Marco de Referencia para la Formulación de un Plan de Continuidad de Negocio para TI, un caso de estudio

M. Bautista

Corporación Centro Nacional de Control de Energía, CENACE

***Resumen*— El propósito de un Plan de Continuidad de Negocio (Business Continuity Plan, BCP por sus siglas en inglés) es proporcionar procedimientos para mantener en funcionamiento los servicios críticos de la organización a causa de una interrupción de los mismos mientras se realiza la recuperación, en caso de un desastre natural o causado por humanos.**

En la actualidad, la iniciativa de implantación de un BCP/DRP tiene una prioridad alta para la mayoría de las organizaciones, es una necesidad estratégica que puede constituirse en el elemento diferenciador entre subsistir o desaparecer del Mercado.

La práctica ha demostrado que existen situaciones en las cuales aparentemente un "simple" mantenimiento de hardware puede dejar a una organización sin su principal herramienta de trabajo, causando el malestar de sus usuarios internos/externos, sanciones disciplinarias/ regulatorias, pérdida de imagen y dependiendo de la gravedad hasta el despido de sus representantes con las respectivas acciones judiciales por daños y perjuicios; simplemente por no contar con procesos, procedimientos e instructivos que identifiquen las acciones previas y posteriores ante un escenario de desastre.

El presente trabajo pretende proponer un marco de referencia que permita a las organizaciones formular un Plan de Continuidad de Negocio para TI o Plan de Recuperación de Desastres, a través de la aplicación de principios claros y esenciales expresados en un lenguaje natural.

Finalmente, se realizará la aplicación del marco de referencia propuesto en el caso de estudio para el DRP del Sistema de Medición Comercial SIMEC del CENACE.

***Palabras clave*— Gobierno de TI, Análisis de Riesgos, Plan de continuidad de negocios, Plan de recuperación de Desastres, Análisis de impacto de negocio.**

***Abstract*— The purpose of the Business Continuity Plan (BCP) is to provide procedures to maintain the operation of an organization's critical services in the event of an interruption, while recovery work is still in process, such as in the event of a natural disaster or human error.**

There is currently a BCP/DRP initiative which has been classified as high priority by the majority of organizations, as it is a necessary strategy that could become the defining element between remaining on the market, or from disappearing from the market.

The practice has shown that there are situations in which an apparently "simple" hardware maintenance procedure could leave an organization without its main work tool, causing problems for its internal/external users, disciplinary/regulatory fines, damage to reputation and depending on the seriousness of the issues, even the laying off of its representatives with legal consequences for damage claims – all due to a lack of proper processes, procedures and instructions which identify the actions to be taken before and after a disaster scenario.

This study attempts to propose a framework that would allow organizations to formulate a Business Continuity Plan for TI or a Disaster Recovery Plan, through the application of clear and essential principles expressed in everyday language.

To conclude, the proposed framework will be applied to the study case – the DRP of the CENACE's SIMEC Commercial Measurement System.

***Index Terms*— TI Government, Risk Analysis, Business Continuity Plan, Disaster Recovery Plan, Business Impact Analysis.**

1. INTRODUCCIÓN

Un desastre es un incidente causado por la naturaleza o por seres humanos, que afecta negativamente a las organizaciones y su entorno llevando a grandes daños, destrucción y devastación a la vida y su propiedad [1].

Los desastres naturales pueden ser causados por: terremotos, inundaciones, tornados, tormentas eléctricas severas e incendios; mientras que los desastres causados por los seres humanos se deben a actos de terrorismo, ataque de hackers, sabotajes, empleados disgustados, entre otros. Existe otro tipo de interrupciones como la pérdida del suministro de energía eléctrica, telecomunicaciones y gas natural que igualmente pueden provocar eventos fatales; así como también, pueden darse otro tipo de incidentes como: eliminación accidental de la información, ataques de negación de servicios, virus, que si bien no pueden generar desastres, pero si pueden llevar a eventos de alto riesgo que pudieran interrumpir el normal desenvolvimiento de una organización.

Cada organización compromete el uso de sus recursos, el capital humano y la ejecución de las actividades diarias con el propósito de permanecer en el mercado, lograr estabilidad y rentabilidad. La mayor parte de ellas poseen bienes tangibles como: insumos, maquinarias, empleados y sistemas computarizados; y bienes intangibles como: procesos, tecnología, información, prestigio, entre otros, la afectación o daño de cualquiera de ellos podrían causar la paralización de actividades. Mientras mayor sea el tiempo de indisponibilidad de estos recursos, mayor será la posibilidad el sufrir un daño irreversible, y en algunos casos se ha visto la desaparición de varias organizaciones por su incapacidad de recuperación ante un evento de desastre.

A continuación se presentan algunas razones por las cuales es indispensable recuperar las actividades de un negocio:

- Valor de la empresa, por naturaleza toda empresa busca generar mayor rentabilidad para sus propietarios y accionistas en función de sus capacidades.
- Presión de los competidores, ante la indisponibilidad de los productos o servicios de una empresa, es la competencia la que adquirirá mayor presencia en el mercado.
- Demandas del mercado, cada vez los requerimientos de los clientes son más exigentes y en tiempos de respuesta menores.
- Disposición de los reguladores, el cumplimiento de la normativa dispuesta por los entes de regulación y control obliga a tomar medidas preventivas a fin de evitar sanciones.

2. CONTINUIDAD DEL NEGOCIO

En el nivel más básico, el Plan de Continuidad de Negocio (Business Continuity Planning, BCP por sus siglas en inglés) puede ser definido como un proceso interactivo que es diseñado para identificar los procesos de misión crítica del negocio y desarrollar políticas, planes y procedimientos para asegurar la continuidad de estos procesos en el caso de un evento imprevisto [2].

El BCP es responsabilidad de la Alta Gerencia debido a que se encarga de la protección de los activos y la viabilidad de la organización, de manera concomitante a lo definido en sus políticas. El BCP es generalmente ejecutado por las unidades de negocio y soporte, a fin de proveer un reducido pero suficiente nivel de funcionalidad en las operaciones, inmediatamente después de detectarse una interrupción mientras las actividades de recuperación se llevan a cabo.

3. RECUPERACIÓN DE DESASTRES

El DRP (Disaster Recovery Planning, por sus siglas en inglés) es el proceso de evaluación de los riesgos que enfrenta una organización, para luego desarrollar, documentar, implementar, probar y mantener procedimientos que ayudan a la organización a retornar rápidamente a las operaciones normales y reducir al mínimo las pérdidas después de un desastre [3]. Un DRP está enfocado a los sistemas de información, diseñado para restablecer la operación de los servicios informáticos críticos específicos (hardware y software), con instalaciones, infraestructura y procedimientos alternos, en caso de una emergencia; el responsable del DRP es el departamento de TI de la organización.

Es por ello que el DRP debería estar alineado con la estrategia de la organización; la criticidad de los diferentes sistemas de información depende de la naturaleza del negocio, así como también, del valor que cada aplicación aporta al negocio.

Debido a que cada organización tiene su identidad, cultura, clima organizacional, relaciones con sus clientes, socios de negocios y el público en general. Estas relaciones deberían conducir a una organización en el emprendimiento de una iniciativa de planificación de recuperación de desastres.

4. RELACIÓN ENTRE EL BCP Y DRP

El alcance de un DRP está generalmente limitado a un conjunto definido de sistemas e infraestructura de TI, cuyo objetivo final es la recuperación oportuna, completa, dentro de un plazo de tiempo definido y con la mínima pérdida de datos. El proceso para la determinación de qué sistemas de TI son necesarios incluir en un DRP, es generalmente manejado por el departamento de TI, con los aportes de los propietarios de las aplicaciones quienes pueden o no ser parte del departamento.

En contraste, el alcance del BCP puede ser toda la empresa, con el objetivo final de recuperar las funciones principales y de misión crítica del negocio para asegurar su supervivencia, considerando aspectos como la infraestructura física y el personal necesario. Las funciones de negocio a ser recuperadas en un BCP se extienden más allá de los sistemas de TI como se muestra en la Tabla 1.

Tabla 1: Alcance del DRP frente al BCP

RECUPERACIÓN DE DESASTRES (DRP)	*CONTINUIDAD DE NEGOCIO (BCP)*
Los esfuerzos de recuperación de desastres continuarán sólo hasta que el desastre se supere por completo.	*Los procesos de continuidad del negocio se extienden incluso después de eliminar un desastre.*
Se enfoca en sistemas y datos afectados por el desastre.	*Está relacionado con todas las operaciones de la empresa.*
Es reactivo, se produce después de un desastre.	*Es proactivo, se produce antes y después de un desastre.*

5. BENEFICIOS DE CONTAR CON UN DRP

Dado el caso de una interrupción real, las organizaciones actualmente dependen en gran medida de la interacción e interdependencia con otros colaboradores en el entorno de su negocio. Incluso el contar con un DRP es un objetivo que beneficiará a las organizaciones de muchas maneras; pero que no garantiza que las mismas sean capaces de recuperarse íntegramente de un desastre.

La efectividad en la ejecución de este plan se debe basar en asumpción de varios supuestos como contar con: la infraestructura y recursos para recuperar los sistemas críticos, los técnicos idóneos, centros de funcionamiento alternos, entre otros.

La organización que tenga implementado un DRP, independientemente de prevenir y minimizar las pérdidas para el negocio, debe garantizar que cuenta con una respuesta planificada ante una interrupción importante que pueda poner en riesgo su subsistencia, aspecto que debería ser considerado muy seriamente para su instauración en todas las organizaciones independientemente del sector, actividad o tamaño que tuvieren.

Entre otros beneficios se tiene:

- Diseño de medidas para reducción de riesgos identificados.
- Determinación de procesos críticos y vulnerables dentro del negocio.
- Operación de procesos críticos de un negocio durante el desastre.
- Identificación de áreas de oportunidad y alternativas de operación durante el desastre.
- Cálculo de pérdidas aproximadas por inoperancia de procesos críticos.
- Ventaja competitiva frente a otras organizaciones.
- Prevención ante la aplicación de sanciones económicas por incumplimiento de requerimientos regulatorios.

6. PROCESOS DE LA RECUPERACIÓN DE DESASTRES

Como cada organización es única, así también lo es cada BCP de TI que lo pertenece. El proyecto de recuperación de desastres es un proyecto solo o como parte de una iniciativa de BCP.

Los procesos para la planificación de recuperación de desastres pueden ser divididos en las siguientes fases del ciclo de vida como se muestran en la Fig. 1.

Figura 1: Ciclo de Vida de la Planificación de Recuperación de Desastres

6.1. Planificación del Proyecto

Se parte de la premisa que el proyecto cuenta con el auspicio y financiamiento necesario por parte de la Alta Gerencia de la empresa como un requisito primario e indispensable. Esta fase comprende la identificación de las actividades que deben realizarse en forma previa para comenzar el proyecto, es decir, qué se va a hacer y por qué.

Los objetivos del proyecto de la planificación de recuperación de desastres son: obtener un entendimiento del actual y futuro ambiente de TI de la organización, definir el alcance, desarrollar la programación y la identificación de riesgos del proyecto, mediante la ejecución de las siguientes tareas:

- Nombrar el coordinador de recuperación de desastres.
- Crear la política de recuperación de desastres.
- Realizar la planificación del proyecto.

6.2. Análisis de Impacto de Negocio – BIA

El análisis BIA es un paso crítico en el desarrollo de una estrategia de recuperación de desastres, consiste en evaluar los procesos críticos (y los componente de TI que los soportan) de la organización y determinar los plazos, prioridades, recursos e interdependencias, como resultado de la paralización de una o varias actividades.

Una vez recopilada la información, su análisis se realiza en base a dos factores de costos independientes que pueden ayudar a tomar la mejor decisión:

- Costo de tiempo de inactividad, en el corto plazo tiene un valor bajo, sin embargo, a medida que el tiempo avanza tiende a crecer rápidamente hasta llegar a un punto de estabilización que representa que el negocio ya no puede funcionar.
- Costo medidas alternativas correctivas, que iniciando con un valor alto empiezan a decrecer en función del tiempo objetivo de recuperación.

Una vez identificados los dos costos y la suma de los mismos como se muestra en la Fig. 2 la organización podría identificar el punto en el cual el costo total puede ser minimizado. Cada punto en la curva en su conjunto, representa una posible estrategia, que a su vez tiene su respectivo costo, normalmente los objetivos de recuperación de tiempos cortos son a su vez los más costosos.

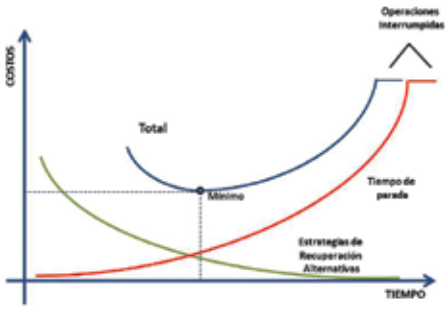

Figura 2: Costo de Inactividad vs. Costo de Medidas Alternativas

El tiempo máximo permitido de interrupción (Max Time Disruption, MTD) que puede ser soportado por la organización hasta que las pérdidas no sean asumibles, junto con el tiempo de recuperación objetivo (Recovery Time Objective, RTO) y el punto de recuperación objetivo (Recovery Point Objective, RPO) son parámetros que están vinculados directamente con la recuperación, y son los principales resultados del BIA. Específicamente, el RTO se refiere al período de tiempo después de un incidente en el que un producto, actividad o servicio debe ser reanudado, o un recurso debe ser recuperado. El RPO se refiere al punto más reciente en el cual los sistemas pueden ser recuperados; por tanto, constituye un indicador de la cantidad de información que una organización puede permitirse perder sin que afecte al negocio.

En la Fig. 3 se ilustra la relación entre el RTO, RPO y el MTD ante la ocurrencia de un evento de desastre.

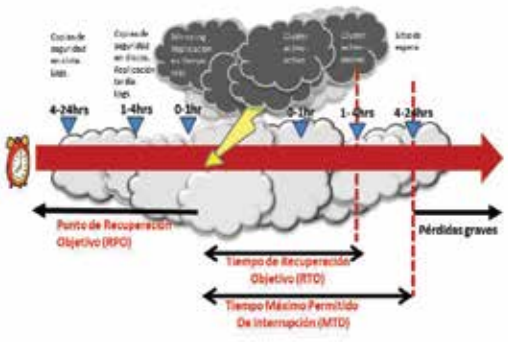

Figura 3: Localización del RTO, RPO y MTD en el tiempo ante la presencia de un evento de desastre

6.3. Evaluación de Riesgos y Análisis

El análisis de riesgos es un proceso sistemático que consiste en identificar las amenazas sobre estos activos y su probabilidad de ocurrencia, las vulnerabilidades asociadas a cada activo y el impacto que las citadas amenazas pueden provocar sobre la disponibilidad de los mismos.

Existen varias metodologías de análisis de riesgos, de igual manera soluciones de software que permiten automatizar dicho proceso, sin embargo, todas se basan en el siguiente esquema de funcionamiento:

- Identificar los activos.
- Identificar y evaluar las amenazas.
- Identificar y valorar las vulnerabilidades.

Calcular el riesgo como la probabilidad de que se produzca un impacto determinado en la organización.

Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (contratando un servicio o un seguro de cobertura), o en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario.

6.4. Medidas Preventivas

En función de los resultados del BIA y el análisis de riegos, se deben identificar y aplicar las medidas de seguridad necesarias para evitar que se produzcan incidentes que al no ser tratados de manera adecuada active el plan de recuperación de desastres.

Las medidas deben permitir reducir la probabilidad de ocurrencia de interrupciones en las actividades críticas, la duración, limitando el impacto que pueda provocar en la organización y así fortalecer al negocio mediante la eliminación de puntos de fallo.

Para ello se elabora un plan que incluye acciones que la organización debe adoptar para prevenir y evitar dentro de lo posible los riesgos que afectan la disponibilidad de las operaciones.

6.5. Estrategia de Recuperación

En base a los resultados del BIA y del análisis de riesgos, el objetivo que se persigue en esta fase es identificar las alternativas de recuperación de los servicios críticos de la organización en concordancia con los tiempos definidos y acordados.

La elección de las diferentes alternativas de recuperación depende de las necesidades de la organización: tiempos de recuperación objetivo (RTO), costos, recursos, seguridad, entre otros; cada plataforma de TI que soporte una función crítica de negocio, deberá contar con una estrategia de recuperación. A continuación se muestran algunas alternativas:

- Hot Sites, normalmente está configurado con todo el hardware y el software requerido para iniciar la recuperación a la mayor brevedad.
- Warm Sites, esta opción no incluye servidores específicos de alta capacidad.
- Cold Sites, esta opción sólo tiene el ambiente básico (aire acondicionado, cableado eléctrico, enlaces de telecomunicaciones, y otros).
- Mirror Sites, se procesa cada transacción en paralelo con el sitio principal.
- Acuerdos recíprocos con otras organizaciones.
- Múltiples centros de procesamiento.

6.6. Desarrollo e Implantación del Plan

Una vez que las estrategias han sido definidas, deben identificarse los métodos, plazos, personas, recursos y tareas necesarias para implementarlas, así como también, la puesta en marcha por los encargados de la recuperación de desastres de la organización.

Un DRP es un conjunto estructurado de procesos y procedimientos destinados a proporcionar una respuesta rápida al desastre y a los esfuerzos de recuperación. El plan debe documentarse y escribirse en un lenguaje simple que sea entendible para todos los equipos de recuperación.

De igual manera se deben establecer las estructuras organizacionales, perfiles de los cargos y los procesos, que darán sostenibilidad a la continuidad del servicio de TI. La definición de roles y responsabilidades es uno de los aspectos más importantes del DRP, ya que es aquí donde se determina cada una de las actividades a cumplir antes, durante y después del desastre por los responsables de la ejecución del plan.

6.7. Pruebas y Actualización del Plan

La efectividad del DRP en situaciones de emergencia se puede valorar si existe un plan de prueba que se lleve a cabo en condiciones reales. La fase de prueba debe contener las actividades más importantes que requieran comprobación y certeza en su funcionamiento futuro.

Se debe probar dentro de un ambiente que simule las condiciones que serían aplicables en una emergencia verdadera. Es también importante que las pruebas se lleven a cabo por las personas que serían responsables de esas actividades en una crisis.

El DRP debe ser mantenido a través de un ciclo de mejora continua. Cualquier cambio a nivel organizativo, operacional o técnico puede impactar en el negocio y por tanto en el plan de recuperación.

En el caso de que se evidencien cambios que afecten a la organización y que tengan impacto en los procesos críticos de negocio y sus servicios de TI, puede ser necesario revisar el BIA y el análisis de riesgos para ver en qué medida dichos cambios pueden provocar desajustes en las estrategias y los procedimientos. De esta forma, la organización puede disponer de ciertas garantías sobre la efectividad de su plan de recuperación de desastres.

7. CASO DE APLICACIÓN - SISTEMA DE MEDICIÓN COMERCIAL SIMEC

El Sistema de Medición Comercial (SIMEC) permite gestionar la medición de los registros cuarto-horarios de energía y otros parámetros eléctricos, en los puntos de generación/entrega del Sistema Nacional Interconectado (SNI). La información generada en el SIMEC constituye el principal insumo para los procesos de liquidación y facturación del Mercado Eléctrico Mayorista Ecuatoriano.

Con base al marco de referencia previamente analizado, se procede con la aplicación a manera ejemplificativa del ciclo de vida de algunos procesos de la planificación de recuperación de desastres aplicados al SIMEC.

a) Análisis de Impacto de Negocio

Dentro de los procesos de la cadena de valor de la Corporación CENACE está el proceso "Administrar y Liquidar las Transacciones del MEM y de las TIE" que utiliza como principal insumo para la ejecución de sus procesos internos la información de los registros de energía cuarto-horarios procedentes del SIMEC.

Ante la incompleta o inexistente información fuente, los procesos de liquidación y facturación simplemente no pueden ejecutarse, de allí que, el SIMEC es considerado como un componente crítico dentro del portafolio de servicios que actualmente dispone el CENACE.

La Regulación No. CONELEC 005/006 estipula, *"es responsabilidad del Agente propietario de los equipos de medición publicar diariamente en el portal de Internet del concentrador primario de medidas del CENACE, los archivos de información generados exclusivamente a partir de lecturas TPL, para cada uno de sus puntos de medición. La hora máxima para realizar esta remisión es hasta las 09:00 del día posterior al de operación"*. En función de este requerimiento normativo, para el SIMEC el tiempo máximo de interrupción está en el orden de horas, considerado como un nivel urgente de recuperación.

Desde el punto de vista de los parámetros utilizados en el BIA, el SIMEC tiene la siguiente configuración:

- RTO: 24 horas
- RPO: 24 horas

b) Evaluación de Riesgos

En la Fig. 4 se presenta un ejemplo de la matriz de riesgos resultante del análisis del sistema SIMEC, tomando como referencia la metodología OCTAVE.

Eventos de riesgo	Riesgo Inherente			Respuesta al riesgo				Respuestas/ actividades de control
	Probabilidad	Impacto	Nivel de riesgo	Evitar	Reducir	Compartir	Aceptar	
1. Perdida del enlace comunicación CENACE - CNT	3	3	A		X			Contratar de un enlace de datos adicional con otro proveedor
2. Actualización de la configuración del sistema operativo	3	3	A			X		Adquirir los servicios de soporte especializado del fabricante
3. Corrupción de la base de datos del SIMEC	3	4	E		X			Implementar una solución de backups automatizada

Figura 4: Matriz de Riesgos SIMEC

c) Medidas Preventivas

A continuación se listan algunas medidas preventivas a fin de prevenir la ocurrencia de incidentes no deseados:

- Establecer un enlace de comunicaciones redundante con un proveedor distinto para la publicación de los portales Web del SIMEC.
- Instalación de un software antivirus en todos los servidores de la plataforma Microsoft.

d) Estrategia de Recuperación

En base a los resultados del BIA, el análisis de riesgos, la naturaleza e importancia del proceso que se lleva a cabo en el sistema SIMEC, la estrategia que luce más adecuada para su recuperación es contar con un Hot Site, que permitiría al CENACE continuar con la operación del SIMEC dentro de los períodos de tiempo requeridos (inclusive con tiempos menores) ante la ocurrencia de un evento disruptivo. Este planteamiento sería la opción deseable desde la óptica conceptual indicada en el numeral 6.5.

Al momento el SIMEC cuenta con las siguientes medidas para asegurar en gran parte su operación diaria y disponibilidad:

- Implementación de Clusters, a nivel de los servidores de base de datos se utiliza la configuración activo/pasivo. Otros componentes como los servidores de registradores, aplicaciones y otros componentes de capa media utilizan clusters bajo la modalidad activo/activo sobre una arquitectura de servidores virtualizados, de manera que ante la caída de un servidor guest virtual el mismo sea arrancado en otro servidor host. En la Fig. 5 se muestra la arquitectura física y virtual del SIMEC.
- Almacenamiento, el SIMEC guarda toda su información en una solución de almacenamiento de la gama corporativa, posibilitando la creación de arreglos de discos virtuales que manejan redundancia del tipo 0, 1, 5 y 6.
- Ejecución de backups, es una tarea automatizada que se realizada a través de un robot de cintas, con esquemas de backup diarios tipo full e incremental.

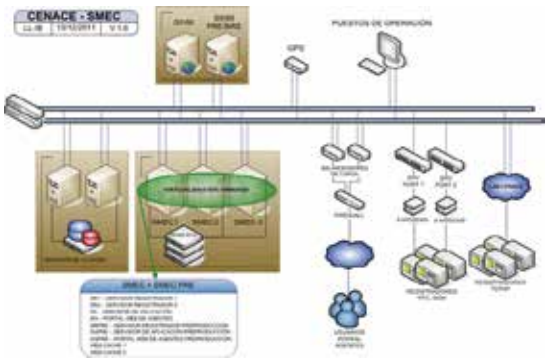

Figura 5: Arquitectura SIMEC

- Las configuraciones previamente indicadas cuentan con sus respectivos instructivos y procedimientos documentados, mismos que constituyen en primera instancia la documentación de recuperación de los componentes del SIMEC.
- Soporte, iniciando desde el hardware de servidores, dispositivos de red, software de base, y culminando con el propio sistema, el CENACE cuenta con el respectivo soporte de los proveedores y con los niveles de respuesta acordes al nivel de exigencia y disponibilidad del sistema.

Finalmente, la operación del SIMEC está bajo la responsabilidad de varios equipos de trabajo interdisciplinarios agrupados en los siguientes roles: Usuarios Operadores, Administradores de Infraestructura y Redes, Bases de Datos y Coordinadores.

8. CONCLUSIONES Y RECOMENDACIONES

- El DRP / BCP involucran procesos complejos que pueden ser los salvavidas de una organización, el contar con procedimientos, infraestructura y recursos para acometer un proceso de recuperación antes de registrarse pérdidas graves, serán la garantía para restaurar la funcionalidad de los servicios de información claves de manera controlada y con la menor pérdida en caso de una interrupción.
- Es vital el conocimiento de la organización y su naturaleza de negocio de parte del equipo de recuperación, pues de ello dependerá la identificación acertada de los procesos críticos sobre los cuales se establecerán las estrategias más convenientes para su implementación, permitiendo además una estimación correcta de los recursos necesarios.
- El SIMEC es un componente crítico para la Corporación CENACE con requerimientos de funcionalidad y disponibilidad establecidos por normativa, que al momento han sido cubiertos satisfactoriamente, sin embargo, existen estrategias de recuperación de desastres alternativas que podrían ayudar a mejorar aún más los niveles objetivo de recuperación, basados en soluciones como Hot Site o el uso de tecnologías emergentes conocidas bajo el nombre de Recuperación como Servicio (Recovery as a Service - RaaS).
- El presente artículo constituye un breve ensayo de lo que sería la aplicación de un plan de recuperación de desastres, es evidente que en un corto plazo este tipo de iniciativas deben ser complementadas a fin de lograr un marco de referencia de acuerdo a la realidad y necesidades propias de CENACE.

REFERENCIAS BIBLIOGRAFÍCAS

[1] EC-Council (2010). “Introduction to Disaster Recovery & Business Continuity”, pp. 8-14, EEUU.

[2] Nickolett, Chip; Schmidt, Jason (2008). “Business Continuity Planning Description and Framework”, Comprehensive Solutions, EEUU.

[3] Erbschloe, M. (2003). Guide to Disaster Recovery. Boston, Massachusetts: Thomson, Course Technology.

[4] ISACA. (2012). CISA Review Manual 2012. 22nd Ed. United States of America.

[5] ISACA. (2012). COBIT 5: Enabling Processes. United States of America.

[6] Alberts, C.y Dorofee A. (2001). OCTAVESM Method Implementation Guide Version 2.0. Pittsburgh: Carnegie Mellon University.

Marco Antonio Bautista Salazar.- Nació en Ambato, Ecuador, en 1976. Recibió su título de Ingeniero en Sistemas Informáticos y de Computación de la Escuela Politécnica Nacional en el 2001, actualmente está desarrollando la tesis de grado para la obtención de su título de Magister en Gerencia de Sistemas y Tecnologías de Información.

Sus áreas de interés están relacionadas con la Administración de Bases de Datos Corporativas, Arquitecturas Orientadas a Servicios, Inteligencia de Negocios, Planes de Continuidad de Negocios y Recuperación de Desastres. Actualmente desempeña las funciones de Coordinador del Área de Informática (Encargado) de la Corporación CENACE.