PLAN DE RECUPERACIÓN DE DESASTRES (DRP) INFORMÁTICOS, EN LA FASE DE ANÁLISIS DE IMPACTO PARA UNA EMPRESA PETROLERA

Acosta Galindo, Ricardo Alfonso
Ricardo.Acosta102@gmail.com
Universidad Piloto de Colombia

Abstract— This article aims to contextualize the importance that a company has Administration Business Continuity (BCM) and its components especially the design of disaster recovery (DRP) with emphasis on its main processes as are the Risk Analysis and Impact Analysis business (BIA) operating as a valuable tool that will enable the company to plan precisely the actions to take in case of adverse events, to ensure business stability and consequently minimize economic losses, having as reference a company in the oil sector.

Keywords: BIA, DRP, Risk analysis

Resumen— Este artículo tiene como objetivo contextualizar la importancia que tiene para una empresa la administración de Continuidad del Negocio (BCM) y sus componentes en especial el diseño del Plan de Recuperación de Desastres (DRP) haciendo énfasis en sus principales procesos como son el Análisis de Riesgos y el Análisis de Impacto del Negocio (BIA) que funcionan como un instrumento valioso que permitirá a la compañía planificar de forma precisa las acciones a emprender en caso de acontecimientos adversos, a fin de garantizar la estabilidad del negocio y en consecuencia minimizar pérdidas económicas, teniendo como referencia una empresa del sector petrolero.

Índice de Términos: Análisis de riesgos, BIA, DRP.

I. INTRODUCCIÓN

Este artículo tiene como objetivo contextualizar la importancia que tiene para una empresa la administración de Continuidad del Negocio (BCM) y sus componentes en especial el diseño del Plan de Recuperación de Desastres (DRP) haciendo énfasis en sus principales procesos como son el Análisis de Riesgos y el Análisis de Impacto del Negocio (BIA) que funcionan como un instrumento valioso que permitirá a la compañía planificar de forma precisa las acciones a emprender en caso de acontecimientos adversos, a fin de garantizar la estabilidad del negocio y en consecuencia minimizar pérdidas económicas, teniendo como referencia una empresa del sector petrolero, la cual cuenta con clientes del sector de los hidrocarburos donde su fuente principal de ingresos es la venta y renta de sus diferentes servicios petroleros, bajo los procesos de licitación con las diferentes operadoras petroleras, estos documentos se encuentran alojados en los servidores de la compañía, teniendo en cuenta que la información es el bien más preciado para una empresa.

El diseño del Plan de Recuperación de Desastres (DRP) en la fase de la fase de análisis de impacto aportará beneficios a la empresa tales como aumentar la confianza de los clientes y proveedores generando mayor competitividad.

II. LA ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

La Administración de la Continuidad del Negocio, BCM, por sus siglas en inglés, Business Continuity Management, de acuerdo con lo expuesto en la CICON 2008 [1] consta de varios componentes como son:

- Plan de Continuidad de las Operaciones (COOP).
- Plan de Respuesta a Incidentes.
- Planes de Contingencia (CP).
- Plan de Recuperación de Desastres (DRP).
- Plan de Continuidad del Negocio (BCP).
- Plan de Reanudación del Negocio (BRP).
- Plan de Comunicación de Crisis.
- Plan de Emergencias.
- Análisis de Impacto del Negocio (BIA).
- Análisis de Riesgos y Amenazas (TRA).

Cada uno de estos componentes está clasificado de acuerdo con la función que cumplen así:

- Componentes base conformados por el BIA y el TRA
- Los orientados a las Tecnologías de la Información (TI) conformados por el Plan de Respuesta a Incidentes, los CP y los DRP.
- El orientado a las instalaciones conformado por el Plan de Emergencias.
- Los orientados al negocio conformados por el COOP, Plan de Comunicación de Crisis, el BRP y el BCP.

Los componentes considerados de alto impacto para el negocio son el COOP, el DRP y el BCP, es por esta razón que se toma para el desarrollo del presente documento como tema principal el DRP en el contexto de una empresa del sector petrolero que ha estado ofreciendo soluciones a las operadoras petroleras desde 1841, la información es su activo más importante, por esta razón la compañía cuenta con un DRP en sus oficinas principales ubicadas en Estados Unidos, salvaguardando toda su infraestructura en una sede alterna con el fin de que ésta no se vea afectada, el problema surge al identificar que en las sedes no se cuentan con un Plan de Recuperación de Desastres (DRP) siendo este un factor de suma relevancia que podría afectar las diferentes unidades de negocio de la compañía.

El área de Tecnologías de la Información (IT) brinda sistemas integrados de información que sirven de instrumento para la correcta toma de decisiones y total disponibilidad de información que le permita mantener el posicionamiento corporativo en la industria del sector petrolero. Es un área de servicios al interior de la compañía por lo tanto cualquier usuario y/o área que requiera los servicios de IT se convertirte en cliente al cual se debe satisfacer respecto a la gestión realizada.

El departamento de IT está compuesto por la siguiente infraestructura: Hardware, Software y Telecomunicaciones las cuales están relacionadas entre sí para su funcionamiento y cuenta con personal especializado que administra, opera y supervisa la infraestructura a su vez también se efectúan mantenimientos y reparación de equipos, aplicaciones y mantenimiento de la estructura de comunicación que utiliza la compañía.

III. PLAN DE RECUPERACIÓN DE DESASTRES, DRP

Un Plan de Recuperación de Desastres, DRP, por sus siglas en inglés, Disaster Recovery Planning, se entiende como las acciones o prácticas efectivas de medidas de seguridad, que garantizan una adecuada recuperación de la operatividad mínima de los sistemas luego de una contingencia o desastre, en la que se vean afectados los procesos y recursos informáticos que soportan un negocio [2]
Según el NIST "*Un DRP es un plan enfocado en sistemas de información, diseñado para restaurar la operatividad del sistema, aplicación o la infraestructura de cómputo objetivo en un sitio alterno después de una emergencia. El DRP puede ser apoyado por múltiples planes de contingencia de sistemas de información para abordar la recuperación de cada uno de los sistemas impactados una vez las instalaciones alternas se han establecido. Un DRP puede soportar un plan BCP o COOP mediante la recuperación de los sistemas que soportan negocios, procesos o funciones misionales en una ubicación alterna. El DRP solo se refiere a interrupciones de sistemas de información que requieren reubicación*". [3]

Dentro del contexto de un DRP existen conceptos que van ligados al proceso como lo es un Plan de Recuperación del Negocio, BRP, por sus siglas en inglés, *Business Recovery Planning*, considerado un proceso superior al DRP porque además del procesamiento de los datos se centra en recuperar las demás operaciones de una empresa incluyendo las relacionadas con los clientes y proveedores procurando que la solución a un problema se de forma integral y el Plan de Continuidad del Negocio, BCP, por sus siglas en inglés, *Business Continuity Planning*, herramienta administrativa que permite a una empresa continuar su funcionamiento aunque de forma mínima, durante o inmediatamente después de ocurrida una emergencia. [4]

La implementación de un DRP representa para una empresa múltiples beneficios reflejados en la reducción de costos, disminución de tiempos de inactividad de los sistemas de información, el respaldo y control de la información existente en las diferentes aplicaciones y el entrenamiento del personal. [5]

Los desastres a los que se ven expuestos los sistemas informáticos pueden ser de diversos tipos y así mismo su impacto a nivel físico puede variar. A continuación, algunos desastres que pueden afectar a una organización:

- Incendios.
- Inundaciones.
- Huracanes.
- Tormentas severas.
- Deslizamientos de tierra.
- Tsunamis.
- Terremotos.
- Volcanes.
- Incidentes de Seguridad.
- Falla de equipamiento.
- Fallas de Energía.
- Fallas de servicios públicos.
- Pandemias.
- Sabotaje.
- Huelgas y paros laborales.
- Disturbios Civiles.
- Terrorismo.
- Guerra.

Los eventos en la anterior lista tienen el potencial de infligir daño a edificios, equipo y sistemas de TI. Pueden matar, herir o desplazar personas, sin mencionar que pueden evitar que asistan a sus trabajos. Los desastres pueden tener los siguientes efectos en las organizaciones:

- Los desastres naturales son imposibles de predecir y mucho menos de contener, estos eventos normalmente presentan daños graves en edificios que impiden el acceso a los mismos, además de los efectos que causa en los trabajadores debido a las potenciales pérdidas humanas causadas por el desastre.
- Un desastre puede afectar los sistemas de telecomunicación, lo que puede dejar a una empresa totalmente aislada de proveedores, contratistas y de sus clientes.
- Las fallas en el trasporte, ya sea por daños en las vías o por disturbios que afecten los sistemas de transporte masivo pueden causar imposibilidad de los trabajadores para desplazarse hasta sus sitios de trabajo.

Estos efectos pueden devastar negocios causándoles el cese de operaciones por horas, días o más. En el peor de los casos, simplemente los negocios no pueden sobrevivir después de experimentar tales interrupciones. Los negocios proveen bienes y servicios a clientes, quienes la mayor parte solo quieren esos bienes y servicios; si los clientes no pueden obtener esos bienes y servicios de un negocio ellos simplemente irán a otro que pueda proveérselos. Muchos negocios no se recuperan de un éxodo de clientes. En este contexto es también importante considerar los conceptos sobre riesgos y amenazas como lo expone el autor Salazar Villalobos citando a autores como Toigo y Hiatt, entre otros [4]:

Los riesgos son considerados como un evento o condición incierta que si sucede tiene un efecto positivo o negativo sobre un proyecto en aspectos como tiempo, costo, alcance o calidad.

Otros autores definen el riesgo como "*el potencial de que algo ocurra*" [6] Esto podría implicar cualquier tipo de evento que afecte vidas humanas. Las compañías de seguros trabajan para cuantificar la probabilidad de que un evento ocurra con el fin de fijar las tasas de seguros. Un riesgo puede ser algún fallo inesperado en el ejercicio de sus funciones de alguien que se creía como fiable. Podría ser la falla en una máquina o el derrame de un contenedor de material tóxico. Adicionalmente una crisis o desastre puede categorizarse por niveles de acuerdo con su nivel de riesgo, así nivel 1 o bajo riesgo, nivel 2 o riesgo moderado y nivel 3 o riesgo alto, lo anterior de acuerdo a los daños que se generen y su impacto en el negocio.

No todos los riesgos se materializan. Cuando se ven nubes que indican el potencial de lluvia. Las nubes negras no indican la certeza de una precipitación, pero indican mayor potencial que un cielo despejado.

Algunos riesgos son inevitables y solo se pueden dar pasos para reducir su impacto. Como es el caso de los desastres naturales como terremotos, tornados, tsunamis, etc. No es posible prevenirlos, pero es posible construir defensas que puedan minimizar los daños.

Riesgos como son los localizados debido a la falla de un computador clave en una oficina afectan directamente solo a algunas personas. Este es un riesgo común que no debe ser directamente cubierto en el plan de continuidad de negocio.

Otros riesgos pueden afectar a toda la compañía. Un ejemplo es una protesta que bloquee las vías y mantenga a los empleados y materiales lejos de su puerta.

Las amenazas son consideradas como eventos o situaciones que podrían impactar directa o indirectamente en el negocio, afectándolo total o parcialmente, por lo cual pueden clasificarse en cuatro categorías como son:

- Accidentales como perdida de electricidad, accidente de transporte, contaminación química, etc.
- Naturales como inundaciones, terremotos, etc.
- Internas como robo, sabotaje, violencia entre colaboradores, etc.
- Conflicto armado como terrorismo, secuestro, etc.

Otro concepto importante dentro del DRP, en especial relacionados con la administración de proyectos se refiere al diseño del proyecto el cual desde la definición dada por Accreditation Board for Engineering and Technology (ABET) establece que "*el diseño en ingeniería es el proceso de idear un sistema, componente o proceso que satisfaga cierta necesidad. Es un proceso decisión-creación (a menudo iterativo), donde las ciencias básicas, matemáticas y ciencias de la ingeniería son aplicadas para convertir recursos de manera óptima para alcanzar un objetivo determinado. Entre los elementos fundamentales del proceso de diseño esta determinar los objetivos y criterios, síntesis, análisis, construcción, pruebas y evaluación*". [7]

De la definición anterior se puede inferir que el proceso de diseño es tanto un proceso científico como creativo que utilizan los humanos para producir artefactos para satisfacer las necesidades de la sociedad.

Para el diseño de un Plan de Recuperación de Desastres (DRP) informáticos se deben conocer los procesos que permiten desarrollar el plan, los cuales se describen a continuación con base en la revisión del tema en la literatura. [8] [9]

A continuación, se describe los principales procesos necesarios para el desarrollo de un proyecto DRP.

A. Análisis de Riesgos (AR)

El proceso de Análisis de Riesgos es el que brinda los elementos base para elaborar el plan de recuperación, el cual consiste en identificar los recursos, las posibles amenazas y las vulnerabilidades que en caso de presentarse podrían ocasionar resultados negativos a una empresa [4] [5], en otras palabras puede considerarse como el proceso responsable de la identificación y valoración de riesgos que puedan generar interrupciones en los servicios de TI, partiendo de tres preguntas claves como son:

- ¿Qué está bajo riesgo?
- ¿Cómo se puede producir?
- ¿Cuál es la probabilidad que suceda?

En este contexto el equipo consultor analizara identificará y evaluará los riesgos que comprometan la disponibilidad de los servicios de TI, los cuales serán insumo para la definición de escenarios de desastres y estrategias de recuperación partiendo del reconocimiento de todos los aspectos involucrados en el tema de riesgos desde un Sistema de Gestión de Seguridad de la Información como se aprecia en la figura 1.

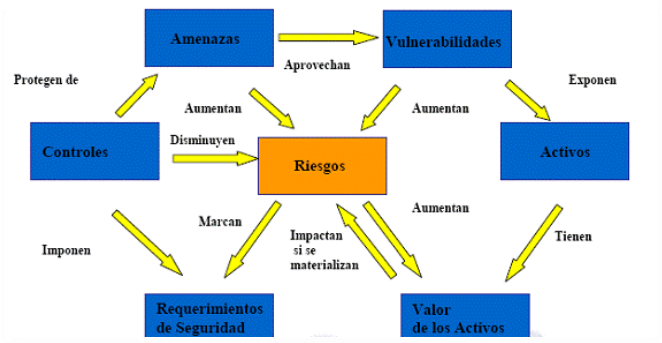

Fig. 1. Componentes de un sistema de gestión de seguridad de la información según ISO 27001. [10]

El análisis de riesgos implica la identificación, evaluación, elaboración de la matriz de nivel de riesgo, controles de reducción del riesgo y documentación de los resultados. La identificación de riesgos tiene como objetivo conocer los recursos y procesos críticos del negocio, los cuales pueden clasificarse como [5]:

- Software y hardware.
- Equipo de comunicaciones.
- Aplicaciones críticas de los sistemas.
- Datos e información crítica.
- Procesos críticos.
- Personal de soporte.
- Ambiente operacional del área (políticas y permisos a usuarios, topología de la red, Backup que protejan la confidencialidad, integridad y disponibilidad de los datos y la seguridad física y ambiental del área).

Para establecer el nivel de exposición a riesgos que comprometan la continuidad de las operaciones se divide la organización en unidades de negocio. En cada una de las unidades se debe dar respuesta a la pregunta: ¿Qué pasaría en la empresa si el componente X deja de funcionar abruptamente, bajo el escenario del peor desastre?

Los componentes que podrían fallar son todos aquellos elementos de hardware, software, comunicaciones, logística, transporte e infraestructura que soportan los procesos del negocio, la información que apoya estos componentes se recolecta mediante, entrevistas, revisión de informes y otros mecanismos en los que la participación de los dueños de procesos de la empresa y así proceder al análisis de impacto.

B. Análisis de Impacto del Negocio (BIA)

El BIA es considerado como el proceso que determina el efecto que cada tipo de amenaza potencial produce en las funciones de una empresa. Los tipos de criterios que pueden emplearse para evaluar el impacto son *[4]*:

- Servicio al cliente.
- Operaciones internas.
- Asuntos legales y financieros.

El propósito del BIA es diseñar una estrategia de recuperación que pueda facilitar el reinicio de la operación en un tiempo razonable en caso de una contingencia enfocado a los procesos críticos de tecnología para la compañía y se tendrá en consideración los aspectos de restablecer los equipos y enlaces de telecomunicaciones vitales para la operación y restablecer las aplicaciones y servidores críticos para la organización.

Desde la literatura existen algunas metodologías que se recomiendan para realizar el análisis de impacto del negocio, una de ellas se refleja en la figura 2, la cual expone unos pasos lógicos.

Fig. 2. Metodología del Análisis de Impacto del Negocio. [11]

1. Identificación de las funciones y procesos del negocio

Se identifican los procesos y funciones que son soportes de la compañía que son parte vital para el desempeño de la compañía, que se describen a continuación:

a) Función: Hardware

Procesos: Mantenimiento de Equipos, Instalación de Equipos, Help Desk (casos centralizados) y soporte a las diferentes divisiones.

b) Función: Software

Procesos: Instalación de Programas, configuración de equipos, encriptar disco duro equipos, licenciamiento de aplicaciones y respaldo de la Información (Backup).

c) Función: Telecomunicaciones

Procesos: Configuración y Mantenimiento de redes, mantenimiento de equipos de comunicación, monitoreo de la red y presentación de Licitaciones operadoras petroleras.

d) Función: Licitaciones

Proceso: Presentación de Licitaciones operadoras petroleras.

e) Función: Facturación

Procesos: Pago de proveedores, cartera pendiente por cobrar y pagar, pago de impuestos y pago de nómina de los empleados.

f) Función: Compras

Procesos: Generar órdenes de compra, suministros e insumos para la operación y administrativa.

g) Función: Pago de Nomina

Procesos: Pago de nómina de los empleados, pago de incapacidades, pago vacaciones y pago de bonos de campo.

2. Evaluación del impacto financiero y operacional

La Valoración del Impacto financiero y operacional es conocer los riesgos y pérdidas económicas que se pueden presentar en los procesos de la compañía y el potencial tiempo de caída de las funciones del negocio. Referente al impacto operacional se definió un esquema de medida jerárquica cualitativo, tal como:

MA= Muy alto A= Alto M=Medio B=Bajo N/A= Ninguno (ver Tabla I)

TABLA I.
JERARQUÍA IMPACTO OPERACIONAL [8]

Funciones	Procesos	Flujo de caja	participacion mercadeo	Competitividad	Satisfaccion cliente
Hardware	Mantenimiento de Equipos	B	M	M	M
	Instalación de Equipos	B	M	M	M
	Help desk (casos centralizados)	B	A	B	A
	Soporte a las diferentes divisiones.	B	A	A	MA
Software	Instalación de Programas	B	B	M	M
	Configuración de Equipos	B	M	M	M
	Encriptar disco duro Equipos.	B	B	A	M
	Licenciamento de Aplicaciones	M	A	A	M
	Respaldo de la Información (Backup).	M	A	MA	A
Telecomunicaciones	Configuración y Mantenimiento de redes	B	M	M	M
	Mantenimiento de equipos de comunicación	B	M	M	A
	Monitoreo de la red.	B	B	M	A
Licitaciones	Presentación de Licitaciones operadoras petroleras.	MA	A	MA	A
Facturación	Pago de proveedores.	A	M	M	M
	Cartera pendiente por cobrar y pagar.	MA	A	A	A
	Pago de impuestos.	M	A	M	M
	Pago de nómina empleados	M	M	M	M
Compras	Solicitud de cotizaciones a proveedores para compra de insumos.	M	A	M	M
	Generar órdenes de compra, suministros e insumos para la operación y administrativa.	M	A	M	M
Pago de Nomina	Pago de nómina empleados	M	B	M	M
	Pago de incapacidades.	M	B	B	M
	Pago vacaciones.	M	B	B	M
	Pago de bonos de campo.	M	B	B	M

3. *Identificación de procesos críticos*

Utilizando los requerimientos identificados y basándose en los impactos financieros y operacionales se define una tabla de procesos críticos para la compañía (ver Tabla II).

TABLA II.
PROCESOS CRÍTICOS DEL NEGOCIO [8]

Funciones	Procesos
Hardware	Help desk (casos centralizados)
Software	Respaldo de la Información (Backup).
Telecomunicaciones	Mantenimiento de equipos de comunicación
Licitaciones	Presentación de Licitaciones operadoras petroleras.
Facturación	Cartera pendiente por cobrar y pagar.
Compras	Generar órdenes de compra, suministros e insumos para la operación y administrativa.
Pago de Nómina	Pago de nómina empleados

4. *Identificación de requerimientos de recursos, establecimiento de los tiempos de recuperación, y disposición del RTO /RPO*

Luego de identificar los procesos críticos de la compañía las buenas prácticas establecen que "l*os requerimientos de los tiempos de recuperación consisten en una serie de componentes que tienen que ver con el tiempo disponible para recuperasen de una alteración"*. [8]

A continuación, se menciona los componentes que se tuvieron en cuenta para fundamentar la metodología revisada:

MTD: Representa el periodo máximo de tiempo de inactividad que la organización puede tolerar. Las buenas prácticas definen ciertos parámetros para cada componente. Entre estos están que la suma de los tiempos del RTO y el WRT son iguales o menores a los del MTD.

En el MTD se debe jerarquizar las prioridades de recuperación definiendo criterios donde un proceso crítico tiene que tener un menor tiempo de recuperación comparado con otro que tenga un mayor tiempo.

RTO: Tiempo disponible para recuperar sistemas o recursos que han sufrido una alteración.

RPO: Hace referencia a la magnitud de la pérdida de datos medida en tiempo que un proceso pueda tolerar.

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

Juntos a estos componentes se establecen los sistemas críticos y no críticos de tecnología de la información y aplicaciones que apoyan los procesos identificados y los procedimientos alternos que permitan que los procesos de negocio puedan continuar al momento que se presenten interrupciones.

Desde la parte práctica, *en la tabla III* se puede apreciar un ejemplo en el que se definen los tiempos de respuesta para cada componente.

A continuación, se muestran los resultados obtenidos al implementar la metodología recomendada en la compañía petrolera frente a sus procesos críticos.

TABLA III
RESUMEN BIA [8]

Funciones	Procesos	MTD Dias	Prioridad de Recuperacion	Sistemas IT Criticos y aplicaciones	RTO	RPO	WRT	Procedimientos alternos
Hardware	Help desk (casos centralizados)	3	Media	Sistema Casos Centralizados Remedy (CRM)	1,5 dias	1 Día	1 Dia	Formato físico
				Sistema Email	1 Dia	1 Día	1 Dia	Apertura de casos a través de correo
Software	Respaldo de la Información (Backup).	2	Alta	Servidor File Server 01	0,5 dia	1 Día	1,5 dias	Copia manual de archivos a medios alternativos
				Servidor Bk01	0,5 dia	1 Día	1,5 dias	Respaldo Manual de Bases de datos
				Servidor 01	1 dia	1 Día	1 dia	
				Aplicación de almacenamiento y restauracion simpana commvault	1,5 dias	1 Día	0,5 dia	
Telecomunicaciones	Mantenimiento de equipos de comunicación	3	Media	Sistema Email	1 dia	1 Día	2 dias	Equipos de comunicaciones de reemplazo
				Servidores	1 dia	1 Día	2 dias	Cláusula de contrato con Prestador de servicio de Internet que especifique el reemplazo de equipos de comunicación por daño en menos de 2 horas
				Aplicaciones Online	1 dia	1 Día	1 dia	
Licitaciones	Presentación de Licitaciones operadoras petroleras.	2	Alta	Sistema Email	1 dia	1 Día	1 dia	Disponer de plan de internet móvil, estableciendo conexiones a través de modem o teléfono celular
				Aplicaciones Online	1,5 Dias	1 Día	0,5 dia	
Facturación	Cartera pendiente por cobrar y pagar.	4	Baja	Sistema Email	1 Dia	1 Día	1 Dia	Uso de correo
				Sistema ax dynamics (ERP)	1,5 dias	1 Día	2 dias	Revisión manual de facturas físicas
Compras	Generar órdenes de compra, suministros e insumos para la operación y administrativa.	2	Alta	Sistema Email	1 Dia	1 Día	1 Dia	Uso de formato físico de orden de compra
				Sistema ax dynamics (ERP)	1 dia	1 Día	0,5 dia	
Pago de Nómina	Pago de nómina empleados	3	Media	Sistema Queryx (ERP)	1 dia	1 Día	1,5 dias	Se paga la nómina del mes anterior
				Sistema Email	1 Dia	1 Día	1 Dia	
				Servidor02 DB empleados	1 dia	1 Día	1,5 dias	

Los recursos no críticos de tecnología identificados son:

- Muebles y enseres.
- Edificación.
- Útiles de Oficina y papelería.
- Materiales de uso y consumo.
- Producto Final
- Equipos de seguridad.
- Maquinarias.
- Herramientas de trabajo y mantenimiento

5. Identificación de procesos alternos

Para los procesos críticos identificados se plantean los siguientes procedimientos alternos (ver Tabla IV):

TABLA IV
PROCEDIMIENTOS ALTERNOS [8]

Funciones	Procesos	Sistemas IT Críticos y aplicaciones	Procedimientos alternos
Hardware	Help desk (casos centralizados)	Sistema casos centralizados Remedy (CRM)	Formato físico
		Sistema Email	Apertura de casos a través de correo
Software	Respaldo de la Información (Backup)	Servidor File Server SrvbogFs01	Copia manual de archivos a medios alternativos
		Servidor Bk01	Respaldo Manual de Bases de datos
		Servidor 01	
		Aplicación de almacenamiento y restauración simpana commvault	
Telecomunicaciones	Mantenimiento de equipos de comunicación	Sistema Email	Equipos de comunicaciones de reemplazo
		Servidores	Cláusula de contrato con prestador de servicio de Internet que especifique el reemplazo de equipos de comunicación por daño en menos de 2 horas
		Aplicaciones Online	
Licitaciones	Presentación de Licitaciones operadoras petroleras.	Sistema Email	Disponer de plan de Internet móvil, estableciendo conexiones a través de modem o teléfono celular
		Aplicaciones Online	
Facturación	Cartera pendiente por cobrar y pagar.	Sistema Email	Uso de correo
		Sistema ax dynamics (ERP)	Revisión manual de facturas físicas
Compras	Generar órdenes de compra, suministros e insumos para la operación y administrativa.	Sistema Email	Uso de formato físico de orden de compra
		Sistema ax dynamics (ERP)	
Pago de Nómina	Pago de nómina empleados	Sistema Queryx (ERP)	Se paga la nómina del mes anterior
		Sistema Email	
		Servidor02 DB empleados	

IV. CONCLUSIONES

La Administración de Continuidad del Negocio (BCM) y sus componentes brindan a las empresas una herramienta muy valiosa para garantizar su funcionamiento en momentos de crisis o eventos adversos.

El Plan de Recuperación de Desastres conocido como DRP es uno de los componentes de alto impacto dentro de la BMC para una empresa, por esta razón el conocer los procesos que lo conforman como son el Análisis de Riesgos y el BIA permitirán seguir una metodología que genere una documentación valiosa en la identificación de procesos críticos, dando la oportunidad de prever los riesgos, amenazas, recursos y vulnerabilidades a las que puede enfrentarse un negocio y por ende minimizar los efectos adversos que puedan presentarse.

El DRP brinda al gerente de un proyecto aspectos relevantes para garantizar el funcionamiento de un negocio en el momento de un desastre.

La participación de los dueños de proceso de una empresa brinda la posibilidad de generar una documentación consistente, coherente y de gran valor para la conformación y estructuración de sistemas de información con datos relevantes sobre el ejercicio administrativo de una compañía.

El análisis de Impacto del Negocio es importante para identificar los procesos que apoyan misionalmente a la compañía y su nivel de importancia frente al funcionamiento y continuidad que debe tener el negocio ante un desastre.

REFERENCIAS

[1] *M. García, «Coordinación con autoridades externas,» de Conferencia Iberoamericana de Continuidad del Negocio, México, 2008.*

[2] *R. C. Peña Gerónimo, M. Matos Cuevas, y M. B. Montas, «Diseño de un Plan de Recuperación ante Desastre (DRP) para salvaguardar las operaciones del área de Tecnologías de la Información y la Comunicación ante una situación de desastre. caso: Institución Educativa Loyola,» Revista ingeniería en redes y telecomunicaciones, vol. 1, nº 1, pp. 18-29, 2014.*

[3] *National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems [en línea], Gaithersburg: NIST, 2010.*

[4] *J. Salazar Villalobos, Guía para crear un Plan de Recuperación en caso de Desastre en el sistema informático del centro de datos de un grupo financiero, San José, Costa Rica: Universidad para la Cooperación Internacional, 2008.*

[5] *M. R. Ávila Vásquez, Diseño e implementación de un DRP (Disaster Ricovery Plan) para Departamento de Ingenierías de la empresa Continental Tire Andina, Cuenca, Ecuador: Universidad de Cuenca, 2013.*

[6] *M. Wallace y L. Webber, The Disaster Recovery Handbook: A step by step plan to ensure business continuity and protect vital operations, facilities and assets, New York: AMACOM, 2011.*

[7] *Y. Haik y T. M. Shalin , Engineering design process, Stamford: Cengage Learning, 2011.*

[8] *A. G. Alexander, Diseño de un sistema de gestión de seguridad de la información, México: Alfaomega, 2007.*

[9] *C. M. Bada y R. C. Sales, Implantación de un sistema de gestión de seguridad de la información según ISO 27001 un enfoque práctico, Madrid : Fundación Confemetal , 2011.*

[10] *A. López Neira y J. Ruiz Spohr, ISO27000.es, 2012.*

[11] *MINTIC, Guía para realizar el Análisis de Impacto de Negocios BIA: seguridad y privacidad de la información, Bogotá: El Ministerio, 2015.*

Autor

Ricardo Alfonso Acosta Galindo
National Oilwell Varco, Ingeniero IT.

Ingeniero de sistemas Corporación Unificada Nacional
de Educación Superior 2009.