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

Andrés Cárdenas Pallo[1],Mario Ron Egas[2] ,Víctor Paliz[3]

1 Escuela Politécnica del Ejército, Ecuador, andrewca.leo@gmail.com
2 Escuela Politécnica del Ejército, Ecuador, mbron@espe.edu.ec
3 Escuela Politécnica del Ejército, Ecuador, vmpaliz@espe.edu.ec

RESUMEN

Las empresas experimentan situaciones de emergencia, directa o indirectamente, las cuales necesitan respuestas inmediatas. El Plan de Continuidad del Negocio (BCP) permite establecer los procedimientos para asegurar la continuidad de una empresa en caso de que esta se viera sometida a una interrupción no deseada de su negocio. El presente trabajo está orientado al desarrollo del Plan de Continuidad del Negocio (BCP) dentro de una empresa de servicios de Seguros de Vida por la factibilidad de conocer sus procesos y tener la apertura para este plan. El desarrollo está basado en la norma ISO 22301 "Sistema de Gestión de la Continuidad del Negocio", siguiendo sus fases el trabajo incluye una breve descripción de la empresa, se evalúa los posibles riesgos y amenazas a las que está expuesta, se realiza un Análisis de Impacto del Negocio(BIA) que es el punto de partida para crear las estrategias de continuidad, se define un conjunto de equipos para el restablecimiento de operaciones y los procedimientos a utilizarse , y se definió objetivamente los procesos críticos de la compañía que apoya a la toma de decisiones empresariales.

Palabras Clave: Plan de Continuidad del Negocio, Análisis de Impactos del Negocio, Riesgos, Amenazas, Equipos de Crisis.

ABSTRACT

Companies have emergency situations, directly or indirectly, which need immediate answers. The Business Continuity Plan (BCP) set procedures to ensure the continuity of the process company in case this is seeing subjected to unwanted interruption. The work will develop the Business Continuity Plan (BCP) for a Life Insurance company because the feasibility to obtain their processes and knowledge of their business. The development is based on the ISO 22301 Management System " Business Continuity ", following work stages a brief description of the company, we evaluate the potential risks and threats to which it is exposed, it takes an Analysis Business Impact Assessment (BIA) which is the starting point to create continuity strategies, defines a set of equipment for the restoration of operations and procedures to be used, and objectively defined critical processes of the company that supports business decisions.

KeyWords: Business Continuity Plan, Business Impact Analysis, Risk, Threats, Crisis Teams.

I. INTRODUCCIÓN

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

La empresa EQUIVIDA S A inició un proceso de mejoramiento de sus políticas y procesos y encontró la necesidad de desarrollar un Plan de Continuidad del Negocio[1] con enfoque en los procesos críticos de la compañía.

Los directivos tendrán a su alcance un plan estratégico de prevención y recuperación que les permita tomar decisiones asertivas en momentos de crisis, también la empresa afirmará la solidez de sus servicios ante cualquier desastre.

El plan contiene las políticas de Continuidad del Negocio, los procesos críticos del negocio, los resultados del análisis de riesgos y las estrategias y procedimientos de mitigación y recuperación.

II. MÉTODOS

METODOLOGÍA PARA EL PLAN DE CONTINUIDAD DEL NEGOCIO.

La metodología aplicada se basa en la norma ISO 22301 “Sistema de Gestión de Continuidad del Negocio” que inicia desde el entendimiento del negocio, la identificación de posibles riesgos, su impacto y valoración, definición de estrategias, elaboración del plan, desarrollo de una cultura, hasta la prueba, mantenimiento y auditoría del plan[7]; Las fases planteadas en la metodología son:

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

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

Estrategia de continuidad de negocio: Las estrategias son desarrolladas para identificar disposiciones que permitan que la organización proteja y recupere actividades críticas, basadas en la tolerancia de riesgo organizacional y dentro de objetivos de tiempo de recuperación definidos.

Procedimientos de continuidad de negocio: La organización debe documentar los procedimientos (incluyendo las disposiciones necesarias) para asegurar la continuidad de las actividades, los procedimientos establecen un protocolo adecuado de comunicaciones internas y externas, son específicos y flexibles para responder a amenazas no anticipadas y a condiciones internas y externas cambiantes.

III. DESARROLLO DEL PLAN DE CONTINUIDAD DEL NEGOCIO

Para el desarrollo del plan es imprescindible el conocimiento de la empresa, su estrategia empresarial, su misión y los procesos del negocio.

Estrategia Empresarial de Equivida

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

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

Análisis del Negocio y Evaluación de Riesgos

Para el análisis del negocio los procesos de la compañía son divididos en: Procesos Primarios, Procesos de Apoyo y Procesos de Gestión como lo muestra la Fig.1

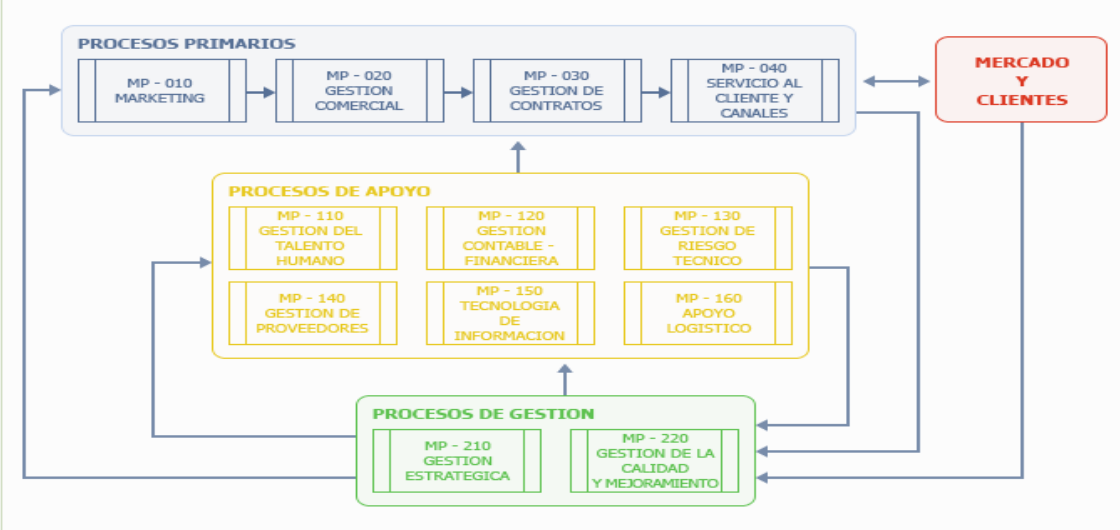

Fig. 1: Macroprocesos Equivida

Los procesos críticos que soportan las operaciones de la compañía son los indicados en la Tabla 1, con su análisis de impacto con enfoque al cliente y empresa.

Tabla 1: Análisis impacto procesos

MACROPROCESOS	CÓDIGO	PROCESO	IMPACTO EN LA EMPRESA	IMPACTO EN EL CLIENTE	TOTAL
Gestión Comercial	PR-021	Ventas Colectivo	3	1	4
Gestión Comercial	PR-022	Incremento de negocio y fidelización de los clientes	3	1	4
Gestión Comercial	PR-023	Ventas Masivas	3	1	4
Gestión Comercial	PR-025	Gestión Posventa Individual – Mantenimiento	3	2	5
Gestión de Contratos	PR-031	Administración de operaciones contractuales colectivo	3	3	**6**
Gestión de Contratos	PR-032	Movimientos y facturación colectivo	3	3	**6**
Gestión de contratos	PR-033	Recaudos	3	3	**6**
Gestión de Contratos	PR-034	Beneficios y prestaciones al cliente – siniestros	3	3	**6**
Gestión de Contratos	PR-035	Administración de contratos individuales	3	3	**6**
Servicio al cliente y canales	PR-041	Atención al cliente y canales vida individual	3	3	**6**
Gestión Contable - Financiera	PR-123	Pagos	3	3	**6**

A continuación se realiza el análisis de riesgo y se determina su probabilidad e impacto. La tabla 2 permite determinar los riesgos propensos de la compañía [4][5].

Tabla 2: Análisis de riesgos propensos

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

En función de los riesgos que se marco como posibles, se establece los escenarios en que una amenaza puede convertirse en un incidente de seguridad. La tabla 3 determina los escenarios y vulnerabilidades expuestas.

Tabla 3: Análisis de vulnerabilidades

ESCENARIOS	VULNERABILIDAD
Fuego inesperado por cortocircuito de cables encima del cielo raso	Material inflamable en todas las áreas de la compañía
Ingreso de personas extrañas al edificio y robo de equipos	No se cuenta con controles de acceso al edificio
Extracción de información confidencial a través de dispositivos portables	No existe políticas de desactivación de los puertos de los dispositivos
Código mal intencionado instalado en los exploradores Web para robo de credenciales	Ausencia de procedimientos para detección de programas espías.
Accesos a sistemas de información de clientes por personas inescrupulosas	Información de clientes en bases de datos no ofuscada
Indisponibilidad del internet por un fallo del proveedor.	No se cuenta con un proveedor secundario de internet
Informe de Roles de pagos en carpetas compartidas para toda la empresa	Carpetas compartidas a nivel de toda la empresa sin controles de autentificación
Interrupción de la energía eléctrica por más de 5 horas	No se cuenta con una planta eléctrica de alta capacidad
Mala configuración de los firewalls expuestos a internet.	Falta de expertos en seguridades de dispositivos físicos

Para gestionar los riesgos y mitigarlos en lo posible, se propone las siguientes contramedidas descritas en la Tabla 4:

Tabla 4: Contramedidas de amenazas

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

IV. PROCEDIMIENTOS DE RECUPERACIÓN Y CONTINUIDAD

En esta fase se define los procedimientos[3], políticas y equipos para el restablecimiento del negocio.

a. PROCEDIMIENTOS PARA LA CONTINUIDAD

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

PROCEDIMIENTO DE EJECUCIÓN DEL PLAN: Una vez notificado del incidente el Comité de crisis se reunirá en el punto de encuentro definido, se evaluará el grado del incidente y decidirá si el Plan de Continuidad del Negocio es puesto en marcha.

PROCEDIMIENTO DE NOTIFICACIÓN DE EJECUCIÓN DEL PLAN: El árbol de notificación y llamadas para avisar a los diferentes equipos se detalla en la Fig. 2

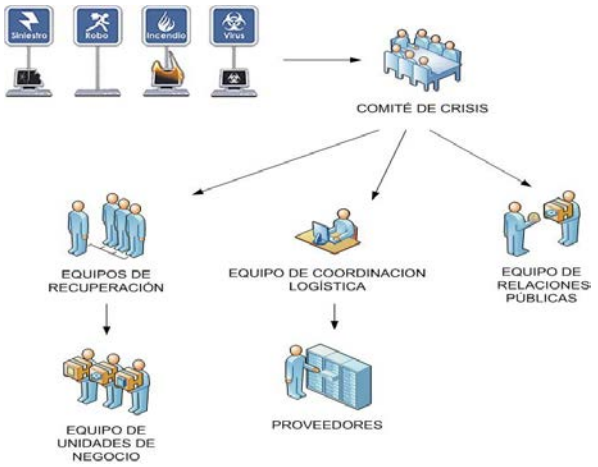

Fig. 2: Procedimiento de ejecución del plan

PROCEDIMIENTOS PARA INCIDENTES DISRUPTIVOS: Los incidentes relacionados con tecnología de la información y de la comunicación son informados telefónicamente a la Jefatura de Sistemas, los demás incidentes son informados telefónicamente a la Jefatura de administración.

GESTIÓN DE INCIDENTES DISRUPTIVOS: Para la gestión se informa a todas las personas responsables sobre la ocurrencia del incidente dentro de su área de responsabilidad y se notifica al comité de crisis, que debe evaluar si es necesario alertar a alguna de las partes interesadas, la persona responsable de erradicar el incidente debe registrar en el Registro de incidentes todas las acciones tomadas.

EQUIPO DE RECUPERACIÓN: El equipo de recuperación [2] es el encargado de poner en marcha todo el proceso de recuperación para restaurar los servicios en las Oficinas de la Sucursal Viscaya, siguiendo los procedimientos de traslado, recuperación de sistemas y comunicaciones.
Los equipos de recuperación se dividen en:

EQUIPO DE COORDINACIÓN LOGÍSTICA: Es responsable de todo lo relacionado con las necesidades logísticas en función del tipo de incidente.

.EQUIPO DE RELACIONES PÚBLICAS: Es responsable de la comunicación externa e interna. Según el incidente será el responsable de comunicar a clientes y proveedores el tiempo en el que los servicios serán restablecidos.

EQUIPO DE UNIDADES DEL NEGOCIO: Formado por las personas que trabajan con las aplicaciones críticas, y serán los encargados de gestionar a sus supervisados para realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas.

b. FASE DE TRANSICIÓN

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

PROCEDIMIENTO DE PUESTA EN MARCHA DEL CENTRO DE RECUPERACIÓN: Una vez que el equipo de recuperación llegue al Centro de recuperación y que los materiales empiecen a llegar, pueden comenzar a instalar las aplicaciones en los equipos que se encuentran en esta oficina.

c. FASE DE RECUPERACIÓN

PROCEDIMIENTO DE RESTAURACIÓN

El orden de recuperación de las funciones se realizará según la criticidad los sistemas definidos en la Tabla 4.

Tabla 4: Contramedidas de amenazas

Sistema	Descripción	Criticidad
VECTOR	Sistema de modelamiento, control y seguimiento de procesos.	**1**
ADAM	Sistema que administra la nómina de la compañía.	**1**
RISK CONTROL SERVICE	Herramienta de control que tiene como objetivo minimizar el riesgo de establecer vínculos con posibles involucrados o señalados en actividades ilícitas como lavado de activos, narcotráfico o terrorismo,	**2**
SISE	Sistema Integrado de Seguros. Este sistema soporta el core del negocio y la parte administrativa financiera, tiene módulos de: Emisión/Facturación Individual y Colectivo, Reaseguros, Siniestros, Generación Intereses, Retiros y Préstamos, Caja Ingresos, Caja Egresos, Contabilidad, Cierres Mensuales, Consultas, Informática.	**1**
CRM	Sistema automatizado para el control de la fuerza de ventas individual	**2**
PORTAL WEB	Portal diseñado para la prestación de servicios online	**2**

PROCEDIMIENTOS PARA LA RECUPERACIÓN DE INFORMACIÓN DESDE LOS BACKUP.: Dentro de las operaciones diarias en la realización de respaldos el departamento de sistemas genera los respaldos mediante los procesos batch los cuales se encargan de crear los archivos de backup, copiarlos a dispositivos de almacenamiento externos los cuales son: servidores alternos dentro de la misma infraestructura, discos duros en estado compartido y cintas magnéticas.

PROCEDIMIENTO DE DOCUMENTACIÓN Y REGISTRO DE CONFIGURACIONES PARA RECUPERACIÓN: SOFTWARE Y HARDWARE: El departamento de sistemas es el encargado de coordinar la distribución e instalación de los sistemas en los equipos entregados provisionalmente para reanudar las actividades.

PROCEDIMIENTO DE SOPORTE Y GESTIÓN: Una vez recuperados los sistemas, se avisará a los equipos de los departamentos que gestionan los sistemas, fig.3 (listado del equipo de Unidades de Negocio) para que realicen las comprobaciones necesarias que certifiquen que funcionen de manera correcta.

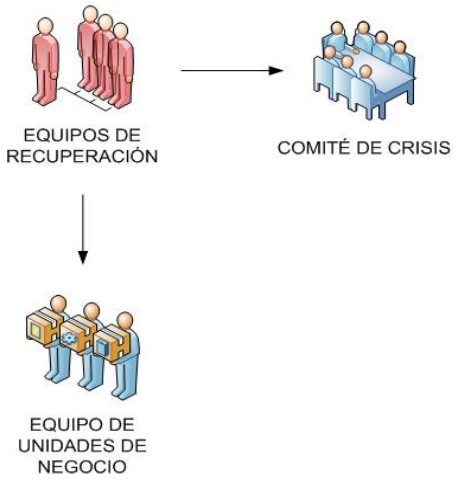

Fig. 3: Procedimiento de soporte y gestión

d. FASE DE VUELTA A LA NORMALIDAD

Una vez restablecido los procesos críticos y solventados la contingencia, hay que definir las diferentes estrategias y acciones para recuperar la normalidad de todos los servicios de la compañía, se realiza una valoración detallada de los equipos e instalaciones dañada. Para ello, el equipo de recuperación junto con el equipo de seguridad, realizarán un listado de los elementos que han sido dañados gravemente y son irrecuperables, así como de todo el material que se puede volver a utilizar. Esta evaluación deberá ser comunicada lo antes posible al equipo director para que determinen las acciones necesarias que lleven a la operación habitual lo antes posible.

ADQUISICIÓN DE NUEVO MATERIAL: Realizada la evaluación del impacto, se determinará la necesidad de nuevo material. El Comité de Crisis contactará con el seguro de la compañía para conocer qué parte cubre el seguro y qué inversión tendrá que hacer la compañía en el material que no se pueda recuperar.

e. FIN DE LA CONTINGENCIA

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

V. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO.

El desarrollo del Plan define objetivamente los procesos críticos de la compañía y permite una consolidación de intereses entre la Alta Dirección y las diferentes Unidades organizativas al constatar que diferentes áreas apoyan a procesos idénticos y generar estrategias efectivas para los incidentes no previstos.

Como trabajo futuro se recomienda:

Dar continuidad al plan con revisiones de los procesos, personas y componentes involucrados a través de talleres al menos una vez al año para generar conciencia de la utilidad del Plan y difundir a los nuevos colaboradores que ingresan a la compañía, para hacerles participe del mismo y fortalecer los Equipos que componen el plan.

VI. REFERENCIAS BIBLIOGRÁFICAS

[1] Borrmart S.A *La necesidad de implantación de un Plan de Continuidad del Negocio.*

[2] Dejan Kosutic (2012) *Equipo del Plan de Continuidad "Business ImpactAssessmentTool.*

[3] Juan Gaspar Martínez *"El Plan de Continuidad del Negocio"*. 1996. McGraw-Hill Interamericana, 2da Edición.

[4] Martin Carrion*, "Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información"* Instituto Nacional de Estadística e Informática. Lima, Febrero 2001

[5] Cristina Gallardo Piedra. *"Análisis de Riesgos Informáticos y elaboración de un Plan de Contingencia TI",* Quito Febrero 2011

[6] Marcelo Moran A., Tesis: *"Elaboración del Plan de Continuidad del Negocio para la Empresa Compteco compra por teléfono consorcio comercial S.A",* Escuela Politécnica del Ejercito, Sangolquí – Ecuador 2011

[7] Gallardo María, Paúl Jácome, Tesis*: "Análisis de riesgos informáticos y elaboración de un plan de contingencia T.I. para la empresa eléctrica Quito S.A",* Escuela Politécnica Nacional, Quito – Ecuador 2011

[8] Laura del Pino J, Tesis: *"Guía de Desarrollo de un Plan de Continuidad del Negocio",* Universidad Politécnica de Madrid, España – Madrid 2009