de http://books.google.com.do/books?id=K_UMxjjB5gUC&printsec=frontcover&dq=Administracion+de+la+continuidad+del+negocio&hl=es&sa=X&ei=EJ4aU8jaE42pkAevvIG4Cw&redir_esc=y#v=onepage&q=Administracion%20de%20la%20continuidad%20del%20negocio&f=false

Sin lugar a duda una adecuada Administración del Plan de Continuidad del Negocio, o ya conocido como BCM, alinea todos los procesos claves sin importar si corresponden a TI y los concentra en una sola guía de gestión dentro de la organización.

La Administración de la Continuidad del Negocio (BCM, por sus siglas en inglés) se considera una buena práctica para todos los temas de gestión de los recursos y forma parte esencial de un buen gobierno corporativo, por lo que se considera un ente estratégico y no simplemente como solamente un instrumento de recuperación.

En Resumen, Business Continuity Management es un proceso de dirección que identifica los impactos potenciales que amenazan a la organización y proporciona el marco adecuado para construir y reforzar la capacidad de dar una respuesta efectiva que salvaguarde los intereses, la imagen y el valor de las actividades realizadas por la misma[4].

[4] Gaspar Martínez, J. (2004). Introducción. (Ed), *Planes de Contingencia - La Continuidad del Negocio en Las Organizaciones*. (pp XXVII). Madrid: Ediciones Díaz de Santos, S.A. Recuperado de http://books.google.com.do/books?id=K_UMxjjB5gUC&printsec=frontcover&dq=Administracion+de+la+continuidad+del+negocio&hl=es&sa=X&ei=EJ4aU8jaE42pkAevvIG4Cw&redir_esc=y#v=onepage&q=Administracion%20de%20la%20continuidad%20del%20negocio&f=false

2.3 Plan de Recuperación ante Desastres (Disaster Recovery Plan, por sus siglas en ingles DRP).

Los planes de recuperación ante desastres (Disaster Recovery Plan, por sus siglas en ingles DRP) son actividades para gestionar temas de disponibilidad y restauraciones de las operaciones y servicios críticos en una organización.

DRP es un proceso continuo. Una vez que se ha definido la criticidad de los procesos de negocios, así como los servicios de TI de soporte, sistemas y datos, estos se revisan y revisitan periódicamente. Hay como mínimo dos resultados importantes de DRP:

- Cambios en la infraestructura de TI (servicios, redes, sistemas de almacenamiento de datos, etc.), cambios en procesos de soporte (aumentar la madurez), procedimientos y estructura organizativa (por ejemplo, nuevo personal de plantilla o nuevos roles). Estos cambios se combinan en programas que se expanden de tres cinco años, conocidos a menudo como estrategias de recuperación de desastres (DR) de TI.
- Los planes (Planes DR) desarrollados como parte de este proceso guiara la respuesta a incidentes desde simples emergencias hasta desastres mayores. Los planes van desde simples procedimientos a nivel de departamento a planes modulares de varias capas que cubren varias ubicaciones y líneas de negocio.

El objetivo principal del proceso DRP es responder a incidentes que puedan tener un impacto en personas y en la capacidad de operaciones de entregar bienes y servicios al mercado y de cumplir con los requerimientos regulatorios[5]. Todos estos temas de recuperación ante desastres involucran directamente temas del objetivo de punto de recuperación (Recovery Point Objetive, por sus siglas en ingles RPO) y objetivo de tiempo de recuperación (Recovery Time Objetive, por sus siglas en ingles RTO).

El **RTO** se determina tomando como base la perdida de datos aceptables en el caso de interrupción de las operaciones. Indica el tiempo mínimo posible en el que se pueden recuperar los datos. El **RPO** cuantifica efectivamente la cantidad permitida de perdida de datos en caso de interrupción. Resulta casi imposible recuperar los datos completamente. Aun después de ingresar los datos incrementales, algunos datos se encuentran perdidas aún se les refiere como datos huérfanos.

Ambos procesos se basan en parámetros de tiempo. Cuando menos tiempo se requiera, mayor serán los costos de estrategias de recuperación, es decir, si el RPO es en minutos (menor perdida posible aceptable de datos), la réplica de datos en espejo (mirroring) o la réplica en tiempo real deben implementarse como

[5] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Planificación de Recuperación en Caso de Desastre (DRP). *Manual de Preparación al Examen CISA 2012* (pp. 326). Estados Unidos de América: ISACA.

estrategias de recuperación. Si el RTO es en minutos, debe utilizarse una combinación de hot site, servidores de repuesto dedicados y clustering[6].

2.4 Regulaciones y Mejores Prácticas de la Continuidad.

El desarrollo y la gestión de planes de continuidad de negocios han convertido en tendencias la utilización y apego de las mejores prácticas mundiales para su adecuada implementación.

Acompañando a las mejores prácticas existen amplias regulaciones para diferentes campos o sectores los cuales hacen cumplir ciertos lineamientos para la protección de los activos de una empresa.

2.4.1 Políticas y Procedimientos.

Las políticas y procedimientos reflejan la orientación y dirección de la gerencia en el desarrollo de controles sobre los sistemas de información, recursos relacionados y procesos del departamento de SI[7].

El propósito de las políticas en una organización, es simplificar la burocracia administrativa y ayuda a la organización a obtener utilidades. Una política tiene

[6] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Objetivo de Punto de Recuperación (RPO) y Objetivo de Tiempo de Recuperación (RTO). *Manual de Preparación al Examen CISA 2012* (pp. 326 - 327). Estados Unidos de América: ISACA.

[7] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Políticas y Procedimientos. *Manual de Preparación al Examen CISA 2012* (pp. 104). Estados Unidos de América: ISACA.

razón de ser, cuando contribuye directamente a que las actividades y procesos de la organización logren sus propósitos[8].

Los procedimientos son pasos más detallados que se definen y se documentan para implementar las políticas. Deben derivarse de la política madre e implementar el espíritu (la intención) del enunciado de la política[9].

Una política de continuidad del negocio es un documento aprobado por la alta gerencia que define la magnitud y el alcance del esfuerzo de continuidad del negocio (un proyecto o un programa continuo) dentro de la organización[10].

Definitivamente las políticas y procedimientos son documentaciones de alto nivel, aprobados por la organización, que se deben de documentar de una forma clara y precisa para que de esta forma pueda ser entendida correctamente por cada uno de los involucrados de una empresa.

2.4.2 Estándares y Marcos de Referencias.

Un estándar, o como muchos llaman mejores prácticas o marcos de referencia, es un nivel de práctica profesional aceptado, apropiado para la población a la que se

[8] Álvarez Torres, M. (1996). Las Políticas. (Ed), *Manual para elaborar Manuales de Políticas y Procedimientos*. (pp 27). México: Panorama Editorial, S.A. Recuperado de http://books.google.com.do/books?id=YnhdFdUDnVIC&printsec=frontcover&dq=politicas+y+procedimientos&hl=es&sa=X&ei=_3UeU7S-I4mUkQez_YHQDQ&redir_esc=y#v=onepage&q&f=false

[9] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Políticas y Procedimientos. *Manual de Preparación al Examen CISA 2012* (pp. 106). Estados Unidos de América: ISACA.

[10] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Políticas de Continuidad del Negocio. *Manual de Preparación al Examen CISA 2012* (pp. 131). Estados Unidos de América: ISACA.

dirige, con recursos disponibles que permiten aplicare y que es observable medible, conseguible y deseable[11].

Como parte del cumplimiento de un plan de continuidad de negocio es importante alinearse a las mejores prácticas mundialmente aceptadas, las cuales soportar los diferentes procesos de desarrollo y mejoramiento continuo de los planes. Dentro de los regularmente utilizados para temas de la continuidad, seguridad de la información y la protección de los activos de las empresas, podemos enlistar:

- Agencia Nacional de Estados Unidos contra Incendios (National Fire Protection Association, NFPA).
- Instituto de Continuidad del Negocio (Business Continuity Institute, BCI).
- Instituto Internacional de Recuperación en Caso de Desastres (Disaster Recovery Institute International, DRII).
- TIER´s para la estandarización de los Centros de Cómputos.
- Norma COBIT.
- Normas Certificables BS 25999-2 e ISO 22301.
- Instituto Nacional de Estándares y Tecnología de los Estados Unidos (US National Institute of Standards and Technology).
- Entre otras documentaciones que dan recomendaciones claves para los procesos de continuidad y seguridad.

[11] Oteo Ochoa, L. (2006). Estándares – Una aproximación al concepto de Estándar. (Ed), *Gestión Clínica: Desarrollo e Instrumentos.* (pp 206-207). Ecuador: Ediciones Díaz de Santos. Recuperado de http://books.google.com.do/books?id=o_TE96PdcdQC&pg=PA206&dq=que+es+un+estandar&hl=es&sa=X&ei=24MeU4b7JNHwkQfprIHABA&redir_esc=y#v=onepage&q=que%20es%20un%20estandar&f=false

Algunas organizaciones ya han comenzado a adoptar las mejores practica para entidades tanto independientes como específicas de la industria y agencias regulatoria[12], de esta forma poder alcanzar ciertos niveles de madurez en el desarrollo de prácticas de continuidad del negocio.

2.4.3 Beneficios e Importancias de un Plan de Continuidad.

Es de suma importancia el disponer de un plan de continuidad para el negocio aumentando los beneficios en la continuidad operativa de la organización. Si nos vamos al origen de poder disponer de un BCP encontraremos la necesidad de mantener operando o poder recuperar los servicios ante cualquier desastre en la empresa.

Sin lugar a duda disponer de un plan de continuidad de negocio es de suma importancia tanto para el negocio como para el área de TI, lo que ayuda desde la identificación de los potenciales riesgos que pudieran afectar la continuidad de las operaciones, como la identificación de los sistemas y aplicativos claves para el negocio y su infraestructura, disponer de los procedimientos necesarios para reponerse en caso de crisis y mantener un enfoque de pruebas y mantenimientos de los diferentes procedimientos existentes.

[12] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Mejores Prácticas en la Gestión de Continuidad del Negocio. *Manual de Preparación al Examen CISA 2012* (pp. 140). Estados Unidos de América: ISACA.

Por lo tanto, el BPC/DRP del sistema de información es un componente principal de la estrategia general de continuidad del negocio y recuperación en caso de desastres de una organización[13].

2.5 Gestión de la Seguridad de los Activos.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable[14].

Dentro de los elementos tomados más en cuenta para la protección de los activos y la privacidad está el poder establecer una base clara para la gestión efectiva de la seguridad de la información.

Los objetivos de seguridad para satisfacer los requerimientos del negocio de las organizaciones, incluyen temas como:

- Asegurar la continua disponibilidad de los sistemas de información.
- Asegurar la integridad de la información en sus sistemas informáticos.
- Preservar la confidencialidad de los datos sensibles mientras están almacenados y en tránsito.
- Asegurar el cumplimiento de leyes, regulaciones y estándares aplicables.

[13] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Planeación de Continuidad del Negocio de SI. *Manual de Preparación al Examen CISA 2012* (pp. 129). Estados Unidos de América: ISACA.
[14] Aguilera, P. (2000). Aproximación al Concepto de Seguridad en Sistemas de Información. *Seguridad Informática* (pp. 9). España: Editorial Editex, S.A. Recuperado de http://books.google.com.do/books?id=dXFcvBCHJzAC&pg=PA43&dq=Seguridad+de+activos+de+TI&hl=es&sa=X&ei=qM0fU9GYHonvkQeg6ICwDQ&redir_esc=y#v=onepage&q=Seguridad%20de%20activos%20de%20TI&f=false

- Asegurar el cumplimiento de los requerimientos de confianza.
- Asegurar que los datos sensibles están bien protegidos cuando se almacenan y cuanto están en tránsito[15].

Todos estos procesos de protección y gestión de la seguridad de la información involucran un detallado y preciso inventario de los activos claves de la organización. Este inventario mantiene asociado el desarrollo de una clasificación de las informaciones y con esto un esquema para la asignación de los niveles de sensibilidad de la misma.

[15] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Importancia de la Gestión de la Seguridad de la Información. *Manual de Preparación al Examen CISA 2012* (pp. 355). Estados Unidos de América: ISACA.

Capítulo III

Gestión de Riesgo

3.1 Concepto de Riesgo.

La palabra riesgo viene del latín *risicare*, que significa atreverse o transitar por un sendero peligroso. En realidad tiene un significado negativo, relacionado con peligro, daño, siniestro o perdida. Sin embargo, el riesgo es parte inevitable de los procesos de toma de decisiones en general y de los procesos de inversión en particular. El beneficio que se pueda obtener por cualquier decisión o acción que se adopte, debe asociarse necesariamente con el riesgo inherente a dicha decisión o acción[16].

Existen otras definiciones de riesgo los cuales determinan este como la posibilidad de la ocurrencia de un evento que pueda afectar cualquiera de los recursos de una organización.

Los riesgos de negocios son la probabilidad de aquellas amenazas que pueden tener un impacto negativo sobre los activos, procesos u objetivos de un negocio u organización especifica. La naturaleza de estas amenazas puede ser financiera, regulatoria u operacional, y puede surgir como resultado de la interacción del negocio con su ambiente, o como resultado de las estrategias, sistemas, así como tecnología, procesos, procedimientos e informaciones particulares usados por el negocio[17].

---

[16] De Lara Haro, A. (2005). Antecedentes de la Administración del Riesgo. *Medición y Control de Riesgo Financiero* (pp. 13). México: Editorial Limusa, S.A. Recuperado de http://books.google.com.do/books?id=PrQ-vTEWLqoC&printsec=frontcover&dq=que+es+el+riesgo&hl=es&sa=X&ei=taEgU7DCIYykkQes2YHwDQ&redir_esc=y#v=onepage&q=que%20es%20el%20riesgo&f=false

[17] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Análisis de Riesgo. *Manual de Preparación al Examen CISA 2012* (pp. 49). Estados Unidos de América: ISACA.

El riesgo de TI es un tipo de riesgo de negocio, específicamente el riesgo de negocio asociado con el uso, la propiedad, la operación, la participación, la influencia y la adopción de TI dentro de la empresa. Estos riesgos consisten básicamente en los eventos relacionados con TI que potencialmente podrían impactar al negocio[18].

3.2 Gestión de la Continuidad del Negocio (Business Continuity Management, BCM) y Administración de Riesgo.

Una adecuada gestión de la continuidad asocia un sinnúmero de temas importantes que alinean a las empresas para cumplir con las tareas necesarias en cuenta a su continuidad de negocio y/o recuperaciones recursos de TI, aquí es donde entra la evaluación y administración del riesgo.

Sin lugar a duda uno de los pasos para el desarrollo de un plan de continuidad de negocio o recuperación ante desastres y su adecuada gestión o Business Continuity Management (BCM) es el poder establecer una evaluación de riesgo bien detallada que incluya temas como; procesos críticos, los sistemas y equipos, la infraestructura de TI y cualquier tema crítico para el adecuado funcionamiento de las operaciones de la empresa.

En un plan de continuidad de negocio se realizan los cálculos de los riesgos de forma cualitativa; terminando así valores al impacto de las amenazas y su

[18] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Análisis de Riesgo. *Manual de Preparación al Examen CISA 2012* (pp. 49). Estados Unidos de América: ISACA.

probabilidad de ocurrencia, y cuantitativamente; asignando valores monetarios para el impacto y un monto de perdida en la ocurrencia de la probabilidad.

El objetivo de la Gestión de la Continuidad de Servicios de TI es ayudar a toda la Gestión de Continuidad del Negocio (BCM) garantizando toda la infraestructura de TI y sus servicios necesarios[19], y con todo esto la administración del riesgo es quien colaborara directamente con la pronta gestión de cualquier ente que pueda afectar la organización en todos sus aspectos.

3.3 Análisis y Evaluación de Riesgo.

Un análisis de riesgo es un proceso de calidad total o mejora continua, que busca estimar las probabilidades de que se presenten acontecimientos indeseables, permitiendo medir la magnitud de dichos impactos negativos en el transcurso de ciertos intervalos específicos de tiempo[20].

Para tecnología de la información una evaluación de riesgos identifica los recursos asociados a los sistemas de información, su comprometimiento con los objetivos de negocio, sus amenazas y vulnerabilidades y otros componentes preventivas y correctivas.

---

[19] itSMF International (2005). Gestión de la Continuidad de Servicios de TI. *Fundamentos de Gestión de Servicios de TI Basado en ITIL* (pp. 159). Holanda: Van Haren Publishing. Recuperado de http://books.google.com.do/books?id=nmw4zEMcyhsC&pg=PT171&dq=Continuidad+de+negocios&hl=es&sa=X&ei=xbogU7mtJOnN0AHs54Fw&redir_esc=y#v=onepage&q=Continuidad%20de%20negocios&f=false

[20] Martínez Ponce de León, J., (2002). Los Análisis de Riesgos (Marco Teórico). *Introducción al Análisis de Riesgos* (pp. 23). México: Editorial Limusa, S.A. Recuperado de http://books.google.com.do/books?id=UZOzKXcpfJQC&pg=PA23&dq=Analisis+y+evaluacion+de+riesgo&hl=es&sa=X&ei=-r8gU7rvHJK10AGj-oCgAQ&redir_esc=y#v=onepage&q=Analisis%20y%20evaluacion%20de%20riesgo&f=false

Los resultados de la evaluación de riesgos, y el BIA se incorporan a la estrategia de continuidad de negocio de SI, la cual describe la tecnología principal y los principios que sirven de base a la protección y recuperación de SI, así como la directriz para implementar la tecnología y los principios[21].

La gran mayoría de las metodologías de análisis de riesgos, utilizadas en los Estados Unidos, son diseñadas por la EPA (Enviromental Protection Agency), la NIOSH (National Institute for Occupational Safaty and Health), la OSHA (Occupational Safety and Health Administration) y el DHHS (Committee to Coordinate Environmental and Related Programs), y se podríamos decir que todas estas entidades han desarrollado sus programas de evaluaciones de riesgos para 1985 y son contemporáneas, manteniendo el mismo enfoque de evaluaciones y derivando criterios y estándares que han sido convirtiéndose en normas y reglamentos para los diferentes sectores de la industria[22].

3.4 Tipos de Análisis de Riesgos.

Como parte de los procesos de evaluación y análisis de riesgos se realizan categorizaciones y segmentaciones para los diferentes tipos de estudios realizados a los riesgos. Tendiendo claro esto, se presentan los cuatro renglones claves para los tipos de análisis de riesgos. Dentro de estos están:

[21] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Planeación de la Continuidad del Negocio de SI. *Manual de Preparación al Examen CISA 2012* (pp. 130). Estados Unidos de América: ISACA.

[22] Martínez Ponce de León, J., (2002). Metodología General para los Análisis de Riesgos (Marco Teórico). *Introducción al Análisis de Riesgos* (pp. 83). México: Editorial Limusa, S.A. Recuperado de http://books.google.com.do/books?id=UZOzKXcpfJQC&printsec=frontcover&dq=analisis+de+riesgos&hl=es&sa=X&ei=IwYhU6_kEobLkQf_94GIBQ&sqi=2&redir_esc=y#v=onepage&q&f=false

Riesgos Humanos: Estos riesgos comúnmente van asociamos a temas como:

- Actos accidentales: estos van asociados con accidentes de trabajo, enfermedades y epidemias, pérdidas de hombres claves y cualquier otro tema parecido a estos.
- Actos culposos: sabotaje, espionaje industrial, fraude, malversación de fondos, estafas, falsificación, robos, daños a la producción, calumnias, infidelidad y traspaso de documentos confidenciales.
- Actos negligentes: mala concepción de un producto o servicio, mala calidad de trabajo, pérdida de documentos, entro otros.
- Actos Subjetivos: tensión, desmotivación, y cambio de actitud, concentrar información y poder de decisión, inestabilidad y deserción de personal capacitado, demandas legales – laborales y/o huelgas.

Riesgos Elementos Físicos: Estos perciben todos los temas de físicos que puedan afectar la infraestructura del negocio, entre lo más comunes tenemos:

- Cataclismos: terremotos, inundaciones, tormentas y huracanes, erupciones volcánicas, maremotos, deslizamientos de tierras.
- Malas condiciones naturales: sequías, exceso de lluvias, granizada, rayos.
- Fallas de materiales y equipos: avería de maquinarias, explosión, incendio, caída de objetos, contaminación, fallas técnicas, choques de vehículos, roturas de techos-paredes, etc.

Para estos muchas empresas y personas quizás los consideran como difíciles de ocurrencia pero si suceden pueden acabar con nuestra organización (edificios, casas, vehículos, cosechas y activos en general) de una forma rápida.

Riesgos Financieros: En esta categoría ubicamos todos aquellos riesgos que nos pueden provocar pérdidas contables o financieras. Por ejemplo: aumento de los costos de producción, liquidez o falta de capital de trabajo, quiebra de clientes o proveedores de nuestra empresa, devaluaciones, aumento de impuestos y tardas para nuestros productos, entre otros.

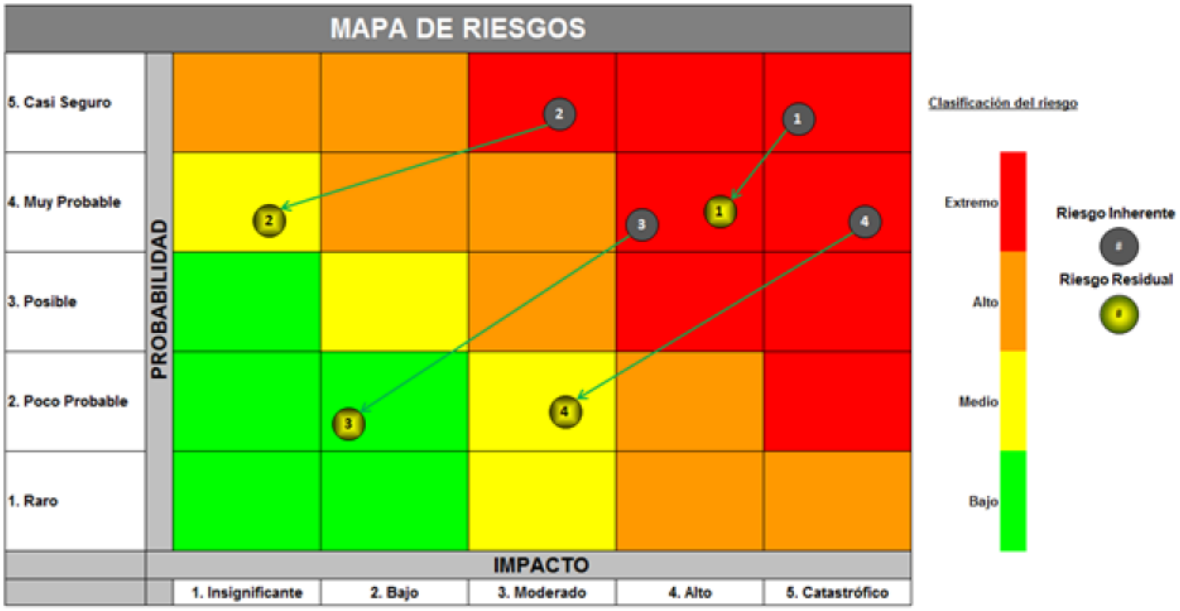
Riesgos Técnico: entre estos riesgos incluimos elementos como; obsolescencia del equipo y maquinaria, Deterioro físico y desgaste de activos fijos, Baja en la capacidad productiva del recurso físico, plagas y enfermedades que bajen rendimientos productivos, Condiciones climáticas adversas, Pérdidas y deterioro de producto terminado, Mala calidad de insumos y materias primas[23].

3.5 Evaluación de Riesgo de la Empresa.

Dentro de los procesos de revisiones al Centro de Procesamiento Transaccional, S.A., se realizaron deferentes evaluaciones para identificar los activos críticos y las potenciales amenazas y vulnerabilidades que pueden paralizar las operaciones críticas del negocio.

[23] Castellón Mora, R., (1995). Tipos de Riesgos. Clasificación. *Administración de Empresas Cooperativas III – Análisis de Riesgos* (pp. 83). Costa Rica: CENECOOP, S.A. Recuperado de http://www.campus.co.cr/educoop/docs/md/caec/caec_ii_unidad_03.pdf

Para nuestra valoración de los riesgos utilizaremos una matriz de riesgo de colores que represente el apetito del riesgo, este contiene escalas de probabilidad e impacto para el cálculo de los riesgos inherente y residual:



Gráfica 3: Mapa de Riesgos – KPMG

Los resultados identificados, bajo la esquematización de este recuadro se estarán expuestos en la identificación de amenazas y vulnerabilidades.

3.5.1 Identificación y Clasificación de los Activos.

Para la gestión de activos en el Centro de Procesamiento Transaccional, S.A. se realizó un inventario detallado de los activos de información, para así determinar el nivel de protección al que estará sujeto. Los activos inventariados, clasificándolo por tipo fueron:

Centro de Procesamiento Transaccional, S.A. Inventario de Activos – 2014					
Nombre Activo	**Marca / Modelo**	**Serie**	**Ubicación**	**Unidad Responsable**	**Persona Responsable**
CPU	Dell OPTIPLEX 790	BFTG231	3er Piso	Mesa de ayuda	Ariel Infante
CPU	Dell OPTIPLEX 790	D3XMVC4	3er Piso	Tecnología	Alicia Ortiz
CPU	Dell OPTIPLEX 790	2Z2GH984	3er Piso	Tecnología	Alicia Ortiz
CPU	Dell OPTIPLEX 790	97TOFF12	3er Piso	Tecnología	Jose Milano
CPU	Dell OPTIPLEX 790	HCMAS105	3er Piso	Tecnología	Jose Milano
CPU	Dell OPTIPLEX 790	DRG8641	3er Piso	Proc. Transacc.	Luis Urbaez
CPU	Dell GX-520	C3MXJ71	3er Piso	Proc. Transacc.	Luis Urbaez
CPU	Dell GX-520	H7V6231	3er Piso	Proc. Transacc.	Diolis Perez
CPU	Dell GX-520	8YRG231	3er Piso	Proc. Transacc.	Diolis Perez
CPU	Dell OPTIPLEX 790	6ZOBVR894	3er Piso	Proc. Transacc.	Fausto Mata
CPU	Dell OPTIPLEX 790	GHH2E	3er Piso	Proc. Transacc.	Fausto Mata
CPU	HP D530	MXJ5420CLT	3er Piso	Proc. Transacc.	Fausto Mata
CPU	Dell GX-520	2X2BQ51	3er Piso	Proc. Transacc.	Fausto Mata
CPU	Dell GX-520	26D1B61	3er Piso	Proc. Transacc.	Fausto Mata
CPU	Dell OPTIPLEX 790	JSRBV98	3er Piso	Tecnología	Eric Mueses
CPU	Dell OPTIPLEX 790	9DDV45203	3er Piso	Tecnología	Luis Cuevas
CPU	Dell OPTIPLEX 790	89711MNB	3er Piso	Tecnología	Romero Santos

CPU	Dell OPTIPLEX 790	2W356RTG	3er Piso	Tecnología	Romero Santos
CPU	Dell OPTIPLEX 790	8RV1MM7	3er Piso	Tecnología	Ivan Cruz
CPU	Dell OPTIPLEX 790	42TXUY9	3er Piso	Tecnología	Ivan Cruz
CPU	HP Compap	USH63900NC	3er Piso	Tecnología	Ivan Cruz
CPU	Dell OPTIPLEX 790	3PZ2ZX864	3er Piso	Tecnología	Jesus Nuñez
CPU	Dell OPTIPLEX 790	4068G215H	3er Piso	Tecnología	Jesus Nuñez
CPU	Dell OPTIPLEX 790	6JGHGH813	3er Piso	Tecnología	Jesus Nuñez
CPU	Dell OPTIPLEX 790	28JWWF45	3er Piso	Tecnología	Jesus Nuñez
CPU	Dell OPTIPLEX 790	2PQFH541	3er Piso	Tecnología	Joaquin Alfau
CPU	Dell OPTIPLEX 790	HP67TR78	3er Piso	Tecnología	Joaquin Alfau
CPU	Dell OPTIPLEX 790	76BVCV87	3er Piso	Tecnología	Joaquin Alfau
CPU	Dell OPTIPLEX 790	FONZDF1	3er Piso	Tecnología	Joaquin Roque
CPU	Dell OPTIPLEX 790	67TOMK19	3er Piso	Tecnología	Jose Almonte
CPU	Dell OPTIPLEX 790	C2KMWCW	3er Piso	Tecnología	Jose Almonte
CPU	Dell OPTIPLEX 790	GFPQZZC8	3er Piso	Tecnología	Jose Manuel
CPU	Dell GX-520	6NG6641	3er Piso	Proc. Transacc.	Junior Gomez
CPU	Dell OPTIPLEX 790	55KTPO2	3er Piso	Tecnología	Leandro Luis
CPU	Dell OPTIPLEX	1Z7KGVD9	3er Piso	Tecnología	Martha

	790				
CPU	Dell OPTIPLEX 790	7YSB4WQ5	3er Piso	Tecnología	Martha
CPU	Dell OPTIPLEX 790	29BF5G4	3er Piso	Tecnología	Martha
CPU	Dell OPTIPLEX 790	960SS71	3er Piso	Mesa de ayuda	Miguel Artiles
CPU	Dell OPTIPLEX 790	3HCWW66	3er Piso	Tecnología	Rey Perez
CPU	Dell OPTIPLEX 790	9DZ154DF	3er Piso	Tecnología	Rey Perez
CPU	Dell OPTIPLEX 790	5225XSW	3er Piso	Tecnología	Rey Perez
CPU	Dell OPTIPLEX 790	CNXJHFDS8	3er Piso	Tecnología	Vacante
CPU	Dell OPTIPLEX 790	CNPMMBV6	3er Piso	Tecnología	Vacante
CPU	Dell OPTIPLEX 790	DTRXXCV9	3er Piso	Tecnología	Vacante
CPU	Dell OPTIPLEX 790	DWMBRT9	3er Piso	Tecnología	Vacante
CPU	Dell OPTIPLEX 790	GT676548	3er Piso	Tecnología	Vacante
CPU	Dell OPTIPLEX 790	J1NZ45HJ	3er Piso	Tecnología	Vacante
CPU	Compap cq2953	RFGZ400R	3er Piso	Mesa de ayuda	Vacante
CPU	Dell GX-520	8QTXJ71	3er Piso	Mesa de ayuda	Vacante
CPU	Dell GX-520	B2X5231	3er Piso	Mesa de ayuda	Vacante
CPU	Dell GX-520	BNH6641	3er Piso	Proc. Transacc.	Vacante
CPU	Dell OPTIPLEX 790	3TKXGF8	3er Piso	Tecnología	Carlos Duran
CPU	Dell OPTIPLEX	6QZDYT8	3er Piso	Tecnología	Carlos Duran

	790				
CPU	HP D530	MX291188GF	3er Piso	Tecnología	Carlos Duran
CPU	Dell OPTIPLEX 790	HN68T955	3er Piso	Tecnología	Carlos Duran
CPU	Dell GX-520	30GFG8	3er Piso	Tecnología	Carlos Duran
CPU	Dell GX-520	2BY53KK	3er Piso	Tecnología	Carlos Duran
CPU	Dell GX-520	DZO4RE8	3er Piso	Tecnología	Carlos Duran
CPU	Compap cq2953	S-0871	3er Piso	Tecnología	Iván Cruz
CPU	Dell OPTIPLEX 790	19BIX81BV	3er Piso	Tecnología	Luis Mota
CPU	Dell OPTIPLEX 790	6Y2599M	3er Piso	Tecnología	Victor Álvarez
CPU	Dell OPTIPLEX 790	4JTSSAHG	3er Piso	Tecnología	Victor Álvarez
DameWare Devel.	DameWare	64530	3er Piso	Seg. de Sistema	Pedro Pared
Evertec	Oracle	S/N	3er Piso	Seg. de Sistema	Cindia Espinal
Fire Wall	Cisco Pix-516	88807263463	3er Piso	Tecnología	Carlos Duran
Fire Wall	Cisco Pix-516	44406186299	3er Piso	Tecnología	Carlos Duran
Fire Wall	Cisco Pix-516	88810410001	3er Piso	Tecnología	Carlos Duran
Fire Wall	Cisco Pix-516	88810540258	3er Piso	Tecnología	Carlos Duran
Fire Wall	Cisco Pix-516	88806251987	3er Piso	Tecnología	Carlos Duran
Fire Wall	Cisco Pix-516	JMX14200158	3er Piso	Tecnología	Carlos Duran
Fire Wall	Cisco 5505e	JMX1420YT89	3er Piso	Tecnología	Carlos Duran
Fire Wall	Cisco 5505e	JMX14284RE4	3er Piso	Tecnología	Carlos Duran
Fire Wall	Cisco 5505e	JMX14283389	3er Piso	Tecnología	Carlos Duran
Fire Wall	Mcafee SG-720	0602993	3er Piso	Tecnología	Carlos Duran
Fire Wall	Mcafee SG-720	0602994	3er Piso	Tecnología	Carlos Duran
Fire Wall	Mcafee SG-720	0602995	3er Piso	Tecnología	Carlos Duran
Fire Wall	Cisco SG-710	06013600398FSDF	3er Piso	Tecnología	Leandro Luis
Fire Wall	Cisco Pix-516	88802254896	3er Piso	Tecnología	Victor Álvarez
Firewall	Cisco SG-720	JMXG78	3er Piso	Seg. de Sistema	Pedro Pared
Firewall	Cisco SG-720	JMXG79	3er Piso	Seg. de Sistema	Pedro Pared
Firewall	Cisco SG-720	JMX60RRT	3er Piso	Seg. de Sistema	Pedro Pared

Firewall	Cisco Pix-516	JMXG69	3er Piso	Seg. de Sistema	Cindia Espinal
Firewall	Cisco Pix-516	JMXG72	3er Piso	Seg. de Sistema	Marcos Perez
Firewall	Cisco Pix-516	JMXG73	3er Piso	Seg. de Sistema	Marcos Perez
Firewall	Cisco Pix-516	JMXG70	3er Piso	Seg. de Sistema	Samuel Perez
Firewall	Cisco Pix-516	JMXG71	3er Piso	Seg. de Sistema	Samuel Perez
Firewall	Cisco Pix-516	JMXG76	3er Piso	Seg. de Sistema	Sol Sanchez
Firewall	Cisco SG-720	JMXG77	3er Piso	Seg. de Sistema	Sol Sanchez
Firewall	Cisco Pix-516	JMXG74	3er Piso	Seg. de Sistema	Omar Abrue
Firewall	Cisco Pix-516	JMXG75	3er Piso	Seg. de Sistema	Omar Abrue
Gestión Informática	E-CASE	S/N	3er Piso	Seg. de Sistema	Pedro Pared
Impresora	HP D-3050	CNO1DFD28U	3er Piso	Tecnología	Carlos Duran
Imp. Cheques	EPSON tm-u295p	CKK007895G1	3er Piso	Tecnología	Jochy Santos
Laptop	IBM t-61	L3-BH748	3er Piso	Tecnología	Alicia Ortiz
Laptop	Dell 6400	HLGYXVF8	3er Piso	Tecnología	Jesus Nuñez
Laptop	Dell 6400	45BBQW82	3er Piso	Tecnología	Joaquin Alfau
Laptop	HP E-5420	DKZNB45	3er Piso	Tecnología	Jose Almonte
Laptop	Dell E4300	15LTR84	3er Piso	Tecnología	Jose Manuel
Laptop	Dell D-850	FMTFJKHG8	3er Piso	Tecnología	Martha
Laptop	HP Compap	CNF440BC21	3er Piso	Tecnología	Rey Perez
Laptop	Dell Inspiron 1525	2W4WWM4	3er Piso	Tecnología	Carlos Duran
Laptop	Dell Inspiron 1525	HN341	3er Piso	Tecnología	Carlos Duran
Laptop	Dell Inspiron 1525	OU8082	3er Piso	Tecnología	Carlos Duran
Laptop	Dell Inspiron 1525	JW71GF8	3er Piso	Tecnología	Carlos Duran
Laptop	IBM T400	L3-AKM9F0208	3er Piso	Tecnología	Leandro Luis
Loglogic	LX-510	S/N	3er Piso	Tecnología	Romero Santos
Loglogic	DS-2010	COO15932015	3er Piso	Tecnología	Romero Santos
Loglogic	TS-3010	COO10858545	3er Piso	Tecnología	Vacante
Microsoft	Microsoft	68868	3er Piso	Seg. de Sistema	Omar Nuñez
Monitor	Dell 1912H	T-0046B	3er Piso	Tecnología	Luis Mota

Monitor	Sharp Dobby 710HG	001854210	3er Piso	Seg. de Sistema	Pedro Pared
Monitor	Sharp Dobby 710HG	001865810	3er Piso	Seg. de Sistema	Pedro Pared
Monitor	Sharp Dobby 710HG	001864718	3er Piso	Seg. de Sistema	Pedro Pared
Monitor	Sharp Dobby 710HG	001858211	3er Piso	Seg. de Sistema	Pedro Pared
Monitor	Dell 1912H	0-3AV-00P9	3er Piso	Proc. Transacc.	Luis Urbaez
Monitor	Dell 1912H	CN--64171	3er Piso	Proc. Transacc.	Luis Urbaez
Monitor	Dell 1912H	CN-OHX-DL	3er Piso	Proc. Transacc.	Diolis Perez
Monitor	Sony SDM-X75FS	S/N	3er Piso	Seg. de Sistema	Samuel Perez
Monitor	Sony SDM-X75FS	S/N	3er Piso	Seg. de Sistema	Samuel Perez
Monitor	Compap LV2001Q	M-100H	3er Piso	Tecnología	Jesus Nuñez
Monitor	Compap LV2001Q	942BB58	3er Piso	Proc. Transacc.	Junior Gomez
Monitor	Compap LV2001Q	GNN841	3er Piso	Proc. Transacc.	Junior Gomez
Monitor	Dell 1912H	T-0058T	3er Piso	Tecnología	Luis Mota
Monitor	Dell 1912H	S/N	3er Piso	Tecnología	Luis Mota
Monitor	Dell 1912H	SN-OCV464	3er Piso	Tecnología	Luis Mota
Monitor	Sony SDM-X75FS	S/N	3er Piso	Seg. de Sistema	Sol Sanchez
Monitor	Sony SDM-X75FS	S/N	3er Piso	Seg. de Sistema	Omar Abrue
Monitor 17 LCD	Dell S2340L	CN--83B-MN15	3er Piso	Tecnología	Alicia Ortiz
Monitor 17 LCD	Dell 1912H	CN-4V-S45C	3er Piso	Tecnología	Jose Milano
Monitor 17 LCD	Dell S2340L	52S-POQR	3er Piso	Tecnología	Jose Milano
Monitor 17 LCD	Dell S2340L	CN-O-NB10	3er Piso	Tecnología	Jose Milano
Monitor 17 LCD	Dell S2340L	76-IO12	3er Piso	Seg. de Sistema	Marcos Perez
Monitor 17 LCD	Dell S2340L	MY-09E-PO81	3er Piso	Seg. de Sistema	Marcos Perez
Monitor 17 LCD	Dell S2340L	C78OP	3er Piso	Tecnología	Jochy Santos
Monitor 17 LCD	Dell S2340L	CN-OT776R29AS	3er Piso	Tecnología	Jochy Santos
Monitor 17 LCD	Dell S2340L	4180-739-WE45	3er Piso	Tecnología	Eric Palmer

Monitor 17 LCD	Dell 1912H	CN-O8-ZX48	3er Piso	Tecnología	Joaquin Alfau
Monitor 17 LCD	Dell S2340L	8-64180-83R-II884	3er Piso	Tecnología	Joaquin Alfau
Monitor 17 LCD	Dell 1912H	S/N	3er Piso	Tecnología	Jose Manuel
Monitor 17 LCD	Dell S2340L	N-OD5428O48	3er Piso	Tecnología	Jose Silva
Monitor 17 LCD	Dell S2340L	83B-HG84	3er Piso	Tecnología	Leandro Luis
Monitor 17 LCD	Dell S2340L	CN-OY46	3er Piso	Tecnología	Martha
Monitor 17 LCD	Dell S2340L	OG34OH-1	3er Piso	Tecnología	Rey Perez
Monitor 17 LCD	Dell S2340L	CN-ORNM	3er Piso	Tecnología	Victor Alvarez
Monitor 17 LCD	Dell S2340L	C-6CM-AS85	3er Piso	Tecnología	Victor Alvarez
Monitor 17 LCD	Dell S2340L	72-058-XC45	3er Piso	Tecnología	Victor Alvarez
Monitor 17 LCD	Dell S2340L	2TR	3er Piso	Tecnología	Romero Santos
Monitor 17 LCD	Dell S2340L	64180-9C8-2WE4	3er Piso	Tecnología	Romero Santos
Monitor 17 LCD	Dell S2340L	CN-OG3003EW	3er Piso	Tecnología	Romero Santos
Monitor 20 LCD	Dell 1912H	S/N	3er Piso	Tecnología	Alicia Ortiz
Monitor 20 LCD	Dell 1912H	MXQW	3er Piso	Tecnología	Jesus Nuñez
Monitor 20 LCD	Dell 1912H	M-46634-6C4-3T15	3er Piso	Tecnología	Jose Almonte
Monitor 20 LCD	Dell 1912H	S/N	3er Piso	Tecnología	Martha
Monitor 20 LCD	Dell 1912H	CN-OFI82	3er Piso	Tecnología	Rey Perez
Monitor 22 LCD	Dell 1912H	CN-O80P-1SAG8	3er Piso	Tecnología	Joaquin Alfau
Monitor 22 LCD	Dell 1912H	S/N	3er Piso	Mesa de ayuda	Elvis Mejia
Monitor 22 LCD	Dell 1912H	64180-93P-1QGL	3er Piso	Mesa de ayuda	Elvis Mejia
Monitor 22 LCD	Dell 1912H	93P-QEL	3er Piso	Mesa de ayuda	Elvis Mejia
Monitor 22 LCD	Dell 1912H	S/N	3er Piso	Mesa de ayuda	Elvis Mejia
Monitor 22 LCD	Dell 1912H	S/N	3er Piso	Mesa de ayuda	Elvis Mejia
Monitor 22 LCD	HP L1740	93P-WWQ	3er Piso	Mesa de ayuda	Elvis Mejia

Monitor 22 LCD	HP L1740	CN-OFFD9B	3er Piso	Mesa de ayuda	Elvis Mejia
Monitor 22 LCD	HP L1740	C-64180-93P-58Y8	3er Piso	Mesa de ayuda	Elvis Mejia
Monitor 22 LCD	HP L1740	5138-72872-HG80	3er Piso	Mesa de ayuda	Elvis Mejia
Monitor 22 LCD	HP L1740	S/N	3er Piso	Mesa de ayuda	Elvis Mejia
Monitor 22 LCD	HP L1740	S/N	3er Piso	Mesa de ayuda	Elvis Mejia
Monitor Plus	Monitor Plus	85182	3er Piso	Seg. de Sistema	Omar Nuñez
Next Point	IDEA V2.03	45421	3er Piso	Seg. de Sistema	Omar Nuñez
Plastificadora	GBC 1300	NHGW8246	3er Piso	Seg. de Sistema	Ramon Santos
Proyector	Sony VPL-EX4	7018553734	3er Piso	Tecnología	Sergio Luis
Router	Cisco 17500	S/N	3er Piso	Seg. de Sistema	Pedro Pared
Router	Catalys	S/N	3er Piso	Seg. de Sistema	Cindia Espinal
Router	Cisco 1700	FHK07111187	3er Piso	Seg. de Sistema	Samuel Perez
Router	Cisco RPS	BNFG7874	3er Piso	Seg. de Sistema	Sol Sanchez
Router	Catalys 2950	S/N	3er Piso	Seg. de Sistema	Sol Sanchez
Router	Collet	R-009	3er Piso	Seg. de Sistema	Omar Abrue
Scanner	HP 5590	CN5C7XQWE	3er Piso	Tecnología	Leandro Luis
Scanner	HP	CN6229BVTH	3er Piso	Tecnología	Leandro Luis
Scanner	HP 5590	CN6CBSW112	3er Piso	Tecnología	Leandro Luis
Scanner	HP 3590	CN7AYTRPO8	3er Piso	Tecnología	Leandro Luis
Scorage Work	HP M-CB70	WSAQERD12	3er Piso	Seg. de Sistema	Peter Mon
Scorage Work	HP M-CB70	WGFGHVF55	3er Piso	Seg. de Sistema	Peter Mon
Scorage Work	HP EVA4400	DKKHHUK1	3er Piso	Seg. de Sistema	Peter Mon
Scorage Work	HP EVA4400	WSVCVBH2	3er Piso	Seg. de Sistema	Peter Mon
Servidor	IBM X3650N3	KQ0636P	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	IBM	KQ0635D	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	IBM	KQ0636G	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	IBM	KQ0634H	3er Piso	Seg. de Sistema	Pedro Pared

Servidor	Dell 2850	5JCJD81	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	HP BL460C	2UX84504ZG	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	HP BL460C	2UX8654FG4	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	HP BL860C	USE03RE879	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	IBM 5100	SV-0987	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	IBM 5100	SV-0108	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	Dell 280	BZW5873	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	Dell EDGE	5VRZ711	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	HP ML310	323138001	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	Dell 1950	982T5C1	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	HP DL380	D329KJN2H870	3er Piso	Seg. de Sistema	Pedro Pared
Servidor	Dell 2850	CMHVI91	3er Piso	Seg. de Sistema	Cindia Espinal
Servidor	EDEGE-2850	2KZJG548	3er Piso	Tecnología	Luis Mota
Servidor	PROLIAN ML330	MO30LE6R54	3er Piso	Tecnología	Luis Mota
Servidor	EDEGE-2550	4VRDGH54	3er Piso	Tecnología	Luis Mota
Servidor	OPTIPLEX 755	54BVR8H41	3er Piso	Tecnología	Luis Mota
Servidor	OPTIPLEX 755	DW66F54	3er Piso	Tecnología	Luis Mota
Servidor	DL380	D311KGF546HJ	3er Piso	Tecnología	Luis Mota
Servidor	Dell Pix-516	87VD65H4	3er Piso	Tecnología	Luis Mota
Servidor	HP SG-720	MXQ86FGHJ54	3er Piso	Tecnología	Luis Mota
Servidor	HP IDEA V2.03	203BA91	3er Piso	Tecnología	Luis Mota
Servidor	Dell EDEGE-2850	6X21JYHAEW	3er Piso	Tecnología	Luis Mota
Servidor	Dell OPTIPLEX 755	2UX83CVG55	3er Piso	Tecnología	Luis Mota
Servidor	Dell OPTIPLEX 755	MXQ9TFG459	3er Piso	Tecnología	Luis Mota
Servidor	Dell OPTIPLEX 755	MXQ93CXZ48	3er Piso	Tecnología	Luis Mota
Servidor	Dell	MXQ94771YTW	3er Piso	Tecnología	Luis Mota

	OPTIPLEX 755				
Servidor	Dell OPTIPLEX 755	MXQ934200PO	3er Piso	Tecnología	Luis Mota
Servidor	Dell R720	7JPWDXC10	3er Piso	Seg. de Sistema	Peter Mon
Servidor	Dell R720	73EJR91TY8	3er Piso	Seg. de Sistema	Peter Mon
Sevidor	Dell 2950	66DFFGFH2	3er Piso	Seg. de Sistema	Peter Mon
Servidor	Dell 2950	FSFFH6848	3er Piso	Seg. de Sistema	Peter Mon
Servidor	Dell 2950	AFZCVBD5	3er Piso	Seg. de Sistema	Peter Mon
Servidor	Dell 2950	XSVFHJY56	3er Piso	Seg. de Sistema	Peter Mon
Servidor	Dell 2950	ZCXBF289Y	3er Piso	Seg. de Sistema	Peter Mon
Servidor	HP ML150	S/N	3er Piso	Seg. de Sistema	Peter Mon
Sumadora	Sharp	S/N	3er Piso	Proc. Transacc.	Many Ruiz
Sun Fire	T-2000 CD20	SGF4VC6348	3er Piso	Seg. de Sistema	Peter Mon
Switch	Console 3502	MI29477N82	3er Piso	Seg. de Sistema	Peter Mon
Teléfono	Astra	S/N	3er Piso	Tecnología	Jose Milano
Teléfono	Meridian	S/N	3er Piso	Tecnología	Eric Mueses
Teléfono	Nortel Net	NNTMDF0HRG89	3er Piso	Mesa de ayuda	Elvis Mejia
Teléfono	Nortel Net	NNTMOFOUTYR8	3er Piso	Mesa de ayuda	Elvis Mejia
Teléfono	Astra	S/N	3er Piso	Tecnología	Leandro Luis
Teléfono	Nortel Net	NNTMTFOSDF82	3er Piso	Proc. Transacc.	Lilian Pierotti
Teléfono	Meridian	T-1378	3er Piso	Mesa de ayuda	Ariel Infante
Teléfono	Meridian	T-3791	3er Piso	Mesa de ayuda	Ariel Infante
Teléfono	Meridian	S/N	3er Piso	Mesa de ayuda	Ariel Infante
Teléfono	Northel Net	S/N	3er Piso	Mesa de ayuda	Ariel Infante
Teléfono	Northel Net	S/N	3er Piso	Mesa de ayuda	Ariel Infante
Teléfono	Northel Net	S/N	3er Piso	Mesa de ayuda	Ariel Infante

Teléfono	Northel telecon	T-0002	3er Piso	Tecnología	Alicia Ortiz
Teléfono	Meridian	S/N	3er Piso	Proc. Transacc.	Andres Feliz
Teléfono	Northel Net	S/N	3er Piso	Proc. Transacc.	Diolis Perez
Teléfono	Meridian	T-0872	3er Piso	Tecnología	Jochy Santos
Teléfono	Northel Net	S/N	3er Piso	Proc. Transacc.	Many Ruiz
Teléfono	Meridian	T-2084	3er Piso	Proc. Transacc.	Many Ruiz
Teléfono	Nortel Net	MNTMD6545BVN	3er Piso	Mesa de ayuda	Elvis Mejia
Teléfono	Nortel Net	NNTMDFCVVNB4	3er Piso	Mesa de ayuda	Elvis Mejia
Teléfono	Meridian	T-0654	3er Piso	Tecnología	Jose Almonte
Teléfono	Astra	S/N	3er Piso	Proc. Transacc.	Jose Espinal
Teléfono	Northel Net	S/N	3er Piso	Proc. Transacc.	Junior Gomez
Teléfono	Meridian	T-0095	3er Piso	Tecnología	Martha
Trituradora	Fellowes	1002590	3er Piso	Mesa de ayuda	Ariel Infante
Trituradora	Fellowes	1002592	3er Piso	Proc. Transacc.	Diolis Perez
Trituradora	Fellowes	1002589	3er Piso	Mesa de ayuda	Miguel Artiles
Trituradora	Fellowes	1002591	3er Piso	Mesa de ayuda	Miguel Artiles
Trituradora	Fellowes W15B	091009VA0652486	3er Piso	Tecnología	Leandro Luis
Trituradora	Fellowes W11C	091009VA0621214	3er Piso	Tecnología	Leandro Luis
Trituradora	GBS 950S	TC02WQF4	3er Piso	Tecnología	Rey Perez
UMT Firewall	SG-720	06023439	3er Piso	Seg. de Sistema	Cindia Espinal
UMT Firewall	SG-720	06023441	3er Piso	Seg. de Sistema	Cindia Espinal
UMT Firewall	SG-720	06023450	3er Piso	Seg. de Sistema	Cindia Espinal
UMT Firewall	SG-720	06023451	3er Piso	Seg. de Sistema	Cindia Espinal
UMT Firewall	SG-720	06023440	3er Piso	Seg. de Sistema	Marcos Perez
UMT Firewall	SG-720	06023442	3er Piso	Seg. de Sistema	Marcos Perez
UMT Firewall	SG-720	06023445	3er Piso	Seg. de	Marcos Perez

				Sistema	
UMT Firewall	SG-720	06023446	3er Piso	Seg. de Sistema	Marcos Perez
UMT Firewall	SG-720	06023447	3er Piso	Seg. de Sistema	Marcos Perez
UMT Firewall	SG-720	06023444	3er Piso	Seg. de Sistema	Samuel Perez
UMT Firewall	SG-720	06023452	3er Piso	Seg. de Sistema	Samuel Perez
UMT Firewall	SG-720	06023453	3er Piso	Seg. de Sistema	Samuel Perez
UMT Firewall	SG-720	06023449	3er Piso	Seg. de Sistema	Sol Sanchez
UMT Firewall	SG-720	06023443	3er Piso	Seg. de Sistema	Omar Abrue
UMT Firewall	SG-720	06023448	3er Piso	Seg. de Sistema	Omar Abrue

Tabla 3: Fuente Centro de Procesamiento Transaccional, S.A., 2014.

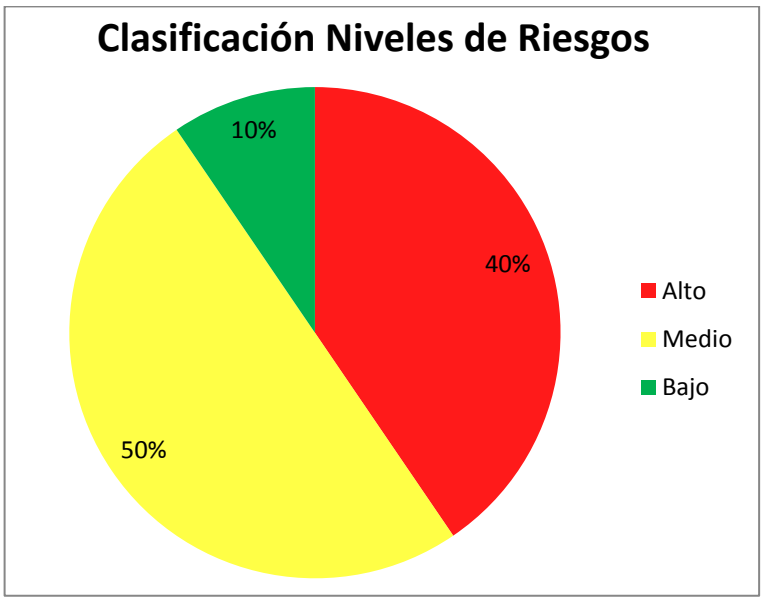
3.5.2 Identificación de Amenazas y Vulnerabilidades.

La identificación de las amenazas y las vulnerabilidades son temas claves para una evaluación de los riesgos. Estos temas de aseguramiento tratan los eventos que puedan afectar directa e indirectamente la continuidad operativa de las empresas y ocasionalmente plantean posibles controles para su mitigación.

Para la evaluación de riesgos (amenazas y vulnerabilidades) a las que el Centro de Procesamiento Transaccional está expuesto, fue desarrollada una matriz detallada de todos los eventos que pueden afectar sus operaciones diarias:

Como parte de las evaluaciones realizadas a las instalaciones, los sistemas y equipos del Centro de Procesamiento Transaccional, S.A., se analizados diez procesos claves del negocio que a su vez asocian un sinnúmero de amenazas y vulnerabilidades que ponen en riesgos la continuidad de las operaciones del Centro.

A continuación presentamos la gráfica de resultados de la evaluación de riesgos realizada a los activos, procesos y/o subprocesos de la institución:



Gráfica 4: Representación Gráfica Niveles de Riesgos, Fuente: Eva. De Riesgos CPT, S.A.

Aquí identificamos el alto porcentaje de riesgos medio y alto, exigiendo adecuados métodos de aseguramiento, desarrollo de planes y estrategias de recuperaciones claras.

Capítulo IV

Análisis de Impacto al Negocio (BIA)

4.1 Objetivos de un Análisis de Impacto al Negocio (Business Impact Analysis, BIA).

El BIA es un paso crítico en el desarrollo de la estrategia de continuidad del negocio y la subsiguiente implementación de las contramedidas de riesgo y el BCP en particular[24].

El análisis de los requisitos para garantizar la continuidad del negocio, y por tanto, el alcance de un análisis de impacto, se puede hacer de manera formal o informal. Algunas organizaciones encuentran adecuado y efectivo, desde el punto de vista de costos el evaluar los impactos de manera informal basándose en el conocimiento que los directivos tienen de los objetivos de la organización y, por tanto, de cuáles son sus funciones críticas. Otras encuentran necesario realizar un Análisis de Impacto en el Negocio de una manera más formal para documentar los impactos y justificar sus tiempos de respuestas[25].

Sin lugar a duda el desarrollo de un análisis de impacto al negocio formal es el que puede otorgar una clara y detallada clasificación de los temas críticos del Negocio, alcanzando un compromiso directo con la organización.

[24] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Análisis de Impacto del Negocio. *Manual de Preparación al Examen CISA 2012* (pp. 133). Estados Unidos de América: ISACA.

[25] Gaspar Martínez, J., (2008). Introducción y Generalidades del Análisis. *El Plan de Continuidad de Negocio – Guía para su Elaboración.* (pp. 17). Madrid: Ediciones Díaz de los Santos, S.A. Recuperado de http://books.google.com.do/books?id=um1V2jADP78C&pg=PA189&dq=analisis+de+impacto+del+negocio&hl=es&sa=X&ei=HSghU5ObOY6gkQf42IGYAQ&redir_esc=y#v=onepage&q=analisis%20de%20impacto%20del%20negocio&f=false

El BIA requiere un alto grado de respaldo por parte de la alta gerencia y una amplia participación del personal de TI y de los usuarios finales[26]. Todos los recursos tecnológicos que representan para la organización un punto clave en apoyo con los objetivos de negocio, deben estar claros y aprobados por la alta Gerencia.

Para el desarrollo de un BIA, regularmente se utilizan diferentes enfoques de metodologías, estos tipos son:

- **Cuestionario:** Este trata sobre la elaboración de un cuestionario detallado y se completa en base a una distribución de los involucrados claves de las áreas de tecnología y del negocio (o usuarios finales de los sistemas de información).
- **Entrevistas Grupales:** Mediante los procesos de entrevistas a grupos estratégicos de la organización, se realizan tabulaciones y análisis de los datos recolectados y se procede a realizar el BIA y detalles de las estrategias.
- **Reuniones Personal Crítico:** Para este método de enfoque se realizan reuniones con el personal clave y/o dueños de los procesos críticos del negocio, para de esta forma llegar a conclusiones de los impactos potenciales en sus diferentes niveles de limitación de los servicios de TI.

[26] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Análisis de Impacto del Negocio. *Manual de Preparación al Examen CISA 2012* (pp. 133). Estados Unidos de América: ISACA.

4.2 Tipos de Impactos y Criterios.

La clasificación o los tipos de impactos y criterios involucran una determinación de riesgos basada en el impacto derivado del periodo de tiempo de recuperación crítico, así como también la posibilidad de que ocurra una interrupción adversa[27]. Para todos estos temas de clasificación del impacto y sus criterios de necesidad, se realizan calificaciones de riesgos basados en las operaciones, sistemas y equipos, influencia económica, entre otros temas, que priorizan la necesidad de recuperar en menos o mayor tiempo cualquier operación interna o servicio de tecnología.

El manual para la preparación CISA (documento basado en CobiT) plantea una clasificación de sistemas, el cual por su detalle puede ser tomado en cuenta para percibir cualquier proceso internos dentro de la organización, esta es:

Clasificación	Descripción
Critica	Este no puede ser realizado a menos que se reemplacen por capacidades idénticas. No se pueden reemplazar las aplicaciones críticas con métodos manuales. La tolerancia a la interrupción es muy baja; por lo tanto, el costo de interrupción es muy alto.
Vital	Estas funciones e pueden realizar manualmente, pero solo por un breve periodo de tiempo. Existe una mayor tolerancia a la interrupción que con los sistemas críticos y, por consiguiente, los costos de interrupción resulta un tanto más bajos, siempre que las funciones se restauren dentro de cierto lapso de tiempo (por lo general cinco días o menos).

[27] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Clasificación de Operaciones y Análisis de Criticidad. *Manual de Preparación al Examen CISA 2012* (pp. 135). Estados Unidos de América: ISACA.

Sensitiva	Estas funciones se pueden realizar manualmente, a un coto aceptable y por un periodo de tiempo prolongado. Aunque se puede realizar manualmente, generalmente es un proceso difícil y es requiere de personal adicional para ejecutarlo.
No Sensitiva	Estas funciones se pueden interrumpir con un periodo de tiempo prolongado, a un costo bajo o nulo para la compañía y requieren poco o ningún esfuerzo de actualización cuando se restauran.

Tabla 4: Fuente Manual de Preparación al Examen CISA 2012.

4.3 Clasificación y Análisis de Impacto a la Empresa.

Con el inicio de esta unidad estaremos viendo todo lo relacionado a las clasificaciones y los recursos que soportan el desenvolvimiento del negocio.

Con nuestras investigaciones y desarrollo del Plan de Continuidad del Negocio para el Departamento de TI del Centro de Procesamiento Transaccional, S.A., determinamos los procesos críticos y los recursos de TI que dependen para su óptimo funcionamiento.

4.3.1 Procesos Claves del Negocio.

Los procesos de negocio son métodos o procedimientos empresariales enfocados para la mejora continua del desempeño corporativo. Para todos los procesos de negocios se realizan métodos evaluativos para validar su adecuado apego con los objetivos de negocios de las organizaciones.

Estos procesos evaluativos se evalúan mediante métodos como El Six Sigma para la evaluación de la calidad y temas de administración de los procesos de negocios o Business Process Management, BPM en inglés.

Con nuestras revisiones interna y levantamientos de información al Centro de Procesamiento Transaccional, S.A. se identificaron las operaciones, procesos y/o sub-procesos del negocio que soportan los servicios corporativos, estos fueron segmentamos por área para de esta forma poder tener de una mayor comprensión, estos son:

Centro de Procesamiento Transaccional, S.A. Procesos Claves de Negocio		
Depart.	**Procesos / Sub-proceso**	**Alcance**
Comercialización y Servicio Técnico	1. Afiliación de Comercios. 2. Gestión de Afiliados. 3. Recalculo de Tasas de Comisión. 4. Reclamaciones Afiliados. 5. Negociación tasas afiliados. 6. Desarrollo Estratégico de nuevos productos. 7. Administración Zonas de Negocios. 8. Consulta Transacciones Electrónicas. 9. Apoyo rentabilidad de la empresa. 10. Concientización Comercios. 11. Distribución Materiales y Equipo a los Clientes. 12. Actualización Datos de Clientes. 13. Programación Equipo POS. 14. Pruebas Equipo para verificación de Funcionalidad. 15. Revisión del equipo por Control de Calidad. 16. Liberación del Equipo Bajo la Certificación de Control de Calidad. 17. Entrega e Instalación del Equipo. 18. Entrenamiento para la Utilización del Equipo POS.	Desde el primer contacto del cliente con el Centro de Procesamiento Transaccional, S.A., hasta culminar el proceso de captarlo como cliente, mantenerlo dentro de la cartera, y establecer relaciones de negocios duraderas a través de la incorporación de nuevos servicios, y un buen servicio al cliente.

Intercambio	1. Gestión reclamaciones y contra cargos clientes. 2. Gestión reclamaciones enviadas por los diferentes bancos. 3. Cumplimiento Contractual con las Marcas. 4. Recuperación de Partidas no Recuperadas. 5. Gestión de los incentivos de Negocios. 6 Envió Cuadres transaccionales de los Puntos de Ventas. 7. Contra Cargos Clientes.	Desde que se recibe una reclamación de un banco hasta que se debite o acredite a la cuenta del Centro de Procesamiento Transaccional, S.A. o su representante, dependiendo del resultado final de la reclamación.
Red ATH / Procesamiento Transaccional.	1. Procesamiento de las Transacciones de la red ATH. 2. Monitoreo Cajeros Automáticos de las Instituciones Afiliadas. 3. Cumplimiento Regulatorio operaciones de los Bancos Afiliados. 4. Mantenimiento Conexión Bancos Afiliados. 5. Tramitar las solicitudes de nuevos cajeros. 6. Procesamiento de todas las transacciones generadas por e-Commerce. 7. Inclusión Nueva Entidad Financiera a la Red ATH. 8. Reporteria Transaccional.	Desde que una institución financiera se conecta a la red ATH hasta velar por el eficiente procesamiento de sus transacciones.
Seguridad / Riesgos al Afiliados	1. Gestión Casos de Fraudes a Afiliados. 2. Informes Gerenciales. 3. Monitoreo de Alertas de Transacciones Fraudulentas a Comercios Afiliados. 4. Revisión Indicadores de Fraudes. 5. Administración Seguridad Física. 6. Seguimiento a los Casos Judiciales. 7. Gestión de los Proveedores de Seguridad Física.	Desde recibir y detectar mediante monitoreo, casos de transacciones fraudulentas, darle el seguimiento y solución final, hasta la gestión de los usuarios de la empresa, su seguridad y su control de accesos.
Autorizaciones	1. Autorización de transacciones. 2. Optimización Procedimiento Transaccional. 3. Cumplimiento Niveles de Servicios (SLA) con Afiliados. 4. Gestión de las Información Transaccionales para Alimentar los Sistemas de Afiliados. 5. Medición (dashboard) Cumplimiento de los Tiempos de Servicios de Afiliados. 6. Identificación de Anomalías en Transacciones. 7. Identificar y solucionar los incidentes Transaccionales con Afiliados.	Desde el primer contacto del comercio afiliado con la empresa, hasta culminar el proceso con la autorización, o la solución de los requerimientos del afiliado.

Finanzas	1. Monitorea de Operaciones Financieras. 2. Informes Gerenciales para la Gestión Financiera. 3. Cuadre de Procesos Internos. 5. Revisión Estados Financieros. 6. Pago a Comercios. 7. Solucionar Situaciones de Rechazo Transaccional. 8. Conciliación Bancaria. 9. Control Activos Fijos. 10. Elaboración y Administración Presupuestaria. 11. Confección Cheques Bancarios. 12. Cobro / Pago a las Marcas Afiliadas. 13. Administración de las Insuficiencias (Transacciones Pendiente por Pagar de los Afiliados). 14. Generación de Reportes Financieros.	Desde el ingreso, cuadre y análisis de las transacciones y registro en la contabilidad hasta la emisión de los Estados Financieros.
Tecnología	1. Gestión de los activos tecnológicos. 2. Gestión de usuarios de todos los empleados. 3. Revisión y mantenimiento de los equipos transaccionales. 4. Monitoreo de la seguridad (alertas) de los equipos y sistemas. 5. Administración de los presupuestos tecnológicos, para dar valor a las adquisiciones realizadas. 6. Evaluación y puesta en producción de los sistemas de información del Centro. 7. Ejecución de tareas para las revisiones del adecuado funcionamiento de los POS (puntos de ventas) para los comercios. 8. Gestión de los proveedores de TI. 9. Asegurar el adecuado funcionamiento de las estaciones de trabajo, los servidores, servicios de TI, redes y cualquier ente tecnológico. 10. Cumplimiento con las mejores prácticas en protección de activos. 11. Gestión de incidentes y crisis. 12. Administración centro de cómputo y la central telefónica. 13. Administración de las bases de datos. 14. Manejo de la Capacidad de los Equipos. 15. Plan adquisición infraestructura. 16. Administración licencias sistemas. 17. Aseguramiento de la data (backup) de los SI y Equipos.	Todo lo relacionado a los temas tecnológicos, desde el desarrollo de un aplicativo para cualquier solución de negocios, hasta la administración de un equipo transaccional el cual hace el enlace directo con las operaciones Centro-Comercio.
Mercadeo	1. Generar ideas publicitarias claras. 2. Gestión de los proveedores publicitarios. 3. Organización actividades institucionales y del público. 4. Diseño de artes publicitarias. 5. Administración presupuestaria de actividades y eventos.	Desde la gestión para el desarrollo de un arte publicitario hasta la organización de un actividad (interna - externa) con todos los temas asociados a presupuestos, imagen corporativa, desarrollo publicitario y responsabilidad social.

Recursos Humanos	1. Reclutamiento y Selección Nuevos Empleados. 2. Pago de Nómina. 3. Contacto con los Banco para fines de Nomina. 4. Evaluaciones de Desempeños Empleados. 5. Gestión Salida Empleados. 6. Gestión Beneficios Empleados. 7. Capacitaciones Internas. 8. Cuadre Fiscal (DGII - TSS). 9. Contacto con el Ministerio de Trabajo. 10. Contacto y Pago Aseguradora de Salud y Laboral. 11. Comunicaciones Internas. 12. Contacto Directo con los Empleados. 13. Gestión de las Policitas y Procedimientos Internos.	Departamento encargado de toda la relación con los empleados (ante, durante y depuse de la contracción) hasta la administración de los beneficios de los colaboradores del Centro. De igual forma mantienen los procesos fiscales y el contacto con el Ministerio de Trabajo.

Tabla 5: Fuente Centro de Procesamiento Transaccional, S.A., 2014.

4.3.2 Recursos de Tecnología de la Información.

Los recursos tecnológicos son soluciones que soportan el servicio o la función del desarrollo de un objetivo personal o de negocio. Estos regularmente presentan una amplia evolución lo que obliga al aceleramiento evolutivo de los mismos.

La aplicación de la TIC a todos los sectores de la sociedad y de la económica mundial han generado una serie de términos nuevos, por ejemplo, *e-business* y *e-commerce* (negocio y comercio electrónico), e-government (gobierno electrónico), e-health (sanidad electrónica), e-learning (formación a distancia), e-inclusion (inclusión social digital), e-skills (habilidades para el uso de las TIC), e-work (teletrabajo), e-mail (correo electrónico)[28], …, por lo que es de suma importancia hacer tratamientos, oportunas identificaciones de las amenazas y vulnerabilidades,

[28] Suárez y Alonso, R. (2010). Conceptos Generales de las Tecnologías de la Información y la Comunicación. *Tecnología de la Información y la Comunicación* (pp. 02). España: Ideas Propias Editorial. Recuperado de http://books.google.com.do/books?id=oPRegn3QhpgC&printsec=frontcover&dq=tecnologias+de+la+informacion+y+comunicacion&hl=es&sa=X&ei=o_cqU-OLMqGR0AHWh4GgCw&redir_esc=y#v=onepage&q=tecnologias%20de%20la%20informacion%20y%20comunicacion&f=false

de igual forma una asignación de controles que puedan asegurar una adecuada continuidad en sus servicios.

Con nuestros entendimientos se identificaron los sistemas de la información que se relacionan directa e indirectamente con los procesos claves del negocio:

Centro de Procesamiento Transaccional, S.A. Recursos de TI	
Sistema	**Descripción**
Acceso Internet.	Plataforma utilizada para el manejo de los sistemas y aplicaciones que necesiten acceso a Internet para su funcionamiento.
Amex App.	Aplicación utilizada para habilitar el paso de las tarjetas American Express en los equipos. Se agrega el terminal del equipo dentro de la aplicación y se le da acceso al sistema para que comunique con la plataforma.
ATHSEC.	Es un sistema utilizado para el monitoreo de las transacciones ATH.
BASE 24Hr.	Herramienta que soporta otras aplicaciones para la revisión de transacciones no reconocidas para los tarjetahabientes y/o comercios afiliados.
Call Timer.	Herramienta utilizada para el control, revisión y medición de las llamadas entrantes y salientes en la empresa.
Cardpac.	Herramienta utilizada para verificar la información de los afiliados, a quien corresponde la asistencia del mismo dentro de la empresa (Técnico/Ejecutivo) y su estatus transaccional.
CICLA.	Sistema utilizado para manejar la condición crediticia de los potenciales clientes y empleados de la organización.
Confeccionaría de Cheques.	Es un sistema utilizado para la emisión de cheques bancarios.
Control Fraude.	Sistema utilizado para el monitoreo de las posibles transacciones fraudulentas en los comercios afiliados.
Correo Interno.	Herramienta utilizada para las comunicaciones internas de la empresa a los empleados.
Dac-Easy.	Sistema utilizado para la administración de los procesos contables y financieros de la organización.
Emulación Bancos.	Sistema utilizado para la recreación de transacciones bancarias desde los Puntos de Venta.

EvaluaTech.	Sistema utilizado por el departamento de Recursos Humanos para la evaluación de nuevo ingreso del personal.
FILEQP.	Sistema de revisión y monitoreo de transacciones que soportado por el área de Intercambio.
Gestor de Casos.	Herramienta utilizada para el manejo y asignación de casos a cada empleado correspondiente para la realización de los mismos.
Intranet.	Red privada de la organización con acceso solo para el personal, en la cual se dispone de herramientas e informaciones de valor para los empleados.
IVR.	Es un sistema automatizado de respuesta interactiva que permite en-rutar llamadas y entregar información sin la necesidad de la intervención humana.
MASTERCOM.	Sistema utilizado para las revisiones y cuadre de las transacciones MasterCard.
MC Match.	Sistema utilizado para la revisión, monitoreo y pruebas transaccionales para las redes de la marca MasterCard.
MC On Line.	Sistema utilizado para la revisión y validación del cumplimiento transaccional de la marca MasterCard.
Meridiam Mat.	Sistema utilizado para medir/mejorar los procesos de negocios para el departamento de Autorizaciones.
Microsoft Office.	Herramienta utilizada para crear, modificar y presentar datos o informaciones útiles para la organización.
Monitor Plus.	Sistema de monitoreo y alerta de las transacciones realizadas por los tarjetahabientes y/o comercios afiliados, en tiempo real.
Monitoreo Bombas de Gasolina.	Sistema para el monitoreo de las Bombas de Gasolina ya que estas son comercios de alto riesgo de fraude.
NAC.	Sistema de autenticación y reforzamiento de la seguridad de la red transaccional.
NICS.	Sistema utilizado para la revisión del adecuado funcionamiento transaccional de los equipos instalados en los comercios.
O. host.	Sistema utilizado para la certificación de la conectividad Comercio/Empresa.
Panagon.	Sistema de búsqueda de información a través todo los reportes almacenados.
Portal Aseguradora de Salud.	Acceso al portal de la Aseguradora de Salud.
Portal Banco (Pago Nomina).	Proceso automatizado para depósito bancario (Sueldo) a los empleados de la empresa.
Portal Bancos.	Acceso a los portales de los distintos bancos del país.

Portal DGII.	Acceso al portal de la Dirección General de Impuestos Internos.
Portal TSS.	Acceso al portal de transparencia de la Tesorería de la Seguridad Social.
QA Cert. System	Sistema utilizado por el departamento de Control de Calidad para la revisión de los equipos y la validez de la programación de los mismos para su liberación y entrega a los comercios.
RRHH APP.	Aplicación utilizada por el departamento de Recursos Humanos para la administración de la información de todos los empleados de la empresa.
Sistema Prevención de Incendios.	Sistema alertador para la prevención de Incendios.
Sistemas Monitoreo CCTV.	Sistema de cámaras para monitoreo por TV 24hrs.
STEP ACH.	Es un sistema de transferencias para el procesamiento de la transacciones generadas por el comercio electrónico (e-Commerce)
V. On line.	Sistema utilizado para la revisión y validación del cumplimiento transaccional de la marca VISA.
Vcenter.	Herramienta utilizada para la programación de los equipos tanto para la información del cliente que deben llevar como para su funcionalidad.
Winpack.	Sistema para el control de los accesos a las diferentes áreas de la empresa. Este sistema otorga los permisos para uno o más departamentos dependiendo de la posición que tiene el empleado.

Tabla 6: Fuente Centro de Procesamiento Transaccional, S.A., 2014.

4.4 Identificación de los Recursos Críticos La Empresa.

La identificación de los recursos (sistemas y equipos) críticos de una organizaciones es imprescindible realizar un amplio entendimiento al universo de los departamentos, procesos y personal que conforman esta.

Para cumplir esta fase con existo, se debe alcanzar una comprensión de la organización, los procesos claves del negocio y los recursos de sistemas de información utilizados para la organización para respaldar los procesos claves del negocio[29].

Dentro de nuestras revisiones, y apoyándonos de la evaluación de riesgos y la identificación de los recursos del negocio y TI, realizamos un análisis cualitativo el cual identifica los procesos críticos para una continua operatividad y sus recursos de TI que los soportan. Estos procesos se identificaron en ciertos niveles de criticidad, donde van desde cero (0 – Sin Nivel de Criticidad) hasta tres (3 – Alto Nivel de Criticidad):

Nivel Criticidad	Cant. Proceso Negocio
No Criticidad (0)	51
Baja Criticidad (1)	12
Media Criticidad (2)	9
Alta Criticidad (3)	20
Total	**92**

Tabla 7: Fuente Procesos Claves - Centro de Procesamiento Transaccional, S.A., 2014.

[29] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Análisis de Impacto del Negocio. *Manual de Preparación al Examen CISA 2012* (pp. 133). Estados Unidos de América: ISACA.

Esta identificación de los recursos críticos de negocio son detallados en los tres niveles (3 - 1) más relevantes de la organización. Estos son:

Alta Criticidad – 3:

Procesos	Descripción del Proceso	Recurso TI	Criticidad
1. Gestión de Afiliados.	Gestiona la captación de potenciales clientes a la cartera de afiliados.	CICLA. Cardpac. Gestor de Casos.	3
9. Distribución Materiales y Equipo a los Clientes.	Instalación de los equipos a utilizar y entrega de material gastable a los clientes.	Cardpac. PANAGON. Gestor de Casos.	3
10. Actualización Datos de Clientes.	Seguimiento a la información de los clientes afiliados para fines de actualización en la base de datos.	Cardpac.	3
11. Programación Equipo POS.	Programación de un equipo ya sea de sustitución por avería o una afiliación nueva.	O. host. V.Center.	3
12. Pruebas Equipo para verificación de Funcionalidad.	Realización de pruebas transaccionales al equipo a fines de verificación buen funcionamiento del mismo antes de entregar a comercio.	MC Match. V.Center.	3
13. Revisión del equipo por Control de Calidad.	Verificación por parte de control de calidad de la programación del equipo tanto en el tipo de programación realizada como en la información del comercio que lleva dentro.	QA Cert. System.	3
1. Reclamaciones Clientes.	Recepción de las reclamaciones de los clientes.	Gestor de Casos.	3
5 Envió Cuadres transaccionales de los Puntos de Ventas.	Envió de los cuadres transaccionales para la gestión de cobros a los comercios y su actualización en los sistemas.	Panagon. MASTERCOM. V On line. MC On line. Gestos de Casos.	3
1. Procesamiento de las Transacciones de la red ATH.	Revisión transacciones no reconocidas por los tarjetahabientes y/o emisores de tarjetas (Bancos).	BASE 24Hr. FILEQP. ATHSEC. STEP ACH. Tserver.	3

3. Cumplimiento Regulatorio Operaciones de los Bancos Afiliados.	Velar porque cada entidad afiliada a los servicios del Centro de Procesamiento Transaccional procese adecuadamente las transacciones, apegadas a los protocolos de transferencia de datos y protección de la información.	FILEQP. Panagon. Correo Interno. Internet.	3
4. Mantenimiento Conexión Bancos Afiliados.	Este proceso vela por el adecuado funcionamiento de las conexiones de datos para el flujo transaccional.	BASE 24Hr. FILEQP. NICS. NAC. Internet. Portal Bancos.	3
6. Procesamiento de todas las transacciones generadas por e-Commerce.	Enrutamiento de las transacciones que se realizan vía internet.	ATHSEC. STEP ACH. BASE 24Hr.	3
7. Inclusión Nueva Entidad Financiera a la Red ATH.	En este proceso, se realizan las inclusiones de los equipos operativos (POS / Cajeros) a las redes transaccionales. Este proceso es posterior a la revisión de las documentaciones y aprobaciones pertinentes.	ATHSEC. STEP ACH. Gestor de Casos.	3
1. Autorización de transacciones.	Aquí se revisan y autorizan las transacciones de afiliados vía telefónico. Este se realiza en menos de 1 minuto por temas de servicio y cola de llamadas.	Call Timer. IVR. Meridiam Mat.	3
6. Identificación de Anomalías en Transacciones.	Aquí se monitorean las transacciones para la oportuna identificación de transacciones anormales, fraudes o cualquier situación no común.	Gestor de Casos. Control Fraude. Monitor Plus	3
7. Identificar y solucionar los incidentes o crisis Transaccionales con Afiliados.	Aquí se revisan todos los temas relacionados a casos de incidentes, errores en procesos de transacciones o direccionamiento con los bancos, cuadre, etc.	Control Fraude. Gestor de Casos. Correo Interno.	3

1. Monitorea de Operaciones Financieras.	Oportuna revisiones a las transacciones financieras realizadas por los operativos del área y los diferentes departamentos el Centro.	Dac-Easy. Panagon.	3
3. Cuadre de Procesos Internos.	Cuadre de las diferentes cuentas contables (CXC, CXP, Proveedores, Marcas, etc.).	Dac-Easy. Panagon.	3
6. Pago a Comercios.	Gestión de pagos de las transacciones procesadas a los comercios, estos se realizan vía cheques o transferencias bancarias.	Confeccionaría de Cheques. Portal Bancos. Acceso Internet.	3
12. Cobro / Pago a las Marcas Afiliadas.	Cualquier tema en cobranza y pago con las Marcas de procesamiento, se realiza vía el Departamento de Finanzas.	Portal Banco. Internet. Dac-Easy. Panagon. Correo Interno.	3

Media Criticidad – 2:

Procesos	Descripción del Proceso	Recurso TI	Criticidad
14. Liberación del Equipo Bajo la Certificación de Control de Calidad.	Visto bueno por parte de control de calidad certificando que el equipo puede ser entregado al cliente.	Gestor de Casos.	2
6. Contra Cargos Clientes.	Reclamación por parte de los afiliados por procesamiento de transacciones no autorizadas.	Gestor de Casos. Vcenter. Correo Interno.	2
2. Monitoreo Cajeros Automáticos de las Instituciones Afiliadas.	Revisión adecuado funcionamiento de los cajeros automáticos conectados a la red transaccional.	NICS NAC. Internet.	2
5. Tramitar las solicitudes de nuevos cajeros.	Gestionar las nuevas conexiones de líneas de datos y enlace a las redes del Centro.	Gestor de Casos. Portal Bancos. Correo Interno. Internet. ATHSEC. STEP ACH.	2
8. Reporteria Transaccional.	Inclusión de todos los reportes transaccionales a los sistemas de consultas (panagon) de la empresa.	ATHSEC. STEP ACH. FILEQP. Tserver	2

3. Monitoreo de Alertas de Transacciones Fraudulentas a Comercios Afiliados.	Revisión continúa de alertas generadas por los tipos de transacciones y equipos POS realizadas en los comercios, de esta forma validar la posibilidad de eventos sospechosos asociados a estas.	Monitor Plus.	2
7. Solucionar Situaciones de Rechazo Transaccional.	Verificación transacciones no procesadas por los bancos para los pagos/débitos a comercios.	Dac-Easy. Cardpac.	2
11. Confección Cheques Bancarios.	Elaboración de los cheques de los diferentes banco, para el pago a los proveedores, empleados o clientes.	Confeccionaría de Cheques.	2
13. Administración de las Insuficiencias (Transacciones Pendiente por Pagar de los Afiliados).	Revisión continúa de los cargos a clientes que, por falta de fondos, no son cobrados.	Dac-Easy. Cardpac.	2

Baja Criticidad – 1:

Procesos	Descripción del Proceso	Recurso TI	Proceso Critico (0 - 3)
6. Consulta Transacciones Electrónicas.	Revisión de las transacciones realizadas en por los comercios.	Vcenter. MC Match.	1
2. Gestión reclamaciones enviadas por los diferentes bancos.	Envió de las reclamaciones a los bancos afiliados.	Correo Interno. Gestor de Casos. Portal Bancos.	1
3. Cumplimiento Contractual con las Marcas.	Cumplimiento transaccional por parte de la empresa de lo solicitado por las diferentes marcas.	Panagon. MASTERCOM. V On line. MC On line.	1
4. Gestión de los incentivos de Negocios.	Gestión de los incentivos ganados por el área de negocios.	Gestor de Casos. Correo Interno.	1
1. Gestión Casos de Fraudes a Afiliados.	Creación, revisión y conclusión de los casos de fraudes a comercios afiliados.	Cardpac, Internet, MC On line, V. On line, Correo Interno, Gestor de Casos, Monitor	1

		Plus y Monitoreo Bombas de Gasolina.	
4. Revisión Indicadores de Fraudes.	Cumplimiento a los indicadores claves de fraudes por comercios establecidos por las marcas afiliadas al Centro de Procesamiento Transaccional, S.A.	MC On line. V. On line. Monitoreo Bombas de Gasolina. Gestor de Casos.	1
5. Administración Seguridad Física.	Mantenimiento de las condiciones físicas de la infraestructura, revisión de la seguridad (interna y externa), monitoreo, acceso a las áreas, entre otras.	Gestor de Casos. Winpack. Sistema Prevención de Incendios. Sistemas Monitoreo CCTV.	1
4. Gestión de las Informaciones Transaccionales de los Afiliados.	Procesos encargado de digitar y actualizar las informaciones de afiliados para las transacciones trabajadas por el personal de Autorizaciones.	Cardpac. Gestor de Casos Correo Interno.	1
8. Conciliación Bancaria.	Cuadre de las transacciones bancarias por emisión de cheques a clientes, empleados y proveedores.	Portal Bancos. Dac-Easy.	1
14. Generación de Reportes Financieros.	Generar y verificar los reportes financieros del Centro.	Panagon. Excel.	1
2. Pago de Nómina.	Aquí se hacen todas las consultas, revisiones y comunicaciones para los pagos de nóminas a los empleados.	Portal Banco. Internet.	1
8. Cuadre Fiscal (DGII - TSS).	Cuadre y gestión de pago de todos los compromisos fiscales.	Portal DGII. Portal TSS. Excel.	1

Tabla 8: Centro de Procesamiento Transaccional, S.A., 2014.

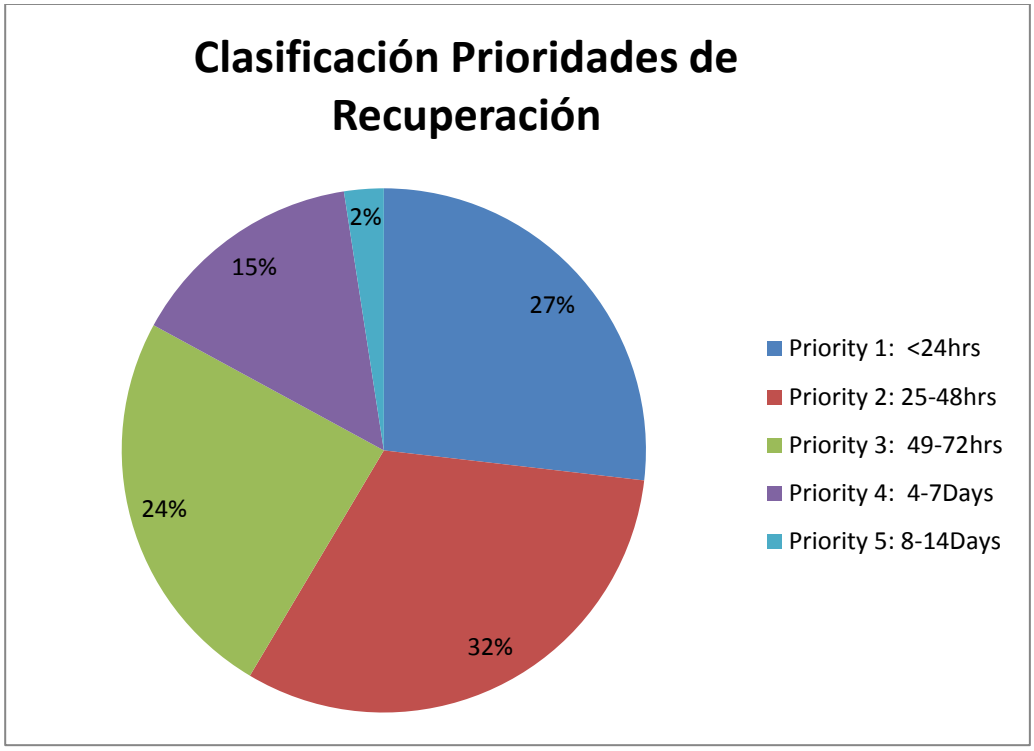
Estos niveles de criticidad con los que se categorizaron las aplicaciones del Centro, fueron realizados en apoyo al cuestionario o checklist de procesos operativos del negocio. Ver Anexo II.

4.5 Matriz de Resultados para los Sistemas Críticos de la Empresa.

Como estrategia fundamental en la puesta en marcha del plan de continuidad para el Centro de Procesamiento Transaccional, S.A. se desarrolló una matriz basado en los procesos estratégicos para la recuperación de las operaciones críticas que soportan los objetivos del negocio.

Este desarrollo se concentró fundamentalmente en la identificación del Punto Objetivo de Recuperación (Recovery Point Objetive, RPO), el Tiempo Objetivo de Recuperación (Recovery Time Objetive, RTO), su Impacto Monetario y No Monetario y la Dependencia Externa (proveedores y/o suplidores de servicios) con los procesos de negocios. Ver Matriz:

Para nuestro análisis de impacto al negocio (BIA) se identificaron significativos resultados que pueden provocar potenciales pérdidas financieras al Centro de Procesamiento Transaccional, S.A. A continuación mostramos la gráfica de resultados del BIA realizado al negocio:



Gráfica 5: Representación Gráfica Prioridades Procesos a Recuperar, Fuente: BIA CPT, S.A.

Esto muestra la alta necesidad que tiene el Centro para disponer de estrategias de recuperaciones de negocios que aseguren la disponibilidad de los servicios.

Capítulo V

Estrategias del Plan

5.1 Estrategias de Recuperación.

Una estrategia de recuperación identifica la mejor manera de recuperar uno o varios sistemas en caso de interrupción, incluyendo desastres, y proporciona una guía según los procedimientos de recuperación detallada que se puedan desarrollar. Es necesario desarrollar diferentes estrategias y presentar todas las alternativas a la alta gerencia[30].

Luego de que se haya desarrollado estrategias que de una forma u otra recuperen los procesos de negocios claves para la organización, la alta dirección es quien debe decidir qué tipo de estrategia sería la más adecuada para la organización. Este tipo de decisión se toma por ciertas combinaciones técnicas, económicas, procesos críticos a recuperar, tiempo de recuperación de cada estrategia, seguridad, entre otros.

Sin lugar a duda las plataformas de tecnología de la información que soportan todos los sistemas o aplicaciones de los procesos claves del negocio requieren un entendimiento y una estrategia de recuperación clara y acertada. Existen muchos método o estrategias alternas, sin embargo el deber de los líderes de tecnología es mostrar cual serían las más viables para la empresas, explicado las diferentes a nivel técnico y monetarios.

Dentro de las decisiones de la alta dirección está en elegir una estrategia que vaya acorde a las necesidades de la empresa y que los costos de recuperaciones y de

[30] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Estrategias de Recuperación. *Manual de Preparación al Examen CISA 2012* (pp. 327). Estados Unidos de América: ISACA.

impacto sean los más aceptables, de acuerdo al nivel de riesgo que se hayan identificado en la evaluación de riesgo y el análisis de impacto al negocio.

5.2 Escenarios del Plan de Recuperación ante Desastres.

En el escenario de un plan ante desastres, se ven las diferentes formas en las que la empresa corre el riesgo de perder información como de paralizar sus operaciones por tiempo indefinido.

Regularmente esta sección de la estrategia es un poco breve, sin embargo no menos importante, ya que enlista los posibles escenarios o las causas en las que se puede ver afectadas las operaciones del negocio. Dentro de estos se pueden ver:

- **Sismos:** Tomando en cuenta que las instalaciones del Centro de Procesamiento de Datos, S.A. y parte de sus oficinas están localizadas en la zona norte del país, están ubicadas exactamente en la misma capa tectónica lo que puede generar situaciones de crisis, como; no operatividad del negocio, perdida de información, pérdidas humanas, pérdidas financieras y de infraestructura.

  Con los últimos estudios de identificación de fallas sísmicas de la isla, se identificados las diferentes provincias que su riesgo a sismos es muy elevado. Ver gráfico:

Gráfica 6: Plan Nacional de Continencia para Terremotos, COE (2009).

- **Servicios Eléctrico:** Como parte de los escenarios de eventos no controlados está la falta de energía eléctrica. En nuestro país se corre el riesgo de disponer de un solo proveedor del servicio eléctrico y de un amplio margen de interrupciones o apagones que ponen en parálisis las operaciones del negocio.

5.2.1 Normalidades de las Operaciones.

La normalización de las operaciones del Centro de Procesamiento Transaccional se basa, fundamentalmente, en poder enlazar las estrategias, conocimiento y recursos tecnológicos para así darse cuenta que las operaciones están en proceso de contingencia, en contingencia y fuera de contingencia.

Este plan de respaldo y la normalización de las operaciones integran tres sub-planes, los cuales establecen las acciones a tomar al momento que se llega a materializar cualquier riesgo ya determinado o no en la evaluación de riesgo, dentro de estos planes están:

- **Plan de Respaldo:** Este plan busca, por encima de cualquier cosa, que una amenaza no llegue a su punto de materialización. Actuando de forma preventiva antes la ocurrencia de situaciones de alerta.
- **Plan de Emergencia:** Aquí se examinan las medidas durante el proceso de la contingencia, justo luego que la amenaza se materializa. El objetivo de este plan es disminuir los efectos que pudo haber traigo la(s) amenaza(s).
- **Plan de Recuperación:** Todos los procedimientos y/o medidas, luego de la ocurrencia de un evento o amenaza, son revisados y puestos en prácticas en este plan. Su objetivo fundamental es recuperar el estado a su normalidad, como si la materialización de la amenaza nunca hubiera ocurrido.

5.2.2 Alternativas de Recuperación.

Una alterativa de recuperación son métodos alternos que una organización desarrolla y evalúa para cuando sus instalaciones principales no estén en disponibilidad operativa.

Las localidades alternas de procesamiento son instalaciones que presentan las condiciones necesarias, en cuento al ambiente, su infraestructura tecnológica y su disponibilidad de la información. Estas soluciones de alternabilidad pueden ser suministradas por un tercero o por el esfuerzo propio.

Este sitio alterno es una localidad muy similar al edificio principal a nivel técnico, entiéndase, que la infraestructura tecnológica esta comunicada y replica la información en su gran mayoría. Este tipo de contingencia proporciona altos niveles de disponibilidad ya que los datos son procesados y almacenados en la localidad principal como en la secundaria utilizando métodos como clustering de datos, mirroring y/o replicación de datos en línea.

Este tipo de alternativa es de las más costosas, sin embargo permite disponer de tiempos de recuperaciones (RTO) menores de las 24 horas, inclusive minutos, todo depende del tipo de configuración, y la cantidad de procesos a recuperar. Dentro de estos tipos de soluciones los más comunes son:

- **Hot Sites:** Son instalaciones con el espacio y la infraestructura básica, todos los equipos de TI, las comunicaciones que se requieren para respaldar las aplicaciones críticas, junto con todo el mobiliario y los equipos de oficina para uso del personal.
- **Warm Site:** Son instalaciones con el espacio y la infraestructura básica, algunos o todos los equipos requeridos y comunicaciones instaladas. Es posible que los equipos tengan menor capacidad que los de la producción normal, pero siguen siento adecuado para sustentar las aplicaciones.

- **Cold Site:** Son instalaciones con el espacio apropiado y la infraestructura básica para apoyar la reanudación de las operaciones, pero sin incluir ninguno de los equipos de TI o comunicaciones, programas, datos o soporte de oficina. El plan que especifique que se utilizara un cold site también debe incluir disposiciones para adquirir e instalar hardware, software y equipos de oficina necesarios para apoyar las aplicaciones críticas[31].

Generalmente las organizaciones que en su plan de recuperación determine un tipo de alternativa como esta es responsable de suministrar todos los equipos necesarios para el adecuado procesamiento de la información, los costos de mantenimiento, estos tienen a ser bajos pero tienden a aumentar si se requieren soluciones sin acuerdos con proveedores.

Teniendo en cuenta que por la alta disponibilidad que requiere el Centro de Procesamiento Transaccional, S.A. para brindar un óptimo servicio a sus afiliados, se recomienda evaluar la alternativa de un sitio alterno, específicamente el **Hot Site**. Por lo que nuestras observaciones y menciones estarán enfocadas a este tipo de solución alternativa.

Para el desarrollo de este tipo de alternativa de recuperación se pueden optar por aplicar diferentes técnicas u opciones, estas son:

La recuperación **independiente o interna**, la cual utiliza los recursos internos de la empresa, tales como instalaciones, equipos de TI y el personal, estos recursos

[31] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Alternativas de Recuperación. *Manual de Preparación al Examen CISA 2012* (pp. 328). Estados Unidos de América: ISACA.

deben estar a la disponibilidad del Centro y en su defecto deberán ser adquiridos para el adecuado desarrollo d sus operaciones.

También está la recuperación dependiente o con terceros, esta ofrece proveedores con alta capacitación en temas de contingencia y/o recuperación de operaciones de negocio. Aquí se determinan contratos de servicios, niveles de servicios (SLA) o cualquier acuerdo legal. Algunos de los proveedores más reconocidos a nivel nacional e internacional, están:

- NAP del Caribe.
- HP.
- Sungard.
- Impsat.
- Entre otros.

Estos tipos de acuerdo pueden especificar si dichos proveedores, suministraran el servicio de infraestructura o no lo harán, también se puede determinar si será un servicio dedicado o no para la recuperación del Centro.

Siguiendo con nuestras revisiones y entendimientos y apegándonos con las evaluaciones de riesgo (RA) y el análisis de impacto (BIA) presentaremos dos alternativas las cuales pueden estar incluidas en el plan de recuperación, como estrategias claves para el negocio.

A. Estrategia 1

En esta estrategia se sugiere la disposición de un Centro de Operaciones Tecnológicas o Centro de Computo Alterno en otro país. Con la consideración de esta se bloquean riesgos a eventos catastróficos en el territorio y al almacenamiento continuo de la información. Este requiere un nivel síncrona o de replicación continua entre las instalaciones principales con las secundarias.

En referencia a las evaluaciones antes mencionadas, RA y BIA, se comprendió la necesidad disponer de un centro de cómputos que cumpla con todos los estándares de alto nivel de la industria y es por tal razón que se recomienda uno con características de TIER 3 (Estándar de Infraestructura de Telecomunicaciones para Data Centers, Telecommunications Infrastructure Standard for Data Centers por sus siglas en ingles), los cuales hace detallada mención a temas de seguridad como: perímetro, vigilancia 24/7, climatización, accesos, áreas de cómputos, estructura física y arquitectónica, conexiones eléctricas y sus paneles, administración de la limpieza, planes de evacuación y sistemas se supresión, entre otros temas que son críticos para una oportuna gestión.

Según la evaluación del BIA, los aplicativos que se deben tomar para la inclusión de esta estrategia de recuperación son:

Imprescindibles	Significativos	Opcionales
• QA Cert. System. • MASTERCOM. • V On line. • MC On line. • BASE 24Hr. • ATHSEC. • STEP ACH. • Tserver. • Monitor Plus • Dac-Easy. • Cardpac • Panagon • O. Host • V. Center • MC Match	• Gestor de Casos. • NICS • NAC. • Portal Bancos. • FILEQP. • Confeccionaría de Cheques.	• Winpack. • Sistema Prevención de Incendios. • Sistemas Monitoreo CCTV. • Excel. • Portal DGII. • Portal TSS. • Correo Interno. • Monitoreo Bombas de Gasolina.

Tabla 9: Criticidad en Recuperación de Aplicaciones, Fuente BIA.

B. Estrategia 2

Para esta estrategia se considera la adquisición y uso de una conexión alterna vía satélite, para la conexión del centro de procesamiento transaccional con el sitio alterno. Se plantea esta opción ya que la conexión por cableado submarino pudiera verse afectado en caso de un terremoto o movimiento de la capa tectónica.

En la actualidad el cable marítimo actual (utilizado para las conexiones con las marcas procesadoras) pudiera ser utilizado como enlace principal, y se contrataría el enlace satelital como línea de datos alterna. Esta se deberá contratar de tipo “Stand By”, el cual solo actuara en caso de ser requerido por un aviso previo con el proveedor.

5.2.3 Operaciones ante Desastres.

Las operaciones y el procesamiento transaccional ante la ocurrencia de una crisis o desastre institucional deben estar claramente definidas, con documentaciones debidamente revisadas y aprobadas, las cuales hagan clara referencia a los procedimientos a realizar ante una recuperación.

Para mantener una oportuna gestión del desastre se desarrollan un sinnúmero de técnicas y/o procedimientos que guían al personal responsable a realizar sus labores sin limitantes o dudas.

Como parte de las operaciones que se deben tener claras y que sin lugar a duda harán la diferencia en contar con un plan de restauración eficiente o no están:

- Adquirir nueva tecnología o reparar rápidamente la disponible.
- Mantener contacto directo con los proveedores de productos y servicios.
- Recuperación de los medios de almacenamiento dentro y fuera del sitio en desastres.
- Oportuna reinstalación de los datos en respaldos (en caso se no existe técnicas de alta disponibilidad o estas presenten alguna avería).
- Mantenerse monitoreando los procesos de recuperación y contingencia de equipos.

Todos estos procedimientos se deben tener claro al momento que algunos de estos deban ser puestos en práctica en plena crisis de recuperación.

5.2.4 Recuperación de Operaciones.

Partiendo de una exitosa recuperación y vuelta a la normalidad de las operaciones del negocio, la división de tecnología debiera determinar el adecuado funcionamiento de las estrategias implementadas y así poder identificar cualquier oportunidad de mejora interna.

Dentro de las actividades post recuperación se deben; 1) realizar actividades grupales para discutir los procesos de restauración implementados, en este se actualizan cualquier documentación (política, procedimiento, guías o plan en específico) que no haya dado respuesta a las situaciones presentadas. 2) Se evalúan los daños y consecuencias provocadas por la situación de desastre. 3) Como procesos final y no menos importante esta la retroalimentación de las situaciones existentes a la alta dirección, para detallar la situación actual que se vive en la empresa.

Todas estas actividades deberán dejarse documentadas y revisadas por los comités o personal responsable a la continuidad del negocio, por lo que se recomienda manejar dichos procesos como actividades de alto nivel para los involucrados.

5.3 Personal Clave en la Toma de Decisiones.

La organización para la gestión de la continuidad del negocio estará recaería en las áreas de Gestión de Riesgo o Gestión a la Continuidad, esta(s) dependencia(s)

serán las encargadas de definir y hacer revisar/aprobar las documentaciones de alto nivel referentes a la continuidad del negocio. Tener una participación clave en el desarrollo de las estrategias, advertir sobre los riesgos asociados a la continuidad y mantener motivación para la incorporación de acciones para la mitigación de largos plazos de recuperaciones.

Todo este personal responsable (gerencial y técnico) deberá contener una lista telefónica o "árbol de llamadas", es decir, un directorio de notificaciones, del personal de TI clave en la toma de decisiones y del personal de usuario final, que se requieran para emprender y llevar a cabo los esfuerzos de recuperación[32].

Para el Centro de Procesamiento Transaccional, S.A., se desarrollaron dos comité que serán el personal clave para la adecuada gestión gerencial (que mantendrá su nivel para la toma de decisiones de alto nivel) y un comité técnico (para la gestión de las tomas de decisiones de nivel técnico en los recursos de TI existentes). Ver detalles:

Centro de Procesamiento Transaccional, S.A.				
Directorio Personal Clave del Plan de Recuperación - 2014				
Comité Gerencial del BCM				
Nombre	**Posición**	**Teléfono 1**	**Teléfono 2**	**Dirección**
Augusto Mejía	VP Ejecutivo	809-937-2356	809-973-6456	C/ 27 de Febrero, Esq. Oeste, No. 320.
Samuel Rodríguez	Director de TI	829-674-8734	809-560-3452	C/ Valentín Pichardo, No. 12, Ens. Mojamet.
Francisco Almanzar	Director Servicio al Afiliado	849-928-2980	809-918.0394	Res. Fernández, Urb Morales, Apart. 12B.
Carmen Paulino	Directora de Negocios	809-450-9839	829-780-3421	C/ José Tapia, Esq. B Torre Fausto Duran.
Morales	Director de	829-980-5687	809-345-9230	Torre Biltmore, Suite 11-1,

[32] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Personal Clave para la Toma de Decisiones. *Manual de Preparación al Examen CISA 2012* (pp. 137). Estados Unidos de América: ISACA.

Picharlo	Finanzas			Naco.
José Amador	Director PMO	809-780-1105	849-802-3412	Av. Enriquillo, Torre Cielos, Piso 7.
Karla Vicini	Gerente de RRHH	829-270-3620	809-560-9090	Edif. A2, Apart. 102, El Vergel.

Centro de Procesamiento Transaccional, S.A.				
Directorio Personal Clave del Plan de Recuperación - 2014				
Comité Técnico del BCM				
Nombre	**Posición**	**Teléfono 1**	**Teléfono 2**	**Dirección**
Miguel García	Director BCM.	849-880-1605	829-590-4569	C/ C-1, Manzana 12, Edif. Ana María IX, Villa Aura.
Iván Marte	Director BCM alterno.	829-908-7683	809-713-2094	C/ B, No. 8, Buena Vista 1era. Sto. Dgo. Norte.
Carlos Nin	Coordinador de TI.	849-660-9820	809-330-1235	Max. Enrique Ureña No. 12, Torre M2, Piantini.
Pavel Mendieta	Coordinador de Prod. Y Serv.	809-340-8371	809-927-2972	Miguel A. Sanche, Naco, Apart. 12E.
Alberto De la Rosa	Coordinador Seguridad Física.	829-980-5687	809-345-9230	Torre Biltmore, Suite 11-1, Naco.
Morales Picharlo	Coordinador de Finanzas.	849-237-0923	809-929-9383	C/ 4, Alma Rosa II, Sto. Dgo. Este.
Edwin Valenzuela	Coordinador RRHH.	809-880-2593	809-837-0283	C/ Carlos Sánchez, No. 22. Naco.

Tabla 10: Guía Responsable BCM, Fuente: CPT, S.A.

Estos directorios deberán ser actualizados periódicamente ya sea por procedimientos o ante algún cambio interno en la organización.

5.4 Resguardo del Plan.

Al desarrollar la documentación del plan de recuperación del negocio se debe tener claro donde se colocara, para que sea de acceso oportuno a los responsables de la continuidad y/o recuperación del Negocio.

Como parte de las mejores prácticas se recomienda la existencia de una copia física en un lugar accesible al personal del Comité Gerencial BCM, también se disponer de copias digitales en un servidor con acceso restringido al personal clave (Gerencial y Técnico) y accesos móviles con alguna herramienta de almacenamiento en la nube.

Como parte de nuestras recomendaciones y sugerencias estratégicas, se le recomienda a la gerencia del Centro de Procesamiento Transaccional, S.A. de la siguiente distribución del plan:

Tipo Documento	Alcance	Personal
Impreso	Estas documentaciones estarán de forma física, y ubicada en las oficinas del personal responsable de la administración del plan de recuperación.	VP Ejecutivo. Director de TI. Director BCM. Director BCM alterno. Coordinador de TI.
Digital	Este tipo de documentación deberá estar ubicada en un equipo (servidor) centralizado de la empresa. Se recomienda que sea un equipo de acceso controlado en la red.	Director de TI. Director BCM. Director BCM alterno. Coordinador de TI.
Repositorio en las Nubes	Acceso en las nubes para las documentaciones del Plan de Continuidad del Negocio. Esta documentación estaría disponible desde cualquier equipos móvil (laptop, Smartphone, tableta, etc.) conectado a una red de internet, y así contar con dicho plan ante cualquier situación de desastres en las localidades del Centro.	Director de TI. Director BCM. Director BCM alterno. Coordinador de TI.

Tabla 11: Centro de Procesamiento Transaccional, S.A., 2014.

En algunas instituciones, todo objeto y colección está calificado y rotulado en función de su importancia, lo que ayuda a garantizar que los objetos más valiosos serán salvados en el caso de que lleguen a la escena de la emergencia personas que no estén familiarizados con las colecciones. Algunos expertos recomiendan que los objetos estén en más amenazas por peligros tales como agua, fuego, o productos químicos, sean los primeros en ser salvados. Los equipos encargados de las colecciones tienen la responsabilidad de establecer este procedimiento con antelación[33].

5.5 Formulario para la Aplicación de las Estrategias (CheckList Operativo).

Un formulario o checklist es una documentación que se crea con la finalidad de agotar ciertos procedimientos sin que se salten pasos necesarios para su adecuada gestión.

El formato de check-list comúnmente utilizado es el de listas de presuntas o paso, y dentro este se diferencian tres modelos en función del tipo de preguntas utilizadas: 1) Mediante preguntas cerradas: se consideran respuestas del tipo: “Si”,

[33] Dorge, V. & Jones, S., (1999). Practicar Frecuentemente los Ejercicios Mentales Relacionados con Emergencias. *Creación de un Plan de Emergencia* (pp. 98). Estados Unidos. The Gretty Conservation Institute. Recuperado de http://books.google.com.do/books?id=m7tQAgAAQBAJ&pg=PA98&dq=guardar+plan+de+contingencia&hl=es&sa=X&ei=8jcyU_WuEIzpkQfkkoDYBg&redir_esc=y#v=onepage&q=guardar%20plan%20de%20contingencia&f=false

"No", "Cumple" o "No Cumple". 2) Mediante preguntas de respuesta múltiple: con diferentes grupos fijos de respuestas posibles. 3) Mediante preguntas abiertas[34].

Tomando en cuenta las evaluaciones y estrategias realizadas, se determinaron ciertos procedimientos claves para que el personal pertinente (Coordinadores del BCM, Técnicos, Proveedores, Alta Gerencia, etc.) cumpla adecuadamente "cómo proceder" ante desastres. Estos procedimientos se basan en los criterios de evaluaciones previstos y soportan los eventos que pueden afectar la continuidad de los servicios en la empresa.

El desarrollo de esta documentación soporte se ve incluido en el desarrollo del plan recuperación ante desastres, en el cual se detallan cada uno de los casos a considerar ante la presencia de un elemento de alto riesgo.

[34] Zapico, F. (2010). La Elaboración de un Plan de Auditoria. *Manual para la Formación del Auditor en Prevención de Riesgo Laborales.* (pp. 133). España. Lex Nova, S.A.U. Recuperado de http://books.google.com.do/books?id=YlhLzWdDHYEC&pg=PA133&dq=que+son+checklist&hl=es&sa=X&ei=JEM0U5K1KNC20AGyr4DgBA&redir_esc=y#v=onepage&q=que%20son%20checklist&f=false

Capítulo VI

Desarrollo del Plan de Recuperación

6.1 Objetivos del Plan de Recuperación.

6.1.1 Objetivos Generales.

Desarrollar un Plan de Continuidad de Negocio para el área de TI (Disaster Recovery Plan, DRP) que garantice la continuidad de las operaciones tecnológicas y la protección de los activos para el Centro de Procesamiento Transaccional, S.A.

6.1.2 Objetivos Específicos

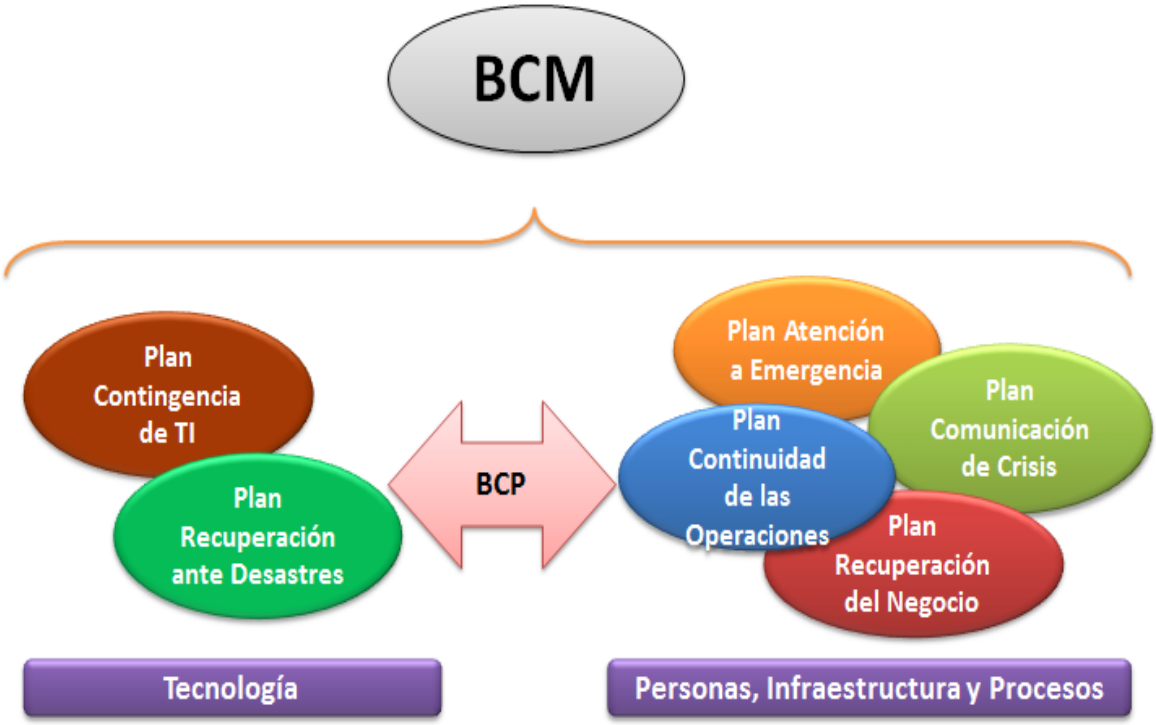
- Elaborar un plan de continuidad del negocio para el Centro de Procesamiento Transaccional.
- Enlistar las ventajas que ofrece la implementación de un plan de continuidad de negocios para el Centro de Procesamiento Transaccional.
- Enlistar las desventajas que tiene la implementación de un plan de continuidad de negocios para el Centro de Procesamiento Transaccional.
- Establecer las características de un adecuado plan de continuidad de negocio para el Centro de Procesamiento Transaccional.
- Establecer la influencia de un plan de continuidad para los clientes, empleados y procesos.
- Indicar los procesos claves a incluir en el plan de continuidad de negocios.
- Identificar las normas, estándares y/o marcos de referencias que hacen relación a la necesidad de disponer de un plan de continuidad de negocios.

6.2 Planes de Acción.

Un plan de acción se define como un conjunto de mecanismos, pasos y/o procedimientos aprobados por la Gerencia, que determinan el que y el cómo se deberá actuar ante la presencia de un desastre.

Estas documentaciones estas conformadas por guías o sub-planes, con sus objetivos y metas claramente definidos. También se busca la orientación estratégica del personal humano, los recursos de TI y sus procesos de negocios.

Para los planes de acciones que el Centro de Procesamiento Transaccional, S.A. se muestran los componentes que forman parte integral de la administración de la continuidad o BCM. De forma gráfica mostramos los diferentes planes que dispondrá el BCM global de la empresa:



Gráfica 7: Estructura de Gestión para la Continuidad del Negocio, BCM.

A continuación se enlistan cada uno de los planes que integran la gestión de la continuidad o BCM:

- **Plan de Contingencia de TI :**

Objetivo: Provee los procedimiento y capacidades esenciales para la recuperación de los servicios y equipos de TI en la organización.

Alcance: Estos planes se centralizan en las situaciones de fallas o complicaciones que puedan tener los sistemas y equipos de tecnología.

- **Plan de Continuidad del Negocio (BCP):**

Objetivo: Conservar la continua operatividad del negocio y sus funciones criticas al momento y justo después que ocurra cualquier situación de desastres o interrupción. Este plan engloba todos los demás planes.

Alcance: Este plan centra todos los temas del negocio, como la infraestructura, la tecnología, las personas, los procesos del negocio, y los alinea en un marco global.

- **Plan de Continuidad de las Operaciones:**

Objetivo: Mantiene su función en la recuperación de los niveles de mando de la organización, a un sitio alternos que soporte directamente al negocio.

Alcance: Procesos operativos y de negocio definidos en la organización.

- **Plan de Atención a Emergencias:**

Objetivo: Suministrar los protocolos para la atención al personal de la empresa, ante un evento de catástrofe o desastre, este plan centra información clave para los primeros auxilios por incidencias.

Alcance: Este solo se concentra en el tratamiento del personal y la infraestructura, no incluyen referencia para los procesos de negocios y la tecnología de la información.

- **Plan de Comunicación de Crisis:**

Objetivo: Este plan proporciona toda la documentación referente a la adecuada comunicación interna y externa con temas de crisis o desastres en la organización.

Alcance: Basa sus procedimientos en cómo comunicarse con los clientes, socios, empleados, las entidades gubernamentales, etc.

- **Plan de Recuperación del Negocio:**

Objetivo: Se fundamente en la recuperación, a un sitio alternos, de todos los procesos de negocios vitales para la operatividad de la empresa ante la ocurrencia de un desastre.

Alcance: Este solo incluye los procesos de negocios definidos por la empresa y que son vitales para su procesamiento de información.

Todas estas documentaciones o tipos de planes de continuidad se deberán desarrollar basados en todos los temas críticos del negocio y dispondrán de todo el apoyo de la gerencia como patrocinadores de dichos esfuerzo de continuidad.

- **Plan de Recuperación ante Desastres:**

Objetivo: Este fundamenta sus esfuerzos en la restauración de los recursos tecnológicos (equipos, bases de datos, sistemas principales, aplicaciones de negocios y cualquier ente asociado) en un lugar alterno para su adecuado procesamiento, por la ocurrencia de eventos que no sean controlados oportunamente.

Alcance: Aquí se abarcan los temas de tecnología (TI), limitándose a perturbaciones o catástrofes que prolonguen los tiempos de recuperación del negocio (RTO).

En este último detallaremos los procedimientos necesarios para restaurar las operaciones de TI ante la presencia de cualquier elemento que afecte la continuidad de los procesos de negocio de la empresa. Ver anexo III.

Capítulo VII

Pruebas y Mantenimientos del Plan

7.1 Importancia de las Pruebas en un Plan ante Desastres.

El Plan de Continuidad de Negocio para TI necesita ser probado periódicamente con el fin de garantizar que la compañía entienda cómo debe ser ejecutado. Probarlo en la organización, evalúa su viabilidad y garantiza un entrenamiento práctico para el personal involucrado de los grupos de recuperación, lo cual representa una parte fundamental sobre cómo reaccionar adecuadamente en caso de presentarse una contingencia[35].

Muchas pruebas que se realizan a los programas de continuidad de las organizaciones no logran a ser una evaluación a gran nivel, limitándose a procesos operativos, estas metodologías no suprimen la necesidad de realización de pruebas totales o parciales al plan, ya que con estas se pueden identificar el adecuado funcionamiento del plan o la identificación de mejoras en partes de él.

Las pruebas deben programarse durante un tiempo que minimicen las interrupciones de operaciones normales. Los fines de semana son, por lo general, un buen momento para realizar las pruebas. Es importante que los miembros claves del equipo de recuperación participen en el proceso de la prueba y le dediquen el tiempo necesario para poner todo su empeño en ello[36].

Todas estas pruebas deben estar documentada por uno o varios integrantes del equipo de pruebas, y determinar los tiempos requeridos para dichas procesos de

[35] Colegio de Contadores Públicos de México, A.C, (2013, 08 de Julio). La Importancia de Implementar un Plan de Continuidad de Negocios (2da Parte). *Dinero en Imagen*. Recuperado de: http://www.dineroenimagen.com/2013-07-08/22715

[36] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Pruebas del Plan. *Manual de Preparación al Examen CISA 2012* (pp. 138). Estados Unidos de América: ISACA.

recuperación. La medición de estos tiempo deben ser evaluación y determinar si cumplen o no con los tiempos de recuperaciones (RTO) definidos inicialmente.

7.2 Programa de Pruebas del Plan.

7.2.1 Especificaciones de las Pruebas.

Para poder llegar a disponer de un adecuado plan de continuidad, hay que poder definir adecuadas pruebas que se ajusten a las necesidades del Centro de Procesamiento Transaccional, S.A. Este se obtiene con la realización de pruebas modulares o como muchos llaman “pruebas paso a paso”, para de esta forma ir identificando debilidades de menor a mayor envergadura, sin poner en riesgo los procesos del negocio.

Existen diferentes tipos de pruebas que ayudan a identificar cualquier debilidad en las documentaciones o temas técnicos del plan, dentro de estas enlistamos tres las cuales abarcarían los temas claves para una rápida y clara absorción del Centro de Procesamiento Transaccional, S.A., estas son:

- **Pruebas Lápiz y Papel:** Aquí se confirman la condición física del plan, se revisa el personal que se involucra en el plan, si estos comprenden en su exactitud los compromisos asociados a esta integración y sus procedimientos ante la ocurrencia de un evento.
- **Pruebas de Preparación (o de Escritorio):** Estas las enfocaremos a revisiones puntuales del plan, se simularan tareas de recuperación reales que

hagan énfasis a la pérdida de algún servicio o procesos del negocio y TI. Este es un tipo de prueba que regularmente se hacen inversiones de recursos, y ayuda a la identificación gradual de evidencia sobre qué tan certero es el plan.

- **Pruebas Completas (o Integrales):** Para este tipo de prueba se utilizaran todos los componentes que integran el Plan, y se realizaran interrupciones en tiempo real, de esta forma se identifica la realidad actual del Plan.

7.2.2 Ejecución de las Pruebas del Plan.

Para los procesos de ejecuciones de las pruebas del plan, se realizan basados en los diferentes tipos descritos más arriba, para agotar todas las fases y disponer de un adecuado plan de continuidad.

- **Prueba Lápiz y Papel:**

Código Prueba	P-01.
Nombre Prueba	Prueba Lápiz y Papel del Plan.
Descripción Prueba	Ejecución de las pruebas en papel del Plan.
Objetivo	▪ Revisar el contenido contextual del plan de recuperación ante desastres. ▪ Apreciar la certeza del plan y cada una de sus partes que lo integra. ▪ Verificar si requiere actualizaciones en informaciones o procedimientos.
Alcance	▪ Policitas y procedimientos del Centro. ▪ Procedimientos de recuperación definidos. ▪ Procesos de negocios. ▪ Árbol de Contactos. ▪ Anexos relacionados.
Frecuencia	Revisión anual o por cada cambio en los procesos de negocio, la infraestructura, la tecnología, etc.

- **Pruebas de Preparación (o de Escritorio):**

Código Prueba	P-02.
Nombre Prueba	Comprobación de todos los componentes del Plan
Descripción Prueba	Verificar la adecuada funcionalidad de los procedimientos del Plan.
Objetivo	Aquí se ensayaran todos los componentes de recuperación existentes, los procedimientos de recuperación y sus tiempos de esfuerzo.
Alcance	▪ Policitas y procedimientos del Centro. ▪ Procedimientos de recuperación definidos. ▪ Procedimientos de operaciones definidos. ▪ Procesos de negocios. ▪ Árbol de contactos. ▪ Anexos relacionados.
Frecuencia	Revisión anual o por cada cambio en los procesos de negocio, la infraestructura, la tecnología, etc.

- **Pruebas Completas (o Integrales):**

Código Prueba	P-03.
Nombre Prueba	Prueba integral o real time.
Descripción Prueba	Consiste en la ejecución en vivo del plan.
Objetivo	En esta prueba se realizaran las pruebas de las estrategias definidas para la recuperación de los procesos de negocio y TI, y se revisaran el adecuado funcionamiento del Sitio Alterno.
Alcance	Plan de Continuidad del Negocio.
Frecuencia	Revisión anual o por cada cambio en los procesos de negocio, la infraestructura, la tecnología, etc.

Tabla 12: Control de Pruebas Plan, CPT, S.A.

Para el desarrollo de estas pruebas, se estableció un calendario que identifica, por tarea de revisión, las fechas en las que serán realizadas:

Centro de Procesamiento Transaccional, S.A.			
CALENDARIO PLAN DE PRUEBAS			
Prueba	**Acción**	**Alcance**	**Fecha**
Prueba Papel y Lápiz	Revisión contenido contextual del plan de recuperación ante desastres	Revisiones políticas y procedimientos del Plan.	4-Aug-14
		Revisión Estrategias de recuperación definidas.	5-Aug-14
		Revisión procedimientos de recuperación.	6-Aug-14
		Identificación y revisión árbol de contactos.	6-Aug-14
		Revisión anexos relacionados.	7-Aug-14
	Apreciación del plan y las partes que lo integra	Revisiones políticas y procedimientos de las áreas claves.	8-Aug-14
		Verificación de los procesos de negocios.	11-Aug-14
		Validación inclusión procesos claves al plan.	12-Aug-14
		Establecer contacto con los involucrados de las áreas de negocio.	12-Aug-14
		Revisión anexos relacionados.	12-Aug-14
	Verificación de actualizaciones del Plan	Revisión de cambios en las documentaciones y/o procesos de negocios.	13-Aug-14
		Actualizar procedimientos de recuperación ante cambio en las documentaciones de alto nivel.	14-Aug-14
		Actualizar procesos de negocios.	15-Aug-14
		Actualizar árbol de contactos ante cambio en la organización.	15-Aug-14
		Revisión anexos relacionados.	15-Aug-14
Pruebas de Preparación	Pruebas Teóricas del Plan	Verificación de los diferentes escenarios del Plan.	19-Aug-14
		Revisión cada punto clave del Site Alterno.	20-Aug-14
		Identificación oportunidades de mejoras en la conceptualización de los escenarios.	21-Aug-14
		Revisión anexos relacionados.	21-Aug-14
		*Ejecución escenario 1 - Corte de Energía.	24-Aug-14
		*Ejecución escenario 2 - Falla de Servidor.	27-Aug-14
		*Ejecución escenario 3 - Incendio.	30-Aug-14

Pruebas Completas o Integrales	Ejecución Integral Plan	*Ejecución escenario 4 - Falla Red de Datos.	31-Aug-14
		*Ejecución escenario 5 - Perdida de Infraestructura.	7-Sep-14
		*Levantamiento Site Alterno niveles controlados.	2-Sep-14
		Contacto con involucrados (Internos / Externos).	En el Proceso
	Verificación Esfuerzos y Tiempos de Respuesta	Toma de los tiempos de recuperación del Plan.	En el Proceso
		Identificar niveles de esfuerzos para cada escenario.	En el Proceso
		Verificación de los tiempos por escenario.	En el Proceso
		Identificación oportunidades de mejoras (cambios documentaciones).	8 al 12 de Sept.

Tabla 13: Plan de Pruebas, CPT, S.A.

*Estas pruebas serán desarrolladas en horarios no laborables, específicamente de 12:00 am a 5:00 am.

7.2.3 Documentaciones de los Resultados.

Para mantener un adecuado nivel de control y documentaciones se deberá documentar cada una de las etapas de las pruebas que se le realizaran al plan. En estas documentaciones se detallan cada una de las observaciones, los inconvenientes o situaciones de problemas y las soluciones tomadas. Es importante que cada equipo de trabajo disponga de un control diario y así mantener documentadas los pasos específicos y las informaciones que serán utilizadas como documentaciones soportes.

Disponer de un buen control de documentaciones ayudara al análisis de informaciones históricas que son de gran importancia para los procesos de recuperaciones del plan.

Para el Centro de Procesamiento Transaccional, S.A. se deberán tener en cuenta la calidad de las informaciones documentadas, para así medir el Plan. Estas deberán basarse en una observación detallada y evaluarlas en base a métodos cualitativos. Dentro de las mediciones específicas se deberán tomar en cuenta:

- **Tiempo:** se identifican y documentan los tiempos involucrados en el plan, desde la entrega de los equipos, integración del personal técnico del BCP, hasta cuando los servicios son restaurados a niveles operativos.
- **Conteo:** parámetro de la cantidad de registros u objetos que presentaron integridad al momento del traslado de la información, al sitio alterno, así como el total de los materiales y equipos utilizados.
- **Cantidad:** se pueden evaluar el esfuerzo del personal que trabajo en el sitio alterno y verificar el volumen de operaciones procesadas en cada sistema de información utilizado durante la crisis.
- **Precisión:** Se verificaran, mediante métodos de muestreo y/o observación la exactitud con que las informaciones fueron capturadas por el personal operativo, en el sitio alterno y estas se compararan con la precisión en situaciones normales.

Todas estas documentaciones deberán ser revisadas y analizadas por la alta gerencia y el nivel administrativo del BCP, de esta forma se podrá llegar a cabo

conclusiones de mejora para los procedimientos existentes. Se almacenaran de forma digital y física, pero siempre estarán disponibles por periodos mayores a las dos últimas actualizaciones del Plan.

7.3 Mantenimiento del Plan.

El Plan de Continuidad de Negocio del área de Tecnología es una documentación viva que debe ser continuamente revisado y actualizado. En estas revisiones se deben revisar todos los cambios organizacionales, las operaciones de negocio, la infraestructura, la tecnología, regulaciones o leyes y cualquier ente sujeto a cambio.

La alta gerencia del Centro deberá disponer de políticas y procedimientos claros para que cada nivel gerencial de la empresa notifique al encargado del plan la existencia de cambios en los equipos, sistemas y/o procesos del negocio, para así poder realizar oportunas evaluaciones y actualizaciones de los planes de recuperación.

Dentro de los lineamientos que se deben tener en cuenta para dicho mantenimiento están:

- Cualquier cambio en los objetivos y/o procesos de negocios deberán ser enviados al encargado operativo del plan de continuidad.
- Toda contratación, movimiento o salida de personal clave para el plan de continuidad se deberá notificar al encargado del plan para la sección de recursos humanos.

- Cualquier cambio en la infraestructura tecnológica, software, equipos de comunicaciones o cualquier recurso de TI que soporte algún proceso de alto impacto para el negocio deberá ser notificado al personal líder del plan para el área de TI.

Para mantener acorde los niveles de mantenimientos del plan, se estableció un calendario de mantenimiento el cual muestra los esfuerzos de actualizaciones a realizar por los líderes del plan:

Centro de Procesamiento Transaccional, S.A.			
Calendario Plan de Mantenimiento			
Evaluación	**Objetivo de Mantenimiento**	**Fecha**	**Frecuencia**
Cambios Organizacionales	Toda contratación, movimiento o salida del personal.	15-Dec-14	Semestral
	Cambios en los objetivos y/o procedimientos de Negocios.	16-Dec-14	Semestral
	Cambios en las descripciones de puestos de áreas claves del Plan.	16-Dec-14	Anual
Infraestructura	Cambios en la infraestructura tecnológica (Equipos, Sistemas, Proveedores, etc.).	17-Dec-14	Anual
	Cambios en el diseño y ubicación de las unidades de trabajo.	22-Dec-14	Anual
Regulaciones o leyes	Cambios en regulaciones o normas de seguridad y del negocio.	28-Dec-14	Anual
	Imposiciones de nuevas regulaciones en protección de activos.	28-Dec-14	Anual

Tabla 14: Plan de Pruebas, CPT, S.A.

Este plan se mantiene programado a ser cumplido según su fecha y frecuencia, sin embargo cualquier cambio que ponga en comprometimiento algún punto de evaluación deberá ser revisado antes de sus tiempos asignados.

Capítulo VIII

Plan de Manejo de Comunicación ante Incidentes y Crisis

Plan de Manejo de Comunicación ante Incidentes y Crisis

Desde el punto de vista social, la comunicación es una forma de inducción informativa de una situación. De igual forma es una eficaz herramienta de gestión, utilizada para la orientación estratégica de las empresas.

La necesidad de las empresas para disponer con una adecuada gestión de comunicación es cada día más grande, ya que su inexistencia crea situaciones de falta de vinculación entre situaciones internas y externas, inadecuada comunicaciones con sus consumidores y su imperativo de la creación de valor, entre otras cosas por dar a conocer.

Un correcto Plan de Continuidad de Negocio debe disponer de un plan de comunicación ante crisis o incidentes para prevenir situaciones de dudas, incertidumbre o cualquier situación de alarma de los involucrados de la empresa. La inexistencia o inadecuada gestión de este plan puede inducir a daños en la imagen corporativa del negocio como la creación de incertidumbre o decepciones internas y externas.

Como parte de nuestro desarrollo del plan de continuidad del negocio, y apegándonos a las mejores prácticas de gestión de continuidad, se cuenta con un plan de comunicación a crisis, con un propósito principal de poder brindar los procedimientos claves para la distribución de los informes de situación al personal internos y público. Estas informaciones tratan de forma clara las informaciones de

negocio y del personal, sin entrar en muchos detalles con los temas internos de tecnología.

Dentro de los procedimientos y/o pasos para el plan de comunicaciones a incidentes y crisis, están:

1. El líder del plan de comunicaciones de crisis deberá mantener oportuna integración con las situaciones de la empresa al momento de una crisis o incidente. Deberá tener un entendimiento claro de los temas del negocio que pueden afectar la operatividad de la empresa.
2. Realizar reuniones con los integrantes del (los) plan (es), para cada una de las áreas, y determinar el nivel de informaciones a suministrar.
3. Documentación de notas o informes con el comunicado a ser expuesto al personal interno y externo de la empresa. Este deberá presentar revisión y aprobación por los líderes operativos del plan, la alta gerencia del plan y la directiva de la empresa.
4. Para los métodos de comunicaciones, se dispondrán de métodos claros y oportunos para que la imagen corporativa del Centro, dentro de estas están:
    a. **Notificaciones o memorándum (interno):** se manejaran informes con las informaciones necesarias de la situación presentada. Estas serán expuesta por el vocero oficial o el líder del plan de comunicaciones de crisis a los empleados y contratistas de la empresa.
    b. **Nota / Rueda de Prensa:** Para dar parte a los clientes, proveedores o cualquier ente social interesado, se realizaran notas o en su defecto

ruedas de prensas, para informar la situación actual de la empresa y los esfuerzos de recuperación tratados.

Todos estos pasos estarán enlazados con los diferentes planes de recuperación ya elaborados, y así poder certificar que un solo comunicado podrá suministrar el mensaje suficiente sin que despierte alerta social.

Capítulo IX

Programa de Capacitación, Concientización y Difusión del Plan

Programa de Capacitación, Concientización y Difusión del Plan.

Todos los temas de nuevos procesos de negocios, implementaciones tecnológicas o cambios en los procesos ya existentes crean mucho disgusto, cuestionamiento, dudas y/o poca aceptación al cambio. Sin embargo es una situación real y de claro entendimiento que la tecnología, los objetivos del negocio, las personas hasta el nivel de cumplimiento regulatorio cambian contantemente y con esto se necesita contar con métodos alternos para salvaguardar los activos de una empresa y todos sus cambios.

Es de suma importancia mejorar la cultura organizacional y la perspectiva en los procesos internos de la empresa por medio de un plan de capacitaciones y concientización continua. Como parte de nuestro desarrollo del plan, se trataran tres temas claves para que todo el personal entienda y acepte los cambios y las nuevas metodologías ante un desastre presentado. Estos son:

Capacitación:

Los programas de capacitaciones del plan de continuidad de negocio para TI detallan y suministran los lineamientos necesarios para suministrar las informaciones teóricas, prácticas y formativas que van dirigidas al personal de la empresa.

Para cumplir con una etapa fundamental en el desarrollo del plan, se determinaron ciertas capacitaciones que ayudaran al desarrollo de las actividades de aprendizaje del plan, dentro de estas están:

- Evacuaciones de Emergencia.
- Catástrofes Naturales.
  - Manejo de Incendios.
  - Manejo de Huracanes e Inundaciones.
  - Manejo de Terremotos.
- Control ante Robo, Intrusos, Terrorismo, etc.
- Primeros Auxilios.

Para cumplir con estos temas de capacitaciones, se desarrolló un calendario de actividades que incluirá todos los temas para una adecuada gestión del conocimiento:

Centro de Procesamiento Transaccional, S.A.			
Plan de Capacitación ante Emergencias 2014.			
Actividad	**Capacitación**	**Fecha**	**Facilitador**
Charla	Fundamentos del BCP/DRP.	05-05-14	Coordinador BCP.
	Importancia del BCP/DRP.	05-05-14	Coordinador BCP.
	Planes de Emergencias y Crisis.	05-05-14	Coordinador Plan Atención Emergencias.
	Manejo ante Robo, Intrusos y Terrorismo.	06-05-14	Gerente Seguridad Física.
	Comunicación ante Crisis.	06-05-14	Coordinador Comunicaciones del Plan
	Administración del Estrés.	08-05-14	Gerente RRHH.
	Equipo Responsable del BCP/DRP.	12-05-14	Coordinador BCP.
	Equipos de Evacuaciones ante Crisis.	12-05-14	Coordinador Plan de Crisis.
Taller y Entrenamientos	Procedimientos de Evacuación.	13-05-14	Coordinador Plan Emergencias.
	Uso Extintores y Escaleras de Emergencias.	14-05-14	Gerente Seguridad Física.
	Reordenamiento del Personal ante Crisis.	15-05-14	Coordinador Plan de Crisis.
	Adecuado Uso de las Redes Sociales.	15-05-14	Coordinador Comunicaciones del Plan

	Manejo con Clientes, Proveedores, Reguladores.	15-05-14	Coordinador Comunicaciones del Plan
	Manejo de Incendios.	16-05-14	Bomberos, Gerente Seguridad Física.

Tabla 15: Plan Capacitaciones Planes, CPT, S.A.

Todas estas capacitaciones serán realizadas en las instalaciones del Centro de Procesamiento Transaccional, S.A. y contaran con el apoyo de la Alta Gerencia, Los Gerentes de áreas y los Supervisores departamentales.

Concientización y Difusión:

Apoyando este plan de capacitaciones, se han desarrollado otras estrategias de concientización y difusión de los planes que ayudaran significativamente a la madurez interna y externa de la institución, dentro de estas están:

- **Mural:** Se instalaran mudares con afiches informativos referentes a consejos de manejo de incidentes, resguardo de información, evacuaciones, entre otros.
- **Correos:** Mediante la mensajería interna se realizaran envió de informaciones referentes a los temas de evacuaciones, alertas de ciclones, tormentas, vaguadas, terremotos y demás eventos catastróficos.
- **Intranet:** Se dispondrá de una sección, en el intranet de la empresa, referente a todas las documentaciones que ofrezcan la orientación necesaria ante la amenazada de un evento que ponga en riesgo la empresa.

Estos métodos de comunicaciones estarán apoyados en un programa anual del conocimiento empresarial y serán revisadas anualmente para mantener una oportuna y eficaz metodologías de comunicaciones.

CONCLUSIÓN

Como parte de las investigaciones y evaluaciones se determinó la importancia, que el Centro de Procesamiento Transaccional, S.A., cuente con un Plan de Continuidad de Negocio para el Área de TI, ya que se reflejaron significativos amenazas y vulnerabilidades que exponen los procesos de negocios y los equipos que los soportan.

El Desarrollo e implementación de este plan no garantizara que el Centro cuente con una continua operatividad de un ciento por ciento en sus procesos de negocios, sin embargo se reducirán considerablemente los potenciales riesgos que se ve expuesta la organización.

Sin lugar a duda con la puesta en marcha de este plan se preverán los potenciales entes maliciosos y se mitigaran con la implementación de controles que reducirán, de forma significativa, los riesgos residuales para la organización.

BIBLIOGRAFÍA

1. Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Gobierno de TI. Manual de Preparación al Examen CISA 2012 (pp. 94). Estados Unidos de América: ISACA.

2. Bon Van, J., Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van der Veen, A. & Verheijen, T. (2008). Gobierno de TI. (Ed), Fundamentos de la Gestión de Servicios de TI Basada en ITIL V3. (pp. 10 – 11). Holanda: Van Haren Publishing. Recuperado de http://books.google.com.do/books?id=QHYs9yWDRsQC&pg=PA10&dq=gobierno+de+ti&hl=es&sa=X&ei=_lYaU4_XNYbQkQfwmoDYDQ&sqi=2&redir_esc=y#v=onepage&q=gobierno%20de%20ti&f=false

3. Gaspar Martínez, J. (2004). Introducción. (Ed), Planes de Contingencia - La Continuidad del Negocio en Las Organizaciones. (pp XXVII). Madrid: Ediciones Díaz de Santos, S.A. Recuperado de http://books.google.com.do/books?id=K_UMxjjB5gUC&printsec=frontcover&dq=Administracion+de+la+continuidad+del+negocio&hl=es&sa=X&ei=EJ4aU8jaE42pkAevvIG4Cw&redir_esc=y#v=onepage&q=Administracion%20de%20la%20continuidad%20del%20negocio&f=false

4. Álvarez Torres, M. (1996). Las Políticas. (Ed), Manual para elaborar Manuales de Políticas y Procedimientos. (pp 27). México: Panorama Editorial, S.A. Recuperado de http://books.google.com.do/books?id=YnhdFdUDnVIC&printsec=frontcover&dq=politicas+y+procedimientos&hl=es&sa=X&ei=_3UeU7S-I4mUkQez_YHQDQ&redir_esc=y#v=onepage&q&f=false

5. Oteo Ochoa, L. (2006). Estándares – Una aproximación al concepto de Estándar. (Ed), Gestión Clínica: Desarrollo e Instrumentos. (pp 206-207). Ecuador: Ediciones Díaz de Santos. Recuperado de http://books.google.com.do/books?id=o_TE96PdcdQC&pg=PA206&dq=que+es+un+estandar&hl=es&sa=X&ei=24MeU4b7JNHwkQfprIHABA&redir_esc=y#v=onepage&q=que%20es%20un%20estandar&f=false

6. Aguilera, P. (2000). Aproximación al Concepto de Seguridad en Sistemas de Información. Seguridad Informática (pp. 9). España: Editorial Editex, S.A. Recuperado de http://books.google.com.do/books?id=dXFcvBCHJzAC&pg=PA43&dq=Seguridad+de+activos+de+TI&hl=es&sa=X&ei=qM0fU9GYHonvkQeg6ICwDQ&redir_esc=y#v=onepage&q=Seguridad%20de%20activos%20de%20TI&f=false

7. De Lara Haro, A. (2005). Antecedentes de la Administración del Riesgo. Medición y Control de Riesgo Financiero (pp. 13). México: Editorial Limusa, S.A. Recuperado de http://books.google.com.do/books?id=PrQ-vTEWLqoC&printsec=frontcover&dq=que+es+el+riesgo&hl=es&sa=X&ei=taEgU7DCIYykkQes2YHwDQ&redir_esc=y#v=onepage&q=que%20es%20el%20riesgo&f=false

8. itSMF International (2005). Gestión de la Continuidad de Servicios de TI. Fundamentos de Gestión de Servicios de TI Basado en ITIL (pp. 159). Holanda: Van Haren Publishing. Recuperado de http://books.google.com.do/books?id=nmw4zEMcyhsC&pg=PT171&dq=Continuidad+de+negocios&hl=es&sa=X&ei=xbogU7mtJOnN0AHs54Fw&redir_esc=y#v=onepage&q=Continuidad%20de%20negocios&f=false

9. Martínez Ponce de León, J., (2002). Los Análisis de Riesgos (Marco Teórico). Introducción al Análisis de Riesgos (pp. 23). México: Editorial Limusa, S.A. Recuperado de http://books.google.com.do/books?id=UZOzKXcpfJQC&pg=PA23&dq=Analisis+y+evaluacion+de+riesgo&hl=es&sa=X&ei=-r8gU7rvHJK10AGj-oCgAQ&redir_esc=y#v=onepage&q=Analisis%20y%20evaluacion%20de%20riesgo&f=false

10. Suárez y Alonso, R. (2010). Conceptos Generales de las Tecnologías de la Información y la Comunicación. Tecnología de la Información y la Comunicación (pp. 02). España: Ideas Propias Editorial. Recuperado de http://books.google.com.do/books?id=oPRegn3QhpgC&printsec=frontcover&dq=tecnologias+de+la+informacion+y+comunicacion&hl=es&sa=X&ei=o_cqU-OLMqGR0AHWh4GgCw&redir_esc=y#v=onepage&q=tecnologias%20de%20la%20informacion%20y%20comunicacion&f=false

11. Colegio de Contadores Públicos de México, A.C, (2013, 08 de Julio). La Importancia de Implementar un Plan de Continuidad de Negocios (2da Parte). Dinero en Imagen. Recuperado de: http://www.dineroenimagen.com/2013-07-08/22715

GLOSARIO

Continuidad: Circunstancia de suceder o hacerse algo sin interrupción.

Procesamiento: Corrida de las operaciones o cuadres de las transacciones electrónicas.

Transacción: Para la economía, las finanzas o el comercio, una transacción es una operación de compra y venta. Cuando alguien vende un producto a un comprador, está llevando a cabo una transacción

Hardware: partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Software: equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Tecnología: conjunto de conocimientos técnicos, científicamente ordenados, que permiten diseñar y crear bienes y servicios que facilitan la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de la humanidad.

Router: dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI.

Transerver: equipo especializado en el flujo y procesamiento de las transacciones electrónicas.

Firewall: parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Quality Assurance (QA): conjunto de actividades planificadas y sistemáticas aplicadas en un Sistema de Calidad para que los requisitos de calidad de un producto o servicio sean satisfechos.

Servidor: En informática, un servidor es un nodo que, formando parte de una red, provee servicios a otros nodos denominados clientes.

ACH: Una transferencia ACH es una transferencia electrónica de fondos entre bancos y cooperativas de crédito a través de lo que se conoce como la red de Cámara de Compensación Automatizada.

ATH: transacciones realizadas por los cajeros automáticos de las instituciones financieras.

POS: equipo físico utilizado para realizar transacciones bancarias en los comercios afiliados a la empresa suplidora.

Backup: copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

Desktop: computadora personal que es diseñada para ser usada en una ubicación fija, como un escritorio.

Laptop: es un ordenador personal móvil o transportable, que pesa normalmente entre 1 y 3 kg. Los ordenadores portátiles son capaces de realizar la mayor parte de las tareas que realizan los ordenadores de escritorio.

Base de Datos: conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido; una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta.

TI: el concepto profesionales TI se emplea para englobar todos aquellos expertos relacionado al ámbito de las tecnologías de la información.

Recuperación: es la acción y efecto de recuperar o recuperarse (volver en sí o a un estado de normalidad, volver a tomar lo que antes se tenía, compensar).

Plan: es una intención o un proyecto. Se trata de un modelo sistemático que se elabora antes de realizar una acción, con el objetivo de dirigirla y encauzarla. En este sentido, un plan también es un escrito que precisa los detalles necesarios para realizar una obra.

Datos en Espejo (Mirroring): es el procedimiento de protección de datos y de acceso a los mismos en los equipos informáticos implementado en la tecnología de RAID1. Consiste en la idea básica de tener dos discos duros conectados.

Mejores Prácticas: se entiende un conjunto coherente de acciones que han rendido buen o incluso excelente servicio en un determinado contexto y que se espera que, en contextos similares, rindan similares resultados.

Activo: bien que la empresa posee y que pueden convertirse en dinero u otros medios líquidos equivalentes.

Six Sigma: metodología de mejora de procesos, centrada en la reducción de la variabilidad de los mismos, consiguiendo reducir o eliminar los defectos o fallas en la entrega de un producto o servicio al cliente.

Red: conjunto de medios (transmisión y conmutación), tecnologías (procesado, multiplexación, modulaciones), protocolos y facilidades en general, necesarios para el intercambio de información entre los usuarios de la red.

Estrategia: es un conjunto de acciones planificadas sistemáticamente en el tiempo que se llevan a cabo para lograr un determinado fin o misión.

Clustering: División de los datos en grupos de objetos similares, Este proceso ayuda a la agrupación estructural de un conjunto de datos.

Replicación: es el proceso de copiar y mantener actualizados los datos en varios nodos de bases de datos ya sean estos persistentes o no. Éste usa un concepto donde existe un nodo amo o maestro (master) y otros sirvientes o esclavos (slaves).

Sniffer: Sistema especializado en las evaluaciones de la transferencia de datos de una red determinada.

Checklist: documento que detalla uno por uno distintos aspectos que se deben analizar, comprobar, verificar, etc.

Repositorio: Un repositorio, depósito o archivo es un sitio centralizado donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos.

ANEXOS

Anexo I

DECANATO DE INGENIERÍA E INFORMÁTICA

ESCUELA DE INFORMÁTICA

Plan de Continuidad del Negocio para el Área de TI del Centro de Procesamiento Transaccional, S.A. para el 2014.

Sustentantes:

Félix José Rodríguez Paulino 2006-0625

Arturo Tomas García Estrella 2007-2239

Iván Emmanuel Martínez Naranjo 2008-0248

Asesores:

Ing. Ramón Gómez

Anteproyecto de la Monografía para Optar por el Título de:

Ingeniero en Sistemas de Información

Distrito Nacional, República Dominicana

2014

Plan de Continuidad del Negocio para el Área de TI del Centro de Procesamiento Transaccional, S.A. para el 2014.

1. SELECCIÓN DEL TÍTULO Y DEFINICIÓN DEL TEMA

Plan de Continuidad del Negocio para el Área de TI del Centro de Procesamiento Transaccional, S.A. para el 2014.

1.1. DEFINICIÓN DEL TEMA

En este proyecto de grado se desarrollará un Plan de Continuidad de Negocio para el área de TI (Disaster Recovery Plan, DRP), para garantizar la adecuada continuidad de los recursos tecnológicos ante cualquier evento que amenace el adecuado funcionamiento de los procesos críticos del Centro de Procesamiento Transaccional, S.A. Este aseguramiento antes mencionado apoyará los planes estratégicos de la organización para así mantener la disponibilidad, integridad y confiabilidad de las transacciones procesadas.

2. PLANTEAMIENTO DEL PROBLEMA

En los últimos años se han producido un considerable aumento en las catástrofes naturales que ha afectado las empresas y sus operaciones, aumentando la preocupación de asegurar los activos (recursos humanos, la información y su infraestructura) de las organizaciones.

Tomando en cuenta estas situaciones las empresas continuamente se ven afectadas por diferentes situaciones que representan un alto riesgo en sus operaciones, dentro de están los terremotos, tsunamis, huracanes, erupciones, deslizamientos y otros eventos los cuales provienen del sector humano, como el robo de información, los ataques cibernéticos, clonaciones de identidad y demás situaciones que afecta directa e indirectamente una organización.

Según IBM de las empresas que han tenido una pérdida principal de registros automatizados, el 43 % nunca vuelve a abrir, el 51 % cierra en menos de dos años y sólo el 6 % sobrevivirá a largo plazo[37].

Para estos se desarrollan planes de continuidad o recuperaciones ante desastres los cuales se documentan basados en estudios y/o análisis que reflejan niveles claves dentro de las organizaciones. En la actualidad estos planes ayudan a mantener un nivel de confiabilidad en los activos críticos para las diferentes áreas de servicios.

En los planes de recuperación ante desastres se desarrollan temas como: Análisis de Impacto al Negocio (Business Impact Analysis, BIA), Evaluación de Riesgos, Levantamiento de los Procesos Claves, entre otros temas que son de igual forma importantes para un adecuado desarrollo del plan.

En República Dominicana se han vivido situaciones que han puesto en crisis amplios sectores empresariales, hechos como ciclón de San Zenón en el 1930, huracán George en el 1998, tormenta Odette para el 2003, inundación en Puerto

[37] Natalia, (2013, 1 de marzo). Plan de Recuperación ante desastres (DRP). *Celingest: Feel The Cloud*. Recuperado de http://blog.celingest.com/2013/03/01/recuperacion-desastres-disaster-recovery/

Plata en 2005, el terremoto de Haití para el 2010 y otra situación trágicas han impulsado las organizaciones al desarrollo de planes de recuperaciones para el aseguramiento del negocio.

En el caso del Centro de Procesamiento Transaccional, S.A., la cual es una empresa que nace por la iniciativa de varias entidades financieras, dispone de procesos como el procesamiento de transacciones de tarjetas, el re direccionamiento de transacciones bancarias, servicios de cobros y otros procesos que son de alta prioridad para el día a día de la ciudadanía.

Actualmente el Centro de Procesamiento Transaccional, S.A. no cuenta con un Plan de Recuperación ante Desastres que esté enfocado directamente en los riesgos potenciales de sus equipos tecnológicos, sus operaciones criticas como las de Finanzas (20%), Negocios y área Técnica (20%) y Tecnología (60%), situación que en caso de un evento aumentaría el riesgo de pérdidas financieras y mala imagen corporativo.

3. OBJETIVOS DE LA INVESTIGACIÓN

3.1. OBJETIVO GENERAL

Desarrollar un Plan de Continuidad de Negocio para el área de TI (Disaster Recovery Plan, DRP) que garantice la continuidad de las operaciones tecnológicas y la protección de los activos para el Centro de Procesamiento Transaccional, S.A.

3.2. OBJETIVOS ESPECÍFICOS

- Elaborar un plan de continuidad del negocio para el Centro de Procesamiento Transaccional.
- Enlistar las ventajas que ofrece la implementación de un plan de continuidad de negocios para el Centro de Procesamiento Transaccional.
- Enlistar las desventajas que tiene la implementación de un plan de continuidad de negocios para el Centro de Procesamiento Transaccional.
- Establecer las características de un adecuado plan de continuidad de negocio para el Centro de Procesamiento Transaccional.
- Establecer la influencia de un plan de continuidad para los clientes, empleados y procesos.
- Indicar los procesos claves a incluir en el plan de continuidad de negocios.
- Identificar las normas, estándares y/o marcos de referencias que hacen relación a la necesidad de disponer de un plan de continuidad de negocios.

4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

4.1. JUSTIFICACIÓN TEÓRICA

Este proyecto busca aplicar mediante procesos de análisis, evaluaciones, entendimientos y recomendaciones el desarrollo de un Plan de Recuperación ante

Desastres para el Centro de Procesamiento Transaccional, S.A. con el propósito de mantener la continuidad de las operaciones en el procesamiento de transacciones de tarjetas ante cualquier ambiente de alto riesgo.

Este plan se enfocará al cumplimiento de las directrices reglamentarias expuestas por diferentes organizaciones que con el pasar del tiempo han adoptado mejores prácticas en entidades independientes como especificas en la industria, algunas de estas entidades o mejores prácticas están:

- Instituto de Continuidad del Negocio (BCI).
- Instituto Internacional de Recuperación en Caso de Desastres (Disaster Recovery Institute International, DRII).
- Agencia Nacional de Estados Unidos contra Incendios (NFPA).
- Asociación Federal de Estados Unidos para el Manejo de Emergencias (FEMA).
- Norma COBIT.
- BS 25999.
- Instituto Nacional de Estándares y Tecnología de los Estados Unidos (US National Institute of Standards and Technology).

Todas estas entidades y normas están directamente asociadas para apoyar las iniciativas en el desarrollo de planes de continuidad y recuperación del negocio, brindando orientación y metodologías de cómo realizar esos procesos claves.

4.2. JUSTIFICACIÓN METODOLÓGICA

En esta investigación se emplearán diversas técnicas e instrumentos para la identificación de potenciales riesgos y amenazas, a los cuales se expone diariamente el Centro de Procesamiento Transaccional, S.A., dentro de estas están:

Entrevistas: Dirigida a individuos específicos que están aptos para brindar ciertas informaciones de forma detallada y especifica.

Encuestas: Dirigida a una población, aplicadas a una muestra de la misma. Esto para representar datos e informaciones en forma masiva.

4.3. JUSTIFICACIÓN PRÁCTICA

Con el desarrollo del Plan de Continuidad de Negocio para el área de TI, se busca mitigar los eventos de alto riesgo en las que se expone día a día las operaciones de que soportan al Centro de Procesamiento Transaccional, S.A.

También se busca una continua planificación que garantice la existencia de adecuados controles que eviten cualquier interrupción en los sistemas de información. Como se detalla en la problemática del Centro, la dependencia de la tecnología para las operaciones del negocio sobrepasa el 60% directamente y casi un 90% indirectamente (ya que existen muchos procesos que son la tecnología aumentaría significativamente su tiempo de realización.

Sin lugar a duda la ausencia del soporte tecnológico para la organización representaría situación de crisis en sus operaciones internas y externas, exponiendo a la empresa a riesgos significativos, como: pérdidas financieras, falta de integridad y/o pérdidas de la información, mala imagen corporativa, entre otros que pueden afectar de forma drástica su posicionamiento.

5. TIPO DE INVESTIGACIÓN

Para la realización de nuestro trabajo de grado se utilizarán los siguientes tipos de investigación:

a) **Descriptiva:** En esta investigación se utilizará el método descriptivo a partir de informaciones que aborden la realidad práctica, las cuales se llevarán a cabo mediante análisis y evaluaciones a los procesos diarios realizados en el Centro de Procesamiento Transaccional, S.A., con el objetivo de determinar la importancia de desarrollar un Plan de Recuperación ante Desastres que pretende mejorar la efectividad y disponibilidad de los sistemas de información ante cualquier amenaza o riesgo.
b) **Explicativa:** Con este tipo de investigación realizaremos pruebas que nos ayuden a determinar las razones por las cuales ocurren ciertos fenómenos y la magnitud de sus consecuencias. De igual forma las informaciones recolectadas serán planteadas mediante análisis, síntesis e interpretaciones.
c) **Documental:** Para este tipo de investigación se realizará análisis de informaciones publicadas en medios escritos, como libros, revistas y otros

trabajos de investigaciones, los cuales proveerán datos claves para el desarrollo de nuestro trabajo de grado. De este modo se sustentará el desarrollo de un Plan de Recuperación ante Desastres para el Centro de Procesamiento Transaccional, S.A.

6. MARCO DE REFERENCIA

6.1. MARCO TEÓRICO

Un plan de recuperación ante desastres es normalmente un conjunto de documentos que muestran todas las actividades que se necesitan llevar a cabo en caso de un desastre. El plan guía al lector para que sepa donde obtener la información o ayuda apropiadas. Todo el personal clave en la empresa necesita estar al corriente del plan, estar familiarizado con su contenido y saber cómo acceder a él[38].

Conseguir que el desarrollo e implementación de un Plan de Continuidad de Negocio sea un proyecto estratégico de toda la organización, involucrando a todos los departamentos y divisiones para que la información necesaria fluya de forma continuada en la medida de las necesidades de los responsables de llevarlo adelante[39].

[38] Chapman, J. (2002). *Plan de Recuperación de Negocios en una Semana.* Barcelona: Gestión 2000.
[39] Martínez, J.G. (2004). *Planes de Contingencia La Continuidad del Negocio en las Organizaciones*. Madrid: Díaz de Santos, S.A.

Recuperación ante Desastres (Disaster Recovery Plan, DRP) es un proceso continuo. Una vez que se ha definido la criticidad de los procesos de negocios, así como los servicios de TI de soportes, sistemas y datos, estos se revisan y se revisitan periódicamente. Hay como mínimo dos resultados importantes de DRP:

- Cambios en la infraestructura de TI (servidores, redes, sistemas de almacenamiento de datos, etc.), cambios en procesos de soportes (aumentar la madurez), procedimientos y estructura organizativa (por ejemplo, nuevo personal de plantilla o nuevos roles). Estos cambios se combinan en programas que se expanden de tres a cinco años, conocidos a menudo como estrategias DR de TI.
- Los planes (planes DR) desarrollados como parte de este proceso guiarán la respuesta a incidentes desde simples emergencias hasta desastres mayores. Los planes van desde simples procedimientos a nivel de departamento a planes modulares de varias capas que cubren varias ubicaciones y varias líneas de negocio.

El objetivo principal del proceso de Recuperación ante Desastres (DRP) es responde a incidentes que pueden tener un impacto en personas y en la capacidad de las operaciones de entregar bienes y servicios al mercado y de cumplir con los requerimientos regulatorios[40].

Todo este deseo de poder disponer de documentaciones, procesos y procedimientos que aseguren los activos de una empresa son sin lugar a duda

[40] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Planificación de Recuperación en Caso de Desastres (DRP). *Manual de Preparación al Examen CISA 2012* (pp. 326). Estados Unidos de América: ISACA.

temas críticas en la continua gestión de seguridad de las empresas. Para estos existen diferentes normas, mejores prácticas o marcos de referencias las cuales ayudan al adecuado desarrollo de estos tipos de proyectos.

Dependiente el tamaño o los requerimientos de la organización, un BCP puede constar de uno o más documentos. Estos deben incluir: Plan de Continuidad de las Operaciones, Plan de Recuperación ante Desastres y Plan de Restablecimiento del Negocio. También se pueden incluir temas como: Continuidad del plan de apoyo / Plan de Contingencia de TI, Plan de Comunicaciones de Crisis, Plan de Respuesta a Incidentes, Plan de Transporte, Plan de Emergencia del Ocupante y Plan de Evacuación y Reubicación de Emergencia[41].

Hay grandes beneficios que se pueden obtener a partir de la elaboración de un plan continuidad de negocio y recuperación de desastres. Algunos de estos son:

- La capacidad de proteger los sistemas críticos para la empresa.
- Reducción de pérdidas tras un incidente.
- Garantizar la fiabilidad de los sistemas de reserva.
- Proporcionar un sentido de seguridad.
- Minimizar el riesgo de retrasos.
- Proporcionar un estándar para probar el plan.
- Minimizar la toma de decisiones en caso de desastre.
- La reducción de las posibles responsabilidades legales.

[41] Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). Elementos de un Plan de Continuidad del Negocio. *Manual de Preparación al Examen CISA 2012* (pp. 136). Estados Unidos de América: ISACA.

- Mejora de la eficiencia general de la organización y la identificación de la relación de bienes y recursos humanos y financieros para los servicios críticos.

Todas las organizaciones están en riesgo de padecer cualquier desastre que haga perder los activos correspondientes a la información de su negocio. Un Plan de recuperación es una herramienta que permite a las empresas no perder información crítica y seguir ofreciendo servicios a pesar de una interrupción[42].

6.2. MARCO CONCEPTUAL

Sistema de Información: es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Tecnología de la Información: Es el conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de la información para apoyar las diferentes soluciones tecnológicas.

Plan de Recuperación ante Desastres (Disaster Recovery Plan, DRP): Es un proceso documentado o conjunto de procedimientos para recuperar y proteger la infraestructura tecnológica de una empresa en caso de un desastre.

[42] Natalia, (2013, 1 de marzo). Plan de Recuperación ante desastres (DRP). *Celingest: Feel The Cloud*. Recuperado de http://blog.celingest.com/2013/03/01/recuperacion-desastres-disaster-recovery/

Contingencia: Riesgo o suceso que puede ocurrir y se debe prever. Este es un concepto que procede del latín contingentĭa y suele referirse a algo que es probable que ocurra, aunque no se tiene una certeza al respecto. Por lo tanto, es lo posible o aquello que puede, o no, concretarse.

Vulnerabilidad: son puntos débiles de un recurso que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo.

Desastre: Es un hecho natural o provocado por el ser humano que afecta negativamente a la vida, al sustento o a la industria y desemboca con frecuencia en cambios permanentes en las sociedades humanas, en los ecosistemas y en el medio ambiente.

Amenaza: Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial), también podríamos decir que es la causa de riesgo que crea aptitud dañina sobre personas y bienes.

Riesgo: Es la vulnerabilidad ante un potencial perjuicio o daño para las unidades, personas, organizaciones o entidades. Por tanto, el riesgo se refiere sólo a la teórica "posibilidad de daño" bajo determinadas circunstancias

Análisis de Impacto al Negocio (Business Impact Analysis, BIA): Guía que determine que necesita ser recuperado y el tiempo que tarde dicha recuperación, actividades que en el Plan de Continuidad de Negocios se convierten quizás en las más difíciles y críticas por realizar adecuadamente.

Objetivo de Punto de Recuperación (Recovery Point Objective, RPO): Es cuando la infraestructura, ya comenzada nuevamente, comenzará a hacerse evidente. También es definido como el punto de recuperación de los datos. Es decir, en qué momento temporal anterior a la pérdida se recuperan los datos.

Objetivo de Tiempo de Recuperación (Recovery Time Objetive, RTO): Define el límite de tiempo máximo tolerable dentro del cual se recuperan los datos. Si se produce un desastre y los sistemas deben estar disponibles inmediatamente, pero se permite que haya alguna pérdida de datos, el RTO es cero. Sin embargo, si se tolera una hora de recuperación de datos, el RTO es una hora.

6.3. MARCO ESPACIAL

Este proyecto será realizado en las instalaciones del Centro de Procesamiento Transaccional, S.A., Santo Domingo, Distrito Nacional, directamente apoyados en las oficinas de la Dirección de Tecnología y ciertas áreas de Negocio de la empresa.

6.4. MARCO TEMPORAL

Esta investigación será evaluada y desarrollada basándonos específicamente en los meses enero – abril el 2014.

7. MÉTODOS, PROCEDIMIENTOS Y TÉCNICAS UTILIZADAS EN LA INVESTIGACIÓN.

7.1. MÉTODOS

Dentro de nuestras metodologías, que soportarán todos los análisis e interpretaciones referentes, para esto se utilizará los siguientes métodos:

a) **Método Inductivo:** Para esta investigación se partirá de hechos y datos particulares a recoger para desarrollar el Plan de Continuidad de Negocios para el área de TI.

b) **Método de Análisis:** Se utilizará este método luego del proceso inductivo para realizar un análisis a las informaciones recogidas. Esto es esencial para llevar a cabo una evaluación.

c) **Método de Síntesis:** Por último se usará este método ya que luego de llevar a cabo el análisis se procedería a generar conclusiones y resúmenes para completar la evaluación junto con sus objetivos.

7.2. PROCEDIMIENTOS

Con las informaciones obtenidas mediante los diferentes métodos antes mencionados se realizarán las siguientes actividades que soportarán nuestra monografía:

a) Levantamiento de información y procesos del Centro de Procesamiento Transaccional, S.A.
b) Análisis y evaluación de riesgos.
c) Análisis de Impacto al Negocio (BIA).
d) Implementación de las estrategias de recuperación del Plan ante Desastres.
e) Desarrollo del Plan de Continuidad de Negocio para el área de TI.
f) Realización de las documentaciones referentes a las pruebas y mantenimientos del Plan.
g) Documentaciones del informe final del proyecto de recuperación.

7.3. TÉCNICAS

En esta investigación, para la recolección de datos e informaciones se usarán las siguientes técnicas e instrumentos:

- **Entrevistas:** Dirigida a individuos específicos que están aptos para brindar ciertas informaciones de forma detallada sobre los procesos claves de la empresa.
- **Cuestionarios:** Para estos se utilizará un conjunto de preguntas especializadas, realizadas de manera metódica en los hechos y aspectos dirigidos a una población y aplicadas a una muestra de la misma. Con esto se representarán datos e informaciones en forma masiva.

8. TABLA DE CONTENIDO

Capítulo VII

PRUEBAS Y MANTENIMIENTOS DEL PLAN

7.1 Importancia de las Pruebas en un Plan ante Desastres.

7.2 Programa de Pruebas del Plan.

7.2.1 Especificaciones de las Pruebas.

7.2.2 Ejecución de las Pruebas del Plan.

7.2.3 Documentaciones de los Resultados.

7.3 Mantenimiento del Plan.

Capítulo VIII

PLAN DE MANEJO DE COMUNICACIÓN ANTE INCIDENTES Y CRISIS

Capítulo IX

PROGRAMA DE CAPACITACIÓN, CONCIENTIZACIÓN Y DIFUSIÓN DEL PLAN

CONCLUSIÓN

BIBLIOGRAFÍA

GLOSARIO

ANEXOS

9. FUENTES DE INFORMACIÓN

- Asociación de Auditoria y Control de Sistemas de Información (ISACA) (2012). *Manual de Preparación al Examen CISA 2012*. Estados Unidos de América: ISACA.

- Alarcón, V.F. (2006). *Desarrollo de Sistemas de Información: Una metodología basada en el modelado*. Barcelona: UPC. Recuperado de http://books.google.com.do/books?id=pTTQ735ac1EC&printsec=frontcover&dq=Sistema+de+Informaci%C3%B3n&hl=es&sa=X&ei=MDr-UrTAEaKRygGHjIDABg&redir_esc=y#v=onepage&q=Sistema%20de%20Informaci%C3%B3n&f=false
- Asociación Nacional para la Protección contra Incendios (National Fire Protection Association, NFPA). (1996), Norma para la Instalación de Sistemas de Rociadores. Argentina: Instituto Argentino de Normalización.
- Chapman, J. (2002). *Plan de Recuperación de Negocios en una Semana*. Barcelona: Gestión 2000.
- Instituto de Continuidad de Negocio (Business Continuity Institute, BCI) (2010), *Lineamientos para la Buena Practica 2010 – Guía para la Gestión de las Buenas Practicas de la Continuidad del Negocio* (Trad. Félix Rodríguez). Reino Unido: BCI.
- Martínez, J.G. (2004). *Planes de Contingencia La Continuidad del Negocio en las Organizaciones*. Madrid: Díaz de Santos, S.A.
- Organización Internacional de Estandarización y Comisión Electrónica Internacional (ISO/IEC), (2005), Estándar Internacional ISO 27002 Tecnología de la Información. Estados Unidos.
- Natalia, (2013, 1 de marzo). Plan de Recuperación ante desastres (DRP). Celingest: Feel The Cloud. Recuperado de http://blog.celingest.com/2013/03/01/recuperacion-desastres-disaster-recovery/

Anexo II

Centro de Procesamiento Transaccional, S.A.

Formulario Levantamiento de Procesos Críticos

En este documento se enlistaran los procesos de negocios de la empresa, para el apoyo al levantamiento de información de los procesos críticos.

Proceso de Negocio	Periodo de Tiempo Máximo sin Servicio (PTMS)	Equipo / Sistema que lo Soporta	Perdida de Data Tolerable en Tiempo (PDTT)

PTMS / PDTT:

Prioridad 1: <24hrs
Prioridad 2: 25-48hrs
Prioridad 3: 49-72hrs
Prioridad 4: 4-7Days
Prioridad 5: 8-14Days
Prioridad 6: 15-30Days
Prioridad 7: >30Days

Responsable	
Posición	
Departamento	
Correo electrónico	
Fecha	

Centro de Procesamiento Transaccional, S.A.

Formulario Levantamiento de Procesos Críticos

En este documento se identifican, por área y responsable de negocio, los diferentes procesos críticos del Centro de Procesamiento Transaccional, S.A.

Proceso	Sub-proceso	Descripción	Uso (Diario/Semanal /Mensual)	Supervisor