MAESTRÍA EN GERENCIA DE SISTEMAS Y TECNOLOGÍAS DE INFORMACIÓN

MARCO DE REFERENCIA PARA LA FORMULACIÓN DE UN PLAN DE CONTINUIDAD DE NEGOCIO PARA TI, UN CASO DE ESTUDIO

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de Magister en Gerencia de Sistemas y Tecnologías de Información

Profesor Guía
Ing. Raúl Sanjinés

Autor
Ing. Marco Antonio Bautista Salazar

Año
2014

DECLARACIÓN DEL PROFESOR GUÍA

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

Raúl Antonio Sanjinés Velarde
Ingeniero
C.I.1726552308

DECLARACIÓN DE AUTORÍA DEL MAESTRANTE

Declaro que este trabajo es original, de mi autoría, que se han citado fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

Marco Antonio Bautista Salazar
C.I. 1802777175

AGRADECIMIENTOS

Al Ing. Gabriel Argüello, por su apoyo.
Al Ing. Gonzalo Uquillas, por su colaboración.
Al Ing. Raúl Sanjinés por su acertada dirección.

Ing. Marco A. Bautista S.

DEDICATORIA

A mi esposa Patty y mis hijos Jhean y Sebastián

Ing. Marco A. Bautista S.

RESUMEN

El presente trabajo de titulación propone un marco de referencia para la formulación de un Plan de Continuidad de Negocio para TI o Plan de Recuperación de Desastres (DRP) a través de la aplicación de principios claros y esenciales expresados en un lenguaje natural, basado en las mejores prácticas establecidas por los profesionales/entidades de la gestión de continuidad y recuperación de desastres a nivel mundial. Inicialmente se parte de una visión conceptual de las mejores prácticas de la industria y estándares que sustentan un plan de recuperación de desastres, mediante el análisis comparativo de tres guías DRP relacionadas y se toma como referencia la Norma ISO 22301. En base a los resultados obtenidos, se plantea un marco de referencia para la formulación de un DRP, en el que se identifica su respectivo ciclo de vida, fases, procesos, relaciones y entregables correspondientes. Posteriormente, la aplicación práctica y ejemplificativa del marco de referencia propuesto se lo realiza en un caso de estudio aplicado a uno de los sistemas críticos del Centro Nacional del Control de Energía "CENACE" que es el Sistema de Medición Comercial "SIMEC", visto dicho sistema como un elemento independiente en la organización. Finalmente, se incluyen las conclusiones y recomendaciones de todas las experiencias vividas en las etapas anteriormente mencionadas.

ABSTRACT

This study propose a framework that would allow organizations to formulate a Business Continuity Plan for IT or a Disaster Recovery Plan, through the application of clear and essential principles expressed in everyday language, based on established best practices by professionals/entities of continuity management and disaster recovery worldwide. Initially, a conceptual vision of best practices of the industry and standards that supports a disaster recovery plan is exposed. Through comparative analysis of three guides related DRP and ISO 22301. According to results obtained, a framework is proposed that allow to formulation of a DRP, in which its life cycle, phases, processes, relationships and respective deliverables are identified. Subsequently, the proposed framework will be applied to the study case – the DRP of the CENACE´s "SIMEC" Commercial Measurement System, one of the most critical systems of the "CENACE" National Center for Energy Control, considering to this system as an independent element in the organization. Finally, conclusions and recommendations of all the impressions of the aforementioned steps are included.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Introducción

I. Antecedentes

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 del negocio a causa de una interrupción de los mismos mientras se realiza la recuperación, en caso de un desastre natural o causado por humanos.

Un BCP de TI (Tecnologías de Información) tiene el mismo enfoque que el BCP, con la particularidad de que su alcance se orienta al tratamiento del entorno tecnológico (sistemas, aplicaciones e infraestructura), dicho plan es comúnmente conocido como DRP (Disaster Recovery Plan, por sus siglas en inglés).

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.

El modelo actual de negocios se basa en una fuerte base tecnológica cuya disponibilidad no debe verse afectada por interrupciones parciales o totales. El bien más preciado de las organizaciones es su información, siendo responsabilidad de la Alta Gerencia emplear todos los mecanismos para su obtención, cuidado y resguardo.

Actualmente son contadas las organizaciones que cuentan con un DRP; sin embargo, las amenazas y vulnerabilidades son comunes para todas las empresas sin importar su tamaño, sector de la industria al que pertenecen, localización geográfica, entre otros. El sector financiero es el que más ha desarrollado normativas e implementaciones referentes a la continuidad y recuperación de desastres (Codificación Resoluciones SBS y Junta Bancaria

del Ecuador, 2005). 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; y todo esto simplemente por no contar con procesos, procedimientos e instructivos que identifiquen las acciones previas y posteriores ante un escenario de interrupción de servicios de TI.

II. Objetivos y Alcance

Objetivo General:

Desarrollar un Marco de Referencia para la formulación de un Plan de Continuidad de Negocio para TI (DRP) en base a las mejores prácticas de la industria.

Objetivos Específicos:

a. Describir los principales componentes para la conceptualización de un Plan de Continuidad de Negocio para TI (BCP/DRP).
b. Identificar estándares que sustenten el desarrollo de un BCP/DRP.
c. Seleccionar los componentes esenciales de frameworks existentes para formular un Marco de Referencia para un Plan de Recuperación de Desastres que le permita a una empresa minimizar cualquier impacto negativo en sus operaciones.
d. Aplicar el Marco de Referencia propuesto, en un caso de estudio para el DRP del Sistema de Medición Comercial de la Dirección de Sistemas de Información del Centro Nacional de Control de Energía - CENACE.

Justificación de la Investigación:

En nuestro medio la mayoría de empresas que disponen de una infraestructura tecnológica que sirve de base para soportar sus operaciones, no cuentan con un Plan de Recuperación de Desastres (DRP), mismo que consiste principalmente en las acciones a ejecutarse por parte de la organización en caso de presentarse una interrupción de los procesos de negocio, debido a la pérdida o incapacidad de acceso a los sistemas de información requeridos para su operación normal. Las principales causas que se identifican para la no adopción de un DRP son las siguientes:

- Falta de conocimiento y de instrucciones claras y concisas que detallen por dónde iniciar, alcance y consideración de los factores críticos para tener éxito en un proyecto de este tipo.
- Poca importancia o desconocimiento de parte de la Alta Dirección.
- La implementación de planes y procedimientos de recuperación son costosas, por lo que solamente empresas del sector financiero o del gobierno pueden financiar una iniciativa de ese tipo.
- Si bien existen manuales y recomendaciones que tratan de guiar a las organizaciones a la adopción de mecanismos de recuperación de desastres, la mayoría de estos documentos son contextualmente teóricos, expresados en un lenguaje técnico y formal, no tienen en cuenta la problemática y las necesidades reales de las empresas.

El presente proyecto de titulación, pretende desarrollar 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.

Alcance:

En el presente trabajo de titulación se han planteado cinco capítulos que se detallan a continuación:

En el primer capítulo se realiza un breve estudio de los conceptos y generalidades de un Plan de Continuidad de Negocio, Recuperación de Desastres y otros Planes relacionados.

El segundo capítulo aborda las mejores prácticas de la industria y estándares que sustentan un DRP; así como también, la revisión de algunas guías utilizadas y errores comunes en su implementación.

En el tercer capítulo inicia con un proceso de comparación de algunas guías para la implementación de un DRP, se toma como referencia la Norma ISO 22301, en base a los resultados obtenidos y la experiencia del investigador se plantea un marco de referencia para la formulación de un DRP; en este capítulo se describen las fases, procesos, componentes y entregables que conforman el marco de referencia propuesto.

El cuarto capítulo aplica el marco de referencia propuesto anteriormente, a un caso de estudio para la obtención de un Plan de Recuperación de Desastres en un sistema crítico del Centro Nacional de Control de Energía (CENACE).

Finalmente, en el capítulo cinco se realizan las conclusiones y recomendaciones, es aquí donde se destacan todas las experiencias vividas en las etapas anteriormente mencionadas.

Aspectos que no forman parte del alcance presente trabajo:

- Crear una nueva norma de continuidad de negocio, ni una nueva metodología de recuperación de desastres.
- El análisis de las leyes y reglamentaciones legales relacionadas con recuperación de desastres.
- La definición de estrategias, planes y procedimientos de continuidad para procesos de negocio, los mismos que están fuera del alcance de un DRP.

1 Capítulo I: Visión conceptual de Continuidad de Negocio y Recuperación de Desastres

El presente capítulo inicia abordando la problemática actual que tienen las organizaciones para el manejo de condiciones de crisis ante la ocurrencia de un desastre, se identifican las posibles causas, consecuencias y razones por las cuales una organización debería tomar en cuenta para la recuperación de su operatividad normal. En base a estos antecedentes se introducen los conceptos de Plan de Continuidad de Negocio y Plan de Recuperación de Desastres identificando: alcances, relaciones, diferencias y beneficios particulares de su implementación en la recuperación de desastres. Al finalizar el capítulo se abordan descriptivamente otros planes que están directa o indirectamente relacionados con la temática de recuperación de desastres y continuidad de negocio.

1.1 Causas y Consecuencias de Interrupción del Negocio

El modelo actual de negocios se basa en una fuerte base tecnológica cuya disponibilidad no debe verse afectada por interrupciones parciales o totales. Para el caso, se puede citar el acontecimiento reciente suscitado en el accidente de la central nuclear de Fukushima I el 11 de marzo de 2011, que comprende una serie de incidentes, tales como: las explosiones en los edificios que albergan los reactores nucleares, fallos en los sistemas de refrigeración, triple fusión del núcleo y liberación de radiación al exterior, registrados como consecuencia de los desperfectos ocasionados por el terremoto de Japón oriental. La ausencia de un muro de contención adecuado para los tsunamis de más de 38 m. que han sucedido en la región, permitió que el maremoto (de 15 m. de altura en la central) penetrase sin oposición alguna. La presencia de numerosos sistemas críticos en áreas inundadas facilitó que se produjese una cascada de fallos tecnológicos, culminando con la pérdida completa de control sobre la central y sus reactores (Ragheb, 2011).

Lo suscitado con la Central Fukushima en Japón, es un breve ejemplo de un suceso de gravedad crítica que afecta a una organización, a sus usuarios, al gobierno y la sociedad en general. En el entorno local, también existe el riesgo a la exposición de varios eventos con semejantes consecuencias, por tanto, se puede afirmar que algunas organizaciones no están preparadas para enfrentar incidentes catastróficos que impacten al normal desarrollo de sus actividades.

1.1.1 Causas

Un desastre es un evento 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, según (EC-Council, 2010, pág. 8).

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, sabotaje, empleados disgustados, errores, entre otros. Existe otro tipo de interrupciones como la pérdida del suministro de energía eléctrica, telecomunicaciones y gas natural que igualmente pueden provocar sucesos desastrosos; así como también, pueden darse otro tipo de eventos como: eliminación accidental de la información, ataques de negación de servicios, virus e intrusión, 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.

1.1.2 Consecuencias

Varias son las consecuencias que una organización tiene que afrontar luego de una interrupción de sus operaciones, entre las principales se tienen:

- Pérdida de negocios, ingresos y clientes.

- Deterioro de la imagen, pérdida de credibilidad y confianza de los inversionistas.
- Sanciones regulatorias por incumplimientos de tipo legal.
- Nuevos costos relacionados con la interrupción.
- Cierre parcial o definitivo de sus operaciones.
- Pérdida de información.

1.2 Razones para Recuperar el Negocio

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, con estabilidad y rentabilidad. La mayor parte de ellas poseen bienes tangibles como: insumos, maquinarias, empleados y sistemas computarizados; y bienes intangibles como su información, prestigio, entre otros. La afectación o daño de cualquiera de ellos podrían causar la paralización de actividades. Mientras mayor sea el tiempo de no-disponibilidad de estos recursos, mayor será la posibilidad el sufrir daños irreversibles, 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 estar preparados para 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.
- Demandas del mercado, cada vez los requerimientos de los clientes son más exigentes y en tiempos de respuesta menores.
- Presión de los competidores, ante la no-disponibilidad de los productos o servicios de una empresa, es la competencia la que adquirirá mayor presencia en el mercado.

- 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.

1.3 Plan de Continuidad de Negocio (BCP)

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, (Nickolett & Schmidt, 2001)

Un ejemplo de un proceso de negocio puede ser el manejo de la contabilidad de una organización o el proceso de servicio al cliente; un BCP puede ser escrito para abordar solamente los procesos críticos, una unidad de negocio o se puede direccionar a todos los procesos de una organización, es importante recordar que cada BCP es diferente de una organización a otra, en base a los requerimientos específicos de su propia necesidad de continuidad.

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, (ISACA, 2012).

1.4 Plan de Recuperación de Desastres (DRP)

El DRP (Disaster Recovery Planning, por sus siglas en inglés) es el proceso de evaluación de los riesgos de interrupción de los servicios de TI 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, (Erbschloe, 2003). 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.

Un 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, por tanto, el desarrollo de un DRP no es un proceso meramente mecánico.

1.5 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. En la **Tabla 1** se muestra el cuadro resumen del alcance de un DRP frente al BCP.

Tabla 1. Alcance DRP frente 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.

Fuente: (Introduction to Disaster Recovery & Business Continuity, 2010)

Tanto el BCP como el DRP forman parte de la Gestión de Continuidad del Negocio (Business Continuity Management, BCM por sus siglas en inglés), que es un proceso de gestión integral en materia de continuidad; el BCM analiza las amenazas relevantes y desarrolla para la organización un esquema de resistencia y de respuesta que salvaguarde de forma efectiva los intereses de las partes y del negocio. Dicho enfoque se aplica de manera similar ya sea en un BCP o DRP.

1.6 Beneficios de 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.

Las organizaciones deberían buscar una respuesta planificada ante una interrupción importante de sus servicios de TI que puedan poner en riesgo su subsistencia, independientemente del sector, actividad o tamaño que tuvieren.

Entre otros beneficios de implementar un DRP se tiene:

- Diseño de medidas para reducción de riesgos identificados.
- Identificación 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.
- Protección de los activos de la organización incluyendo al recurso humano.
- Provisión de una base de conocimiento para nuevos empleados.
- Disminución del riesgo de demoras, asegurando que cada recurso esté disponible cuando se lo necesite.
- Orientación en la toma de decisiones durante un desastre, una situación de desastre es altamente estresante, volviendo a la toma de decisiones críticas una actividad exponencialmente compleja en razón al tiempo de reacción.

1.7 Otros planes de Continuidad

Dada la estrecha relación entre TI y los procesos de negocios en toda organización se requiere una gran coordinación desde la planificación hasta la puesta en marcha de cada plan de contingencia, a fin de garantizar la eficacia y eficiencia de las estrategias y recursos establecidos. En la **Figura 1** se muestra la interrelación de cada plan, así como la implementación para responder a los eventos dentro de su ámbito.

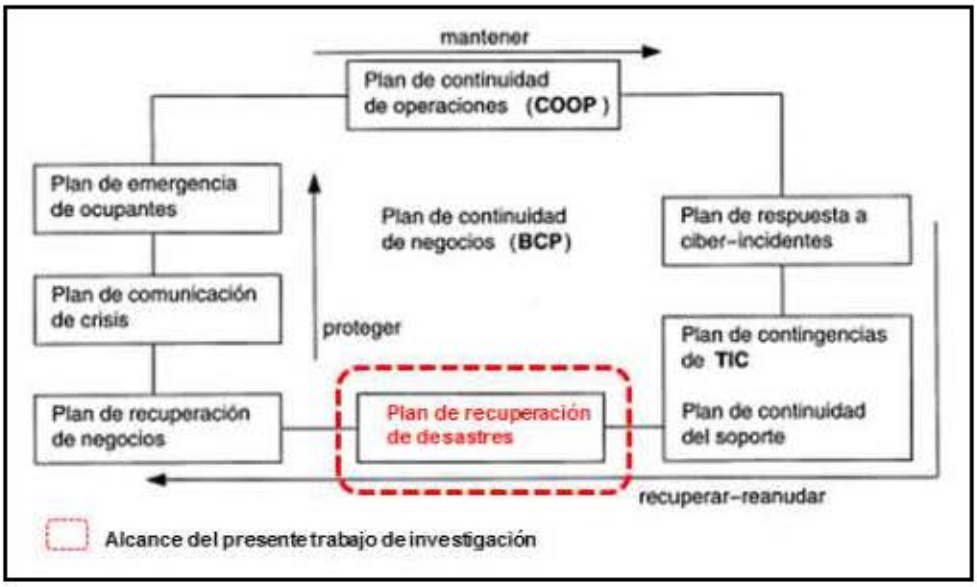


Figura 1. Interrelación entre Planes para el Tratamiento de Emergencias
Fuente: (Seguridad de la Información Redes, Informática y Sistemas de Información, 2008, pág. 260)

A continuación una breve descripción de los planes indicados y presentados en orden alfabético:

- **BCP (Business Continuity Plan)**: Orientado a mantener los procesos de misión y negocio de una organización durante y después de un desastre.

- **COOP (Continuity of Operations Plan)**: Orientado a restaurar los procesos de misión crítica a fin de mantener las funciones esenciales y estratégicas del negocio.

- **CCP (Crisis Communications Plan)**: Implementa procedimientos estándares para la difusión de reportes de estado al cliente, al público y al personal, en el evento de una interrupción.

- **CIRP (Cyber Incident Response Plan)**: Establece procedimientos para el tratamiento de cyber ataques contra los sistemas de información de la organización.

- **DRP (Disaster Recovery Plan)**: Se enfoca en los sistemas de información implementando procedimientos de recuperación de capacidades en un sitio alterno, donde la afectación es de gran magnitud y con efectos a largo plazo.

- **OEP (Occupant Emergency Plan)**: Orientado precautelar la salud y la seguridad de las personas, así como también, su entorno de trabajo.

Cada uno de los planes listados se enfocan en un ámbito específico de acción, definiendo responsabilidades distintas en cada uno de ellos.

En adelante y como objetivo de estudio del presente trabajo, se abordarán los temas relacionados específicamente al Plan de Recuperación de Desastres DRP, cuyo estudio en detalle se presenta en el Capítulo II.

2 Capítulo II: Marco Teórico y Prácticas Recomendadas para la Definición de un Plan de Recuperación de Desastres (DRP)

Este capítulo trata en primer lugar la revisión teórica de los principales marcos de referencia y estándares internacionales que tienen una relación directa con la recuperación de desastres en una organización, a fin de identificar los elementos claves que servirán de base en la elaboración del plan. Posteriormente, la fundamentación teórica continúa con la revisión y análisis de tres guías propuestas para la implementación de un DRP; dichas guías han sido escogidas considerando la diversidad de enfoques en la industria, de manera que en el análisis posterior su aporte sea más significativo. El capítulo finalmente concluye con una breve reseña de aquellos errores que se suelen cometer desde el proceso inicial hasta la culminación de un DRP.

2.1 Normatividad de Referencia

Sin lugar a duda, al momento la mejor referencia para los temas de gestión de continuidad de negocio y recuperación de desastres se encuentran en los frameworks de COBIT, ITIL y en la norma internacional ISO 22301 recién liberada en el año pasado. Es indispensable realizar una revisión de los conceptos y aportes que bajo distintas ópticas son abordados por estos tres referentes.

2.1.1 Consideraciones de COBIT e ITIL

COBIT 5 (Control Objetives for Information & Related Technologies), es un marco para el gobierno y la gestión de las Tecnologías de Información corporativas, que ayuda a las empresas a crear un valor óptimo a partir de TI, manteniendo un equilibrio entre los beneficios, riesgos y recursos.

Se fundamenta en cinco principios que permiten a la organización construir un efectivo marco de Gobierno y Gestión de TI, basado en una serie holística de

siete habilitadores, que optimizan la inversión en tecnología e información, así como su uso en beneficio de sus interesados.

El marco COBIT 5 establece un nuevo Modelo de Referencia de Procesos (Process Reference Model, PRM por sus siglas en inglés), que define y describe en detalle los procesos de gestión: APO (Align, Plan and Organise), BAI (Build, Acquire and Implement), DSS (Deliver, Service and Support) y MEA (Monitor, Evaluate and Assess); y, de gobierno EDM (Evaluate, Direct and Monitor) (COBIT 5 Enabling Processes, 2012).

De manera particular, en el dominio de gestión Entregar, dar Servicio y Soporte (DSS) se encuentra el proceso DSS04 Gestionar la Continuidad, que se refiere a establecer y mantener un plan para que el negocio y TI puedan responder a incidentes e interrupciones con el objetivo de continuar con la operación de los procesos críticos y servicios de TI necesarios, así como, mantener la disponibilidad de la información en un nivel aceptable para la organización. En la **Tabla 2** se muestra el resumen de los subprocesos que soportan el proceso DSS04.

Tabla 2. Subprocesos DSS04

CÓDIGO	NOMBRE	DESCRIPCIÓN
DSS04.01	Definir la política de continuidad del negocio, objetivos y alcance	La política de continuidad y alcance deben estar alineados con los objetivos de la organización y los interesados.
DSS04.02	Mantener una estrategia de continuidad	Evalúa las opciones de gestión de continuidad del negocio, escoge una estrategia de continuidad rentable y viable que asegurará la recuperación y continuidad de la organización en el evento de un desastre o un incidente grave.
DSS04.03	Desarrollar e implementar una respuesta de la continuidad del negocio	Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documenta los procedimientos e información relacionada para su uso en un incidente y que permita a la organización continuar con sus actividades críticas.
DSS04.04	Preparar, probar y revisar el BCP	Probar los mecanismos de continuidad de forma regular para ejercitar los planes de recuperación frente a determinadas situaciones y permitir soluciones innovadoras a ser desarrolladas que ayuden a verificar a tiempo que el plan funcione como se había previsto.

DSS04.05	Revisar, mantener y mejorar el plan de continuidad	Realizar una revisión de la gestión de la continuidad de la capacidad en intervalos regulares para asegurar su continuidad, sustentabilidad, adecuación y eficacia.
DSS04.06	Impartir la capacitación del plan de continuidad.	Provee sesiones de capacitación frecuentes relacionados con los procedimientos, roles y responsabilidades en caso de una interrupción, tanto para usuarios interno y externos.
DSS04.07	Administrar los medios de backup	Mantener disponible la información crítica del negocio.
DSS04.08	Realizar una revisión posterior a la reanudación.	Evalúa la suficiencia del BCP luego de una recuperación satisfactoria de los procesos o servicios del negocio, después de una interrupción.

Fuente: (COBIT 5 Enabling Processes, 2012)

Por otra parte, ITIL V3 (Information Technology Infraestructure Library), es un marco de trabajo y librería de referencia de las buenas prácticas de la gestión de TI. Ofrece una descripción detallada de los procesos más importantes en una organización de TI, incluyendo listas de verificación para tareas, procedimientos y responsabilidades que puede servir como base para adaptarse a las necesidades concretas de cada organización (ITIL Foundations v3 Plus - Manual de Estudiante, 2010).

Bajo la perspectiva de ITIL un servicio es un medio para entregar valor a los clientes, facilitando los resultados que los clientes quieren conseguir sin asumir costos o riesgos específicos, según (ITIL V3 Foundation, 2009).

ITIL enfoca la gestión de servicios a partir del Ciclo de Vida de un servicio, cuyo ciclo consta de cinco fases como se muestra en la **Figura 2.**

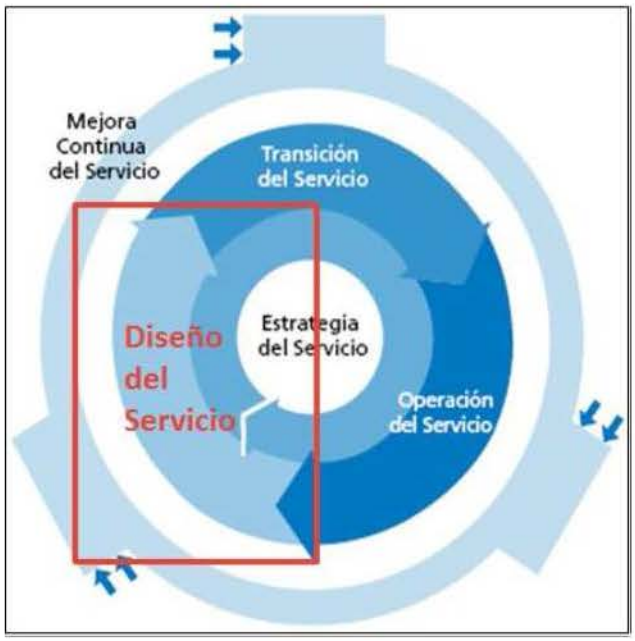


Figura 2. Ciclo de Vida del Servicio
Fuente: (The Art of Service, 2009)

En la fase de Diseño del Servicio del ciclo de vida, todas sus actividades parten de las necesidades del cliente y reflejan la estructura, planificación y la política establecidas en la fase de Estrategia del Servicio. En el diseño se identifican 7 procesos fuertemente relacionados para desarrollar servicios eficaces y eficientes que satisfagan las necesidades de los clientes, en particular, por la temática que se está desarrollando es necesario conocer y analizar el proceso Gestión de la Continuidad del Servicio de TI (IT Service Continuity Management ITSCM, por su siglas en inglés).

El principal objetivo del ITSCM es dar soporte al proceso global de continuidad del negocio, de manera que se garantice que toda la infraestructura y los servicios de TI fundamentales puedan volver a su operatividad dentro de los plazos de tiempo acordados en la organización. Incluye la realización de las siguientes actividades:

- Elaborar y mantener actualizado el análisis de impacto de negocio y análisis de riesgo.
- Desarrollar medidas proactivas para mejorar la disponibilidad de los servicios.

- Acordar y elaborar una estrategia de gestión de continuidad de negocio
- Elaborar los planes de continuidad y recuperación.
- Realizar las pruebas de los planes de continuidad y recuperación.
- Mantener la operación los planes de continuidad y recuperación.
- Establecer acuerdos con los proveedores de TI para comprometer la provisión de los servicios e infraestructura suficientes y necesarios para soportar los planes de continuidad y recuperación.

Es importante recordar que el alcance del ITSMC está centrado en aquellos eventos catalogados como desastres (ver 1.1.1), mientras que los eventos de menor impacto son atendidos por el proceso de Gestión de Incidencias del macro proceso Operación del Servicio.

2.1.2 Norma ISO 22301 Continuidad del Negocio

La norma ISO 22301:2012 denominada Seguridad Societaria – Sistemas de gestión de la continuidad del negocio – Requisitos, proporciona el mejor marco de referencia para gestionar la continuidad del negocio en una organización, es considerada como una actualización de la norma británica (BS 25999-2 Business Continuity Management, 2007). Posibilita a una organización estar preparada para responder adecuadamente ante la ocurrencia de un evento de desastre, así como también, ayuda a minimizar el riesgo de un incidente catastrófico; no tiene limitante en el tamaño, tipo o naturaleza de la organización para su implementación. La medida de la aplicación de los requisitos de esta norma depende del entorno operativo de la organización y su complejidad.

2.1.2.1 Contenido de la Norma

De manera general, la ISO 22301 está organizada en las siguientes cláusulas conforme lo indicado en la **Tabla 3**.

Tabla 3. Cláusulas ISO 22301

CLÁUSULA ISO	DESCRIPCIÓN
0. Introducción	Lineamientos generales sobre la naturaleza, contenido y elementos motivadores para la adopción de este estándar internacional, las relaciones con otras normas que son indispensables para su aplicación, y finalmente la descripción de los términos y definiciones utilizados.
1. Alcance	
2. Referencia a Normativas	
3. Términos y Definiciones	
4. Contexto de la Organización	En base a los objetivos estratégicos establecidos por la organización, la entrega de productos y servicios claves, el apetito al riesgo, el cumplimiento de las obligaciones legales y regulatorias, y los requerimientos de sus partes interesadas; la organización puede diseñar, implementar, mantener y mejorar continuamente su Sistema de Gestión de Continuidad de Negocio (Business Continuity Management System, BCMS por sus siglas en inglés).
5. Liderazgo	Establece el liderazgo y compromiso de la Alta Gerencia con el BCMS, el involucramiento de distintos miembros de la organización con las responsabilidades y autoridad en los roles asignados. La Alta Gerencia establece la política del BCMS.
6. Planificación	Fase en la cual se definen de los objetivos de continuidad de negocio que gobernarán el funcionamiento del BCMS y los planes para alcanzarlos.
7. Soporte	Se concentra en la identificación, disponibilidad y uso de los recursos apropiados para la realización de cada actividad, incluye: determinación de competencias, capacitación, toma de conciencia, comunicación interna y externa, e información documentada y controlada.
8. Operación	Incluye la realización de las siguientes macro actividades: análisis de impacto de negocio, evaluación de riesgos, determinación y selección de la estrategia de continuidad de negocio, definición e implementación de los procedimientos de continuidad de negocio, y para finalizar la realización de las pruebas y ejercicios de los citados procedimientos a fin de asegurar que éstos sean consistentes con los objetivos de continuidad.
9. Evaluación de Desempeño	La norma demanda un seguimiento continuo del BCMS mediante revisiones frecuentes de su funcionamiento, a través del monitoreo, mediciones, análisis y evaluación; permite tomar las acciones necesarias a fin de asegurar su conformidad, adecuación y eficacia. También se identifican los procesos de auditoría interna y revisiones del sistema por parte de la Alta Gerencia.
10. Mejora	Cuando una no conformidad ocurre, ésta debe ser controlada y corregida. El proceso de mejora continua está orientado a identificar oportunidades de mejora en toda la organización, para aumentar la eficacia y la eficiencia de los procesos de manera que permitan entregar mayores beneficios a la organización y a sus partes interesadas.

Fuente: (NORMA ISO 22301, 2012)

2.1.2.2 El modelo Plan-Do-Check-Act (PDCA)

La norma ISO 22301 aplica el modelo conocido como "PHVA: Planificar-Hacer-Verificar-Actuar" (Plan-Do-Check-Act, PDCA por sus siglas en inglés) que puede describirse brevemente como se indica en la **Tabla 4.**

Tabla 4. Modelo PHVA

Planificar	Establecer la política, objetivos, controles, procesos y procedimientos indispensables para mejorar la continuidad del negocio a fin de proveer resultados que estén alineados con las políticas y objetivos organizacionales.
Hacer	Implementar y operar la política, procesos y procedimientos.
Verificar	Realizar el seguimiento y la medición respecto a las políticas y objetivos de continuidad de negocio, informar sobre los resultados, y determinar acciones para remediación y mejora.
Actuar	Tomar acciones para mejorar continuamente el BCMS en base a las acciones correctivas ejecutadas, los resultados de la revisión de gestión y la revisión de su alcance.

Fuente: (NORMA ISO 22301, 2012)

La aplicación del modelo PDCA en los procesos del BCMS asegura un nivel de consistencia con otros sistemas de gestión estandarizados, por ejemplo: ISO 9001, ISO/IEC 27001, entre otros; permitiendo de esta manera que la implementación y funcionamiento con sistemas relacionados sea integral y coherente. En la **Figura 3** se ilustra gráficamente la manera como el BCMS se relaciona con las entradas de las partes interesadas, los requerimientos para la gestión de continuidad, y a través de los procesos y acciones necesarias producir las salidas requeridas.

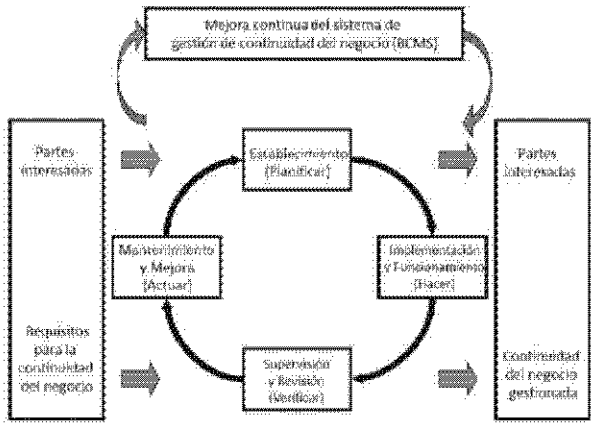


Figura 3. Modelo PDCA aplicada a los procesos del BCMS
Fuente: (NORMA ISO 22301, 2012)

2.2 Revisión de Guías Propuestas para la Implementación de un DRP

En la actualidad existen varias propuestas para la realización de un plan de recuperación de desastres, algunas sustentadas desde la perspectiva universitaria, otras desde el punto de vista de consultores de TI, así como también, las formuladas por los organismos de estandarización, entre otros. Ante esta gran cantidad de información, es preciso realizar una breve recopilación de las principales guías e identificar sus elementos fundamentales sobre los que se basa su funcionamiento. En los siguientes acápites se presentan las guías para la recuperación de desastres planteadas por: la Universidad de Toronto, el investigador Michael Erbschloe e ITIL.

2.2.1 Guía propuesta por la Universidad de Toronto

La Universidad de Toronto realiza el planteamiento de un esquema que podría ser considerado como una guía a manera de ejemplo de los requisitos para la implementación de un plan de recuperación de desastres (Universidad de Toronto, 2011). Propone elaborar un producto que no es sólo de TI, sino que también involucra a los usuarios de los servicios y de gestión de personal que tiene la responsabilidad de la protección de los activos de la organización.

La metodología propuesta enfatiza que para el éxito del desarrollo del DRP, es imprescindible contar con la colaboración de todas las áreas de negocio soportadas por los sistemas de información, así como, la necesidad de contar desde la planificación con personal técnico valioso y los recursos necesarios. La metodología hace hincapié en el desarrollo de ocho fases distintas que se describen a continuación:

Fase 1 - Actividades de Planificación (Inicio del proyecto)

Es usada para la recopilación de información que permita comprender el entorno informático actual y proyectado de la organización, a fin de definir el alcance del proyecto. En esta fase se conforma un Comité Directivo, que se

encargará de la dirección y orientación del Equipo del Proyecto, toma decisiones relacionadas con las actividades de planificación para la recuperación. El Director del Proyecto deberá trabajar con el Comité de Dirección para realizar la Valoración de la Seguridad y el Análisis de Impacto del Negocio.

Los entregables de esta fase son: el desarrollo de una política de apoyo a los programas de recuperación y un programa de concienciación para educar a los involucrados en el proyecto.

Fase2 - Valoración de Vulnerabilidades y Definición General de Requisitos

Esta fase hace referencia a las medidas que se deben tomar para reducir la probabilidad de ocurrencia de un desastre, incluye tareas como: evaluación de la seguridad informática y de comunicaciones incluyendo al recurso humano, infraestructura física, hardware, software, seguridad de bases de datos, seguridad de comunicaciones de voz y datos, control de aplicaciones, entre otros. Esta evaluación permitirá tomar acciones para mejorar los planes de emergencia y las respectivas medidas de prevención.

Otras actividades incluyen el análisis, recomendación y compra de un software para la planificación de recuperación y mantenimiento que apoyen los planes actuales.

Fase 3 - Evaluación de Impacto en el Negocio (BIA - Business Impact Assessment)

La evaluación de impacto en el negocio de todas sus unidades, permitirá al Equipo de Proyecto identificar: sistemas críticos, procesos y funciones; el impacto económico de incidentes y/o desastres resultantes de la imposibilidad de acceso a los servicios, y plazos en los que deberán recuperarse.

Fase 4 - Definición Detallada de los Requisitos

En esta fase se desarrolla un perfil que es usado como base para el análisis de estrategias alternativas de recuperación; este perfil identifica los requisitos de

recuperación para apoyar las funciones críticas previstas en la fase 3, incluye: hardware, software, documentación, soporte externo, instalaciones y personal para cada unidad del negocio. Las estrategias de recuperación se establecerán para: corto, mediano y largo plazo.

Otro entregable clave de esta fase es el documento con la definición del alcance, objetivos y supuestos del plan.

Fase 5 - Desarrollo del Plan

En esta fase se documentan los componentes de los planes de recuperación, se incluye: la actualización de los procedimientos operativos necesarios para apoyar las estrategias, negociación de contratos con proveedores y la definición de los equipos de recuperación, sus roles y responsabilidades. Adicionalmente, se pueden desarrollar durante esta fase estándares de recuperación.

Fase 6 – Programa de Pruebas/ Entrenamiento

En esta fase se desarrolla el plan de pruebas/entrenamiento que permitirá establecer y evaluar las estrategias de experimentación alternativas mediante un programa de pruebas establecido.

Fase 7 - Programa de Mantenimiento

El mantenimiento del plan es crítico para el éxito en caso de una recuperación. Es obligatoria la existencia de un proceso de gestión de cambios que tome en cuenta el mantenimiento del plan de recuperación, muchos productos de software de recuperación toman en cuenta este requerimiento.

Fase 8 - Prueba del Plan Inicial e Implementación

Una vez definido los planes, las pruebas iniciales se llevan a cabo y cualquier modificación necesaria se realizará en base a los resultados obtenidos. A medida que se definen las estrategias de recuperación, los procedimientos de prueba deben ser desarrollados para asegurar que los planes sean completos y precisos.

2.2.2 Guía propuesta por el investigador Michael Erbschloe

El principio esencial para el desarrollo de un plan de recuperación de desastres sólido, requiere contar con el apoyo y participación de la Alta Gerencia, Asesoría Legal y Directores de todos los departamentos funcionales. El citado principio tiene varias implicaciones:

- La implementación del plan y respuesta a los desastres es un esfuerzo de toda la organización.
- El desarrollo del plan requiere de diferentes tipos de conocimientos y habilidades; y,
- La elaboración de una adecuada planificación debe considerar los obstáculos sociales y políticos que afectan a la organización.

El plan de recuperación de desastres puede ser desglosado en ocho pasos importantes según (Erbschloe, 2003) que se indican a continuación:

Paso 1: Organizando el Equipo de Planificación de Recuperación de Desastres

La conformación del equipo de planificación es el primer paso en el desarrollo del plan de recuperación de desastres, éste debe estar conformado con los representantes de todas las funciones de la organización, quienes deberán designar un líder y posteriormente establecer un cronograma de trabajo que incluyan los ocho pasos de la planificación. El equipo debe iniciar una campaña de sensibilización y concienciación acerca de la planificación de recuperación de desastres dentro de la organización bajo el liderazgo de la Alta Gerencia.

Paso 2: Evaluando el Riesgo en la Empresa

El Análisis de Impacto en el Negocio (Business Impact Analysis, BIA por sus siglas en inglés) es un método para la evaluación de riesgos y la determinación de pérdidas económicas potenciales que pueden ocurrir como resultado de esos riesgos.

Mediante el uso del BIA, todos los procesos de negocio deben ser analizados y evaluados para determinar las pérdidas potenciales en las que se podrían incurrir en caso de una interrupción, adicionalmente, el equipo de planificación deberá revisar las afectaciones legales y contractuales, seguros relacionados y coberturas.

Paso 3: Estableciendo Roles en todos los Departamentos y Organizaciones

El equipo de planificación determina el aporte que cada departamento puede hacer con el plan de recuperación de desastres, asegurando que todos los recursos necesarios sean movilizados en un desastre, así como también, las contribuciones que otras organizaciones pueden aportar incluyendo a socios, servicios de emergencia locales, organismos policiales, servicios públicos, proveedores de comunicaciones y de TI.

Paso 4: Desarrollando Políticas y Procedimientos

Las políticas son directrices que rigen el desarrollo de los procedimientos de recuperación de desastres. Los procedimientos son métodos diseñados paso a paso para restaurar una función o proceso de negocio de la organización.

Paso 5: Documentando Procedimientos de Recuperación de Desastres

Las políticas y procedimientos previamente desarrollados son documentados, aprobados e incluidos en el plan para asegurar su éxito. Es necesario establecer un grupo de personas que se encargue de la administración de la documentación, revisiones, actualizaciones y aprobaciones.

Paso 6: Preparando el Manejo de Desastres

Durante este paso el plan final es distribuido a todos los departamentos, organizaciones y empleados involucrados en dar respuesta ante la recuperación de desastres.

Es necesario intensificar los programas de concienciación internos y externos para asegurar que todos los involucrados conozcan del plan, así como también,

que el personal en todos los departamentos sea capacitado en los procedimientos generales y en aquellos en los cuales son directamente responsables.

Paso 7: Entrenamiento, Prueba y Ensayo

Tiene por objetivo probar y ensayar el plan mediante un simulacro de desastre con todos los departamentos y organizaciones de apoyo tal como se lo haría en un desastre real, dicha actividad permitirá ajustar procedimientos, modificar roles, y responsabilidades de los departamentos y empleados involucrados.

Paso 8: Mejoramiento Continuo

Llamada también fase de mantenimiento, una vez terminado el plan, al equipo de planificación le corresponde ajustar continuamente los procedimientos de recuperación debido a la aparición de nuevas amenazas, ajustes a cambios en estructura de la organización, impactos de las nuevas tecnologías, entre otros.

2.2.3 Guía propuesta por ITIL

La ITSCM (IT Service Continuity Management) es un proceso cíclico que adapta continuamente los planes de recuperación y continuidad del servicio a los planes de continuidad del negocio, dicho proceso se desarrolla según (ITIL V3 Foundation, 2009) en cuatro fases:

Fase 1- Iniciación

Se enfoca en toda la organización y está compuesta por las siguientes acciones: definición de la política, especificación de términos de referencia y alcance, asignación de recursos, inicio del proyecto y controles.

Fase 2 - Requisitos y Estrategia

La determinación de los requisitos de negocio para la ITSCM implica la ejecución de un Análisis de Impacto sobre el Negocio y un Análisis del Riesgo.

- El Análisis de Impacto sobre el Negocio tiene por objetivo cuantificar el impacto tangible y/o intangible debido a las pérdidas de los servicios.
- El Análisis o Estimación de Riesgos es una evaluación de los posibles riesgos que podrían provocar una interrupción del servicio o una violación de la seguridad, identifica además las respuestas y contramedidas que se pueden adoptar con justificación de costos.

Desde el punto de vista de las estrategias se tienen:

- Las medidas de reducción del riesgo que se implementan en combinación con la Gestión de la Disponibilidad.
- Las opciones de recuperación de ITSCM que implican un equilibrio entre los costos de las medidas de reducción de riesgo y las alternativas de recuperación para restaurar los procesos de negocio en los tiempos acordados.

Fase 3 - Implementación

Una vez aprobada la estrategia se procede con la creación de los planes de ITSCM, el proceso en referencia debe realizarse con el auspicio de la Alta Gerencia, un líder y un equipo de trabajo interdisciplinario.

Esta fase también incluye los procesos de pruebas exhaustivas, que permitan verificar la eficacia de los planes de ITSCM.

Fase 4 - Operación Continuada

Corresponde la ejecución de las siguientes actividades: educación, concienciación y formación del personal, auditoría, gestión de cambios y pruebas definitivas. Toda la información generada durante el desarrollo de estas fases debe ser documentada para el mantenimiento de los planes de ITSCM.

Al finalizar la revisión de los lineamientos de las guías presentadas para la recuperación de desastres, inmediatamente corresponde realizar el análisis comparativo de las mismas, a fin de obtener un modelo básico aplicable para la

elaboración de un DRP, el citado análisis será tratado en detalle en el Capítulo III.

2.3 Errores Comunes en la Creación de un DRP

El diseño y desarrollo de un DRP es el paso inicial, pero no el último; durante sus etapas de implementación y pruebas se puede recurrir a modificaciones o corrección de errores detectados en la propuesta. 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 basa en de varios supuestos como contar con: la infraestructura y recursos para recuperar los sistemas críticos, los técnicos idóneos, centros de funcionamiento alternos, capacitación, apoyo de la Alta Gerencia, pruebas continuas, entre otros. A continuación se describen los errores más comunes que se deberían evitar en el proceso de planificación de recuperación de desastres (Wallace & Webber, 2011).

- **Confianza ciega en el plan:** Algunas organizaciones tienen la creencia de que es suficiente contar con un DRP y no consideran que éste debe ser sometido a un proceso permanente de pruebas y mantenimiento, pues su utilidad dependerá de ello.
- **Alcance reducido:** El alcance del plan debería cubrir una amplia gama de posibilidades para una recuperación efectiva de los procesos claves del negocio.
- **Inadecuada priorización:** Es necesario la priorización de los proceso clave de la organización, pues de ello depende la correcta inversión de tiempo, dinero y recursos para la recuperación de los procesos que permitirán la sobrevivencia del negocio.
- **Planes desactualizados:** Los cambios en los procesos productivos conducen necesariamente a la actualización del plan.

- **Falta de liderazgo:** Para la implementación de este tipo de proyectos se requiere de capital humano con: poder de liderazgo, influencia, sentido de prioridad, organización y trabajo en equipo, entre otros.
- **Problemas de comunicación:** Se requiere mantener canales de comunicación adecuados y precisos con: empleados, directivos, socios, clientes y proveedores.
- **Pérdida de controles de seguridad:** Es posible que durante el proceso de recuperación se dejen de lado los controles de seguridad, exponiendo a la organización a un mayor riesgo.
- **Pérdida de apoyo de las áreas de negocio:** Es conveniente involucrar a todas las áreas/departamentos en la iniciativa de implementación de un DRP, debido a que la continuidad del negocio y la recuperación de un desastre no sólo le corresponde a TI.
- **Documentación no disponible:** Es importante contar con respaldos de la información necesaria para el DRP en instalaciones fuera de la organización en el caso de la ocurrencia de un desastre.
- **Falta de entrenamiento y capacitación del personal necesario:** La práctica, adiestramiento y socialización de las diferentes medidas compendiadas en un plan, ayudarán a sobrellevar el estrés y ansiedad que acompaña a un desastre.
- **Falta de compromiso de la Alta Gerencia:** Todo plan será inútil sin el auspicio y compromiso de las máximas autoridades de la organización, esto incluye la provisión de los recursos necesarios durante las fases que conlleva un DRP.
- **Falta de flexibilidad en la implementación:** Debido a la naturaleza y requerimientos propios de cada organización, la utilización de la metodología y alcance del DRP debería ser susceptible de modificaciones según sea necesario para lograr sus objetivos.
- **Falta de pruebas:** Todo plan deberá someterse a su correspondiente protocolo de pruebas, mismo que deberá contemplar la mayor cantidad de escenarios de verificación y prueba.

3 Capítulo III: Diseño de un Marco de Referencia para la formulación de un DRP

El presente capítulo inicia con el proceso comparativo conceptual de las tres guías consideradas para la implementación de un DRP (Universidad de Toronto, Michael Erbschloe e ITIL), y su respectiva correspondencia con las cláusulas de la Norma ISO 22301 a través de una matriz de comparación, obteniendo como resultado una serie de elementos comunes e indispensables que podrían ser considerados como la base para la formulación de una propuesta de un DRP. Se parte de un enfoque en el cual la recuperación de desastres debe ser entendida como un proceso continuo y de importancia estratégica para la Alta Gerencia, se plantea una propuesta de un marco de referencia para la planificación de recuperación de desastres con las siguientes fases generales: Planificar, Hacer, Verificar y Actuar (PHVA).

Finalmente, como resultado del análisis de las cuatro fases del marco de referencia propuesto, se identifican los documentos entregables mínimos que evidencian el plan de recuperación de desastres de la organización.

3.1 Comparativo de Guías para la Implementación de un DRP

En relación a las guías revisadas en la sección 2.2, la **Tabla 5** muestra el resumen de las fases/pasos que plantean cada una de ellas.

Tabla 5. Resumen Guías DRP

GUÍA DRP	FASES/PASOS
Universidad de Toronto	Fase 1 - Actividades de Planificación (Inicio del proyecto)
	Fase2 - Valoración de Vulnerabilidades y Definición General de Requisitos
	Fase 3 - Evaluación de Impacto en el Negocio
	Fase 4 - Definición Detallada de los Requisitos
	Fase 5 - Desarrollo del Plan
	Fase 6 – Programa de Pruebas/ Entrenamiento
	Fase 7 - Programa de Mantenimiento
	Fase 8 - Prueba del Plan Inicial e Implementación
Investigador Michael Erbschloe	Paso 1: Organizando el Equipo de Planificación de Recuperación de Desastres
	Paso 2: Evaluando el Riesgo en la Empresa
	Paso 3: Estableciendo Roles en todos los Departamentos y Organizaciones
	Paso 4: Desarrollando Políticas y Procedimientos
	Paso 5: Documentando Procedimientos de Recuperación de Desastres

	Paso 6: Preparando el Manejo de Desastres
	Paso 7: Entrenamiento, Prueba y Ensayo
	Paso 8: Mejoramiento Continuo
ITIL	Fase 1 - Iniciación
	Fase 2 - Requisitos y Estrategia
	Fase 3 - Implementación
	Fase 4 - Operación Continuada

Fuentes: (Erbschloe, 2003) (ITIL V3 Foundation, 2009) (Universidad Toronto, 2013).

De manera general se puede observar la presencia de componentes comunes como: planificación, requisitos, riesgos, pruebas y mantenimiento; sin embargo, en el análisis individual de cada una de las guías se podrían identificar otros elementos relevantes que se evidenciarán posteriormente en la matriz de resultados.

3.1.1 Identificación de Elementos Básicos con Referencia a la Norma ISO 22301

En base a la Norma ISO 22301:2012 los elementos necesarios a considerarse en la formulación de un plan de continuidad de negocio son los indicados en la **Tabla 6.**

Tabla 6. Principales Elementos Norma ISO 22301:2012

CLÁUSULA*	REQUISITO DE LA NORMA
4. Contexto de la Organización	4.1 Entendimiento de la organización y su contexto. 4.2 Entendimiento de las necesidades y expectativas de las partes interesadas. 4.3 Determinación del alcance del sistema de gestión de continuidad de negocio. 4.4 Sistema de gestión de continuidad de negocio.
5. Liderazgo	5.1 Liderazgo y compromiso. 5.2 Compromiso de la dirección. 5.3 Política 5.4 Roles organizacionales, responsabilidades y autoridades.
6. Planificación	6.1 Acciones para direccionar el riesgo y oportunidades. 6.2 Objetivos de continuidad de negocio y planes para alcanzarlos.
7. Soporte	7.1 Recursos 7.2 Competencias 7.3 Sensibilización 7.4 Comunicación 7.5 Información documentada

8. Operación	8.1 Planificación operativa y control. 8.2 Análisis de impacto de negocio y evaluación de riesgo. 8.3 Estrategia de continuidad de negocio. 8.4 Establecimiento e implementación de procedimientos de continuidad de negocio. 8.5 Ejercicios y pruebas.
9. Evaluación de Desempeño	9.1 Seguimiento, medición, análisis y evaluación. 9.2 Auditoría interna. 9.3 Revisión por la dirección.
10. Mejora	10.1 No conformidades y acciones correctivas. 10.2 Mejora continua

*Las cláusulas 0,1, 2 y 3 son de carácter informativo en el contexto de la norma.

Fuente: (NORMA ISO 22301, 2012)

Con referencia a los elementos indicados por la norma ISO 22301, se procede con la elaboración de una comparativa conceptual entre las guías revisadas en el acápite 2.2 del capítulo previo, cuyos resultados se indican en la siguiente sección.

3.1.2 Matriz de Resultados

La construcción de la matriz con la comparativa de las guías revisadas para la implementación de un DRP se realiza bajo el siguiente esquema:

- La primera columna identifica los requisitos de la norma ISO 22301 que serán tomados como la referencia general para el comparativo de las guías.
- Las siguientes tres columnas muestran los componentes de las guías que guardan relación (según el Investigador) con los requisitos de la norma. Una celda en blanco indica que las fases o pasos de la guía analizada no tienen ninguna correspondencia semejante con la norma.

La **Tabla 7** recoge los resultados de la comparación de las tres guías para la implementación de un DRP con la norma ISO 22301.

Tabla 7 Comparativo de Guías DRP frente Norma ISO 22301

REQUISITO NORMA ISO 22301	UNIVERSIDAD TORONTO	MICHAEL ERBSCHLOE	ITIL
4.1 Entendimiento de la organización y su contexto.	F1. Actividades de Planificación		
4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.		P1. Organizando el Equipo de Planificación de Recuperación de Desastres	F1.2 Especificación de términos de referencia y alcance
4.3 Determinación del alcance del sistema de gestión de continuidad de negocio.			
4.4 Sistema de gestión de continuidad de negocio.			
5.1 Liderazgo y compromiso.	F1. Actividades de Planificación	P1. Organizando el Equipo de Planificación de Recuperación de Desastres	
5.2 Compromiso de la dirección.			
5.3 Política		P4. Desarrollando Políticas y Procedimientos	F1.1 Definición de la política.
5.4 Roles organizacionales, responsabilidades y autoridades.	F5. Desarrollo del Plan	P3. Estableciendo Roles en todos los Departamentos y Organizaciones	F1.4 Definición de la organización del proyecto y la estructura de control
6.1 Acciones para direccionar el riesgo y oportunidades.	F2. Valoración de Vulnerabilidades y Definición General de Requisitos		
6.2 Objetivos de continuidad de negocio y planes para alcanzarlos			F1.5 Acuerdo del proyecto y de los planes de calidad.
7.1 Recursos	F1. Actividades de Planificación	P3. Estableciendo Roles en todos los Departamentos y Organizaciones	F1.3 Asignación de recursos
7.2 Competencias			F4.1 Educación concienciación y formación personal
7.3 Sensibilización		P6. Preparando el Manejo de Desastres	
7.4 Comunicación			
7.5 Información documentada	F5. Desarrollo del Plan F7. Programa de Mantenimiento	P.5 Documentando Procedimientos de Recuperación de Desastres	F3.2 Documentación de procesos F4.4 Gestión de Cambios
8.1 Planificación operativa y control.			
8.2 Análisis de impacto de negocio y evaluación de riesgo.	F3. Evaluación del impacto de negocio	P2. Evaluando el Riesgo en la Empresa	F2.1 Definición de requisitos y estrategia.
8.3 Estrategia de continuidad de negocio.	F4. Definición detallada de los requisitos	P4. Desarrollando Políticas y Procedimientos	F2.2 Análisis de impacto de Negocio. F2.3 Análisis de riesgo
8.4 Establecimiento e implementación de procedimientos de continuidad de negocio.	F5. Desarrollo del Plan F8. Prueba del Plan Inicial e Implementación		F3 Implementación
8.5 Ejercicios y pruebas.	F6. Programa de Pruebas /	P7. Entrenamiento, Prueba y	F3.1. Aplicación de diferentes

	Entrenamiento F8. Prueba del Plan Inicial	Ensayo	tipos de pruebas: superficiales, completas, parciales, escenarios de prueba. F4.3 Realización de pruebas F4.5 Prueba definitiva
9.1 Seguimiento, medición, análisis y evaluación.	F5. Desarrollo del Plan F8. Prueba del Plan Inicial e Implementación		F4.2 Revisión y Auditoría
9.2 Auditoría interna.			
9.3 Revisión por la dirección.			
10.1 No conformidades y acciones correctivas.			
10.2 Mejora continua	F7. Programa de Mantenimiento	P8. Mejoramiento Continuo	

Fuentes: (Erbschloe, 2003) (ITIL V3 Foundation, 2009) (Universidad Toronto, 2013) (ISO, 2012)

En función del análisis comparativo de las tres guías y considerando los requisitos de la norma ISO 22301, se han identificado doce componentes comunes en las guías revisadas, por tanto, dichos elementos son catalogados como relevantes en la elaboración de un marco de referencia para la planificación de recuperación de desastres, de acuerdo al siguiente listado:

A. Comprender la organización y sus necesidades.
B. Conformar el equipo de trabajo y nombrar el coordinador
C. Establecer la política de recuperación.
D. Definir el alcance del proyecto, fijar los objetivos, comprometer a la Alta Gerencia y proveer recursos
E. Realizar el análisis de impacto de negocio (BIA)
F. Realizar el análisis de riesgos.
G. Identificar y aplicar medidas preventivas.
H. Determinar la estrategia de recuperación.
I. Establecer los procedimientos de recuperación.
J. Capacitar y ejecutar pruebas.
K. Realizar el seguimiento y auditorías.
L. Propiciar la mejora continua.

3.2 Enfoque del Marco de Referencia Propuesto para un DRP

El DRP es un proceso continuo, por tanto, para abordar su alcance y la relación entre cada uno de sus componentes, el marco de referencia a proponer parte del modelo PHVA (analizado previamente en la sección 2.1.2.2) cuyas fases: planificar, hacer, verificar y actuar, constituyen los cuatro pilares que acogen los componentes clave para la planificación de recuperación de desastres.

Por otra parte, los resultados obtenidos en la matriz de análisis de la sección 3.2.1, proporcionaron doce elementos catalogados como relevantes para la elaboración del DRP.

En consideración a los conceptos del modelo PHVA en el contexto de la recuperación de desastres, cada uno de los componentes clave son

clasificados en base a sus criterios de afinidad de acuerdo a lo mostrado en la **Tabla 8.**

Tabla 8. Fases PHVA Frente a Componentes Relevantes de Guías y Procesos del Marco de Referencia

FASES PHVA	COMPONENTES RELEVANTES DE LAS GUÍAS DE RECUPERACIÓN DE DESASTRES	PROCESOS DEL MARCO DE REFERENCIA PROPUESTO
F1 - Planificar	A. Comprender la organización y sus necesidades.	F1.a – Ambiente de la Empresa
	B. Conformar el equipo de trabajo y nombrar el coordinador.	F1.b – Nombrar el Coordinador de Recuperación de Desastres
	C. Establecer la política de recuperación.	F1.c – Crear la Política de Recuperación de Desastres
	D. Definir el alcance del proyecto, fijar los objetivos y comprometer a la Alta Gerencia.	F1.d – Planificación del Proyecto
F2 - Hacer	E. Realizar el análisis de impacto de negocio (BIA).	F2.e – Análisis de Impacto de Negocio (BIA)
	F. Realizar el análisis de riesgos.	F2.f – Análisis de Riesgos
	G. Identificar y aplicar medidas preventivas.	F2.g – Medidas Preventivas
	H. Determinar la estrategia de recuperación.	F2.h – Estrategia de Recuperación
	I. Establecer los procedimientos de recuperación.	F2.i – Implementación de Procedimientos de Recuperación
	J. Capacitar y ejecutar pruebas.	F2.j – Capacitación y Pruebas
F3 - Verificar	K. Realizar auditorías.	F3.k – Auditorías Internas
F4 - Actuar	L. Propiciar la mejora continua.	F4.l – Acciones de Mejora

Fuentes: (NORMA ISO 22301, 2012) (Erbschloe, 2003) (ITIL V3 Foundation, 2009) (Universidad Toronto, 2013)

El resultado de la combinación del PHVA y los componentes clave, constituyen el marco de referencia propuesto para la planificación de recuperación de desastres[1].

En resumen, el ciclo de vida de la planificación de recuperación de desastres propuesto se divide en cuatro fases; cada fase aborda un conjunto definido de procesos secuenciales e interdependientes como se muestra en la **Figura 4.**

[1] Las particularidades que definen a cada organización las hacen únicas, por lo tanto, el DRP que se implemente será la respuesta a sus propias necesidades.

Figura 4. Marco de Referencia para la Planificación de Recuperación de Desastres

En la siguiente sección se analiza en detalle las fases y procesos que se deberían llevar a cabo en una organización para planificar de forma proactiva, así como también, gestionar las consecuencias de un evento de desastre.

3.3 Descripción de las Fases del Marco de Referencia Propuesto

Cada una de las fases indicadas en la sección previa, involucran la ejecución de una serie de procesos que producen entregables (planes, procedimientos, instructivos, entre otros) indispensables para el inicio y ejecución de una siguiente fase en particular; por tanto, es necesario abordar con el suficiente detalle el alcance de las cuatro fases del marco de referencia para la planificación de recuperación de desastres descritos en los siguientes numerales.

3.3.1 Fase 1 (F1): Planificar

Se parte de la premisa que el proyecto cuenta con el compromiso y la provisión de recursos necesarios por parte de la Alta Gerencia de la organización como requisito primario e indispensable. Sus procesos se encuentran listados en la **Tabla 9**.

Tabla 9. Fase 1 - Planificar

CÓDIGO	PROCESOS FASE 1
F1.a	Ambiente de la Empresa
F1.b	Nombrar el Coordinador de Recuperación de Desastres
F1.c	Crear la Política de Recuperación de Desastres
F1.d	Planificación del Proyecto

3.3.1.1 F1.a – Ambiente de la Empresa

Componente relacionado: A. Comprender la Organización y sus Necesidades

Descripción del proceso: Consiste en conocer el entorno en el que se desenvuelve la organización, identificar las actividades de negocio que contribuyen en la provisión de productos y/o servicios, identificar sus clientes externos e internos, conocer su modelo organizativo, cadena de valor, entre otros. Es importante tener un amplio conocimiento de la naturaleza de la organización, a fin de determinar su situación actual y sus perspectivas futuras (Universidad de Toronto, 2011).

Entregable: E01 Diagnóstico de Situación Actual

3.3.1.2 F1.b – Nombrar el Coordinador de Recuperación de Desastres

Componente relacionado: B. Conformar el Equipo de Trabajo y Nombrar el Coordinador.

Descripción del proceso: El Coordinador de Recuperación de Desastres[2] es el encargado de gestionar y supervisar el proceso de elaboración e implantación del plan de recuperación de desastres, adicionalmente, en función del tamaño de la organización y del alcance establecido, es necesario la conformación de un Equipo de Recuperación de Desastres[3] con los representantes clave de las distintas áreas o procesos de negocio y servicios de TI (Erbschloe, 2003). Se recomienda que el Coordinador sea miembro del equipo de la Alta Gerencia con la suficiente autoridad para llevar a cabo el proyecto satisfactoriamente. La Alta Gerencia y/o el Comité Ejecutivo[4] de la organización tienen la responsabilidad de establecer las directrices para el Equipo, por ejemplo, identificar el alcance y los objetivos que persigue el plan, así como también, las actividades de negocio que son consideradas críticas.

Entregable: E02 Organización Equipo de Recuperación de Desastres

3.3.1.3 F1.c - Crear la Política de Recuperación de Desastres

Componente relacionado: C. Establecer la Política de Recuperación.

Descripción del proceso: La política de recuperación de desastres (Erbschloe, 2003) -paso 4- es un documento corto, consistente, de fácil entendimiento, aprobado por la Alta Gerencia y que define a alto nivel (estratégico) los siguientes elementos en la gestión de la recuperación de desastres:

- Objetivos
- Alcance
- Responsabilidades

---

[2] Se utiliza indistintamente el término Coordinador de Recuperación de Desastres o simplemente el Coordinador.
[3] Se utiliza indistintamente el término Equipo de Recuperación de Desastres o simplemente el Equipo.
[4] El Comité Ejecutivo, se define como un órgano de dirección y administración, conformado por los máximos representantes de cada departamento/área de la organización.

Entregable: E03 Política de Recuperación de Desastres

3.3.1.4 F1.d - Planificación del Proyecto

Componente relacionado: D. Definir el Alcance del Proyecto, Fijar los Objetivos y Comprometer a la Alta Gerencia.

Descripción del proceso: El Coordinador en conjunto con su Equipo, deben realizar la programación de actividades, elaborar presupuestos, coordinar recursos, definir los tiempos e identificar los hitos principales de proyecto con sus respectivos mecanismos de seguimiento (Universidad de Toronto, 2011); todo esto con el objetivo de cumplir con la política y objetivos previamente establecidos.

Entregable: E04 Plan del Proyecto para Recuperación de Desastres

3.3.2 Fase 2 (F2): Hacer

Para la realización exitosa de esta fase, previamente se debe tener un entendimiento de la organización, las actividades clave del negocio que se encargan del desarrollo de productos y servicios, así como también, los recursos de TI necesarios que soportan a dichas actividades, el personal involucrado y sus respectivos proveedores. La **Tabla 10** muestra los procesos pertenecientes a esta fase.

Tabla 10. Fase 2 - Hacer

CÓDIGO	PROCESOS FASE 2
F2.e	Análisis de Impacto de Negocio (BIA)
F2.f	Análisis de Riesgos
F2.g	Medidas Preventivas
F2.h	Estrategia de Recuperación
F2.i	Implementación de Procedimientos de Recuperación
F2.j	Capacitación y Pruebas

3.3.2.1 F2.e - Análisis de Impacto de Negocio – BIA

Componente relacionado: E. Realizar el Análisis de Impacto de Negocio (BIA).

Descripción del proceso: El análisis BIA es un paso necesario en el desarrollo de una estrategia de recuperación de desastres, consiste en evaluar los procesos críticos (y los servicios 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 (CISA Review Manual 2012, 2012).

Con el BIA se deberá determinar la criticidad de los recursos de información (por ejemplo: información, sistemas de software, bases de datos, redes, almacenamiento de datos, entre otros) que soportan los procesos críticos de negocio.

Para la ejecución del BIA, una alternativa válida es realizar entrevistas a grupos y/o usuarios clave de las diferentes áreas/departamentos de la organización, las principales tareas a realizar son:

- Identificar sitios físicos y sistemas de información.
- Evaluar la criticidad de los sistemas de información.
- Determinar el RTO[5] y el RPO[6] de cada sistema.

En el Anexo 1 se presenta un modelo de "cuestionario-BIA" que sirve de apoyo para la ejecución de estas tareas.

Entregable: E05 Análisis de Impacto de Negocio

---

[5] El tiempo de recuperación objetivo (Recovery Time Objective, RTO por sus siglas en inglés) se refiere al período de tiempo después de un incidente en el que un producto/servicio debe ser reanudado, o un recurso debe ser recuperado (CISA Review Manual 2012).

[6] El punto de recuperación objetivo (Recovery Point Objective, RPO por sus siglas en inglés) 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 (CISA Review Manual 2012).

3.3.2.2 F2.f - Análisis de Riesgos

Componente relacionado: F. Realizar el Análisis de Riesgos.

Descripción del proceso: 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 (Introduction to Disaster Recovery & Business Continuity, 2010).

Existen varias metodologías de análisis de riesgos[7], de igual manera soluciones de software[8] que permiten el acompañamiento y automatización de dicho proceso, sin embargo, todas se basan en un mismo esquema de funcionamiento indicado a continuación:

- Identificar activos. Los activos son componentes o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. Los activos deben ser inventariados y valorados en cada una de las actividades críticas de la organización.
- Identificar amenazas. Las amenazas son la causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. Sobre los activos identificados previamente es necesario evaluar sus amenazas y la probabilidad de su ocurrencia.
- Identificar vulnerabilidades. Son toda debilidad que puede ser aprovechada por una amenaza. Para los activos identificados previamente se realiza la identificación y valoración de sus vulnerabilidades o debilidades.
- Calcular el riesgo como la combinación de [impacto de la vulnerabilidad] x [probabilidad de ocurrencia relacionada con un recurso particular de

[7] Como ejemplos de metodologías de análisis de riesgo se tiene: ISO/IEC 27005, MAGERIT, OCTAVE, COSO ERM, entre otras.
[8] Algunos programas computaciones que permiten automatizar el proceso de evaluación de riesgos son: EAR / PILAR, CURA Assesor, entre otros.

información], el riesgo es proporcional al valor de la pérdida/daño y la frecuencia estimada de la amenaza (CISA Review Manual 2012).

El proceso de evaluación de riesgos puede ser desarrollado desde un enfoque cuantitativo, cualitativo o una combinación de ambos, cada uno de ellos tiene sus ventajas y desventajas, la selección de la metodología a utilizar dependerá, del nivel de conocimiento y experiencia del evaluador. En el Anexo 2 se presenta un modelo de "formato para la evaluación cualitativa de riesgos" que sirve de apoyo para la ejecución de esta actividad.

Como resultado de este proceso se obtiene un mapa de riesgos que permite identificar y priorizar aquellos que pueden ocasionar la paralización de los recursos críticos y a su vez las respectivas actividades del negocio.

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 la última circunstancia, aceptando que pudiera ocurrir y anticipando recursos para actuar cuando sea necesario. Es un proceso fundamental en la recuperación de desastres y debe ser realizado con la cercana colaboración de los usuarios clave que conocen las actividades de la organización y el personal especializado de TI.

Entregable: E06 Análisis de Riesgos

3.3.2.3 F2.g - Medidas Preventivas

Componente relacionado: G. Identificar y Aplicar Medidas Preventivas.

Descripción del proceso: A partir de los resultados obtenidos en el 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, pueden activar innecesariamente los procedimientos de recuperación.

Las medias preventivas permiten reducir la probabilidad de ocurrencia de interrupciones en las actividades críticas y minimizar el impacto que pueda provocar en la organización mediante la eliminación de puntos de fallo (Guía práctica para PYMES: cómo implantar un Plan de Continuidad de Negocio, 2010). Para ello se elabora un plan preventivo que incluye acciones que la organización debería adoptar para evitar dentro de lo posible los riesgos que afectan la disponibilidad de sus servicios críticos.

La identificación e implantación de medidas de seguridad debe ser el resultado del equilibrio entre los siguientes factores:

- Riesgo mitigado o impacto reducido.
- Costo de implantación de las medidas de seguridad (económico, humano, ente otros).
- Beneficios aportados a la seguridad de la organización.

Es decir, en lugar de esperar los efectos perjudiciales de un evento de desastre para observar como la organización se recupera, es preferible tomar la iniciativa mediante la aplicación de acciones proactivas frente a posibles amenazas previamente identificados.

Entregable: E07 Plan de Medidas Preventivas de Recuperación de Desastres

3.3.2.4 F2.h - Estrategia de Recuperación

Componente relacionado: H. Determinar la Estrategia de Recuperación.

Descripción del proceso: 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. Una estrategia de recuperación identifica la mejor ruta para recuperar un sistema (o varios) en caso de una interrupción o desastre, y provee los lineamientos básicos para el desarrollo de los procedimientos detallados de recuperación.

Las alternativas de recuperación[9] más comunes son: Cold Sites, Mobile Sites, Warm Sites, Hot Sites, Mirrored Sites y Acuerdos Recíprocos; la elección de la mejor alternativa de recuperación depende de las necesidades de la organización, la criticidad de los procesos de negocio, las aplicaciones que los soportan, el tiempo de recuperación (RTO), costos, recursos, seguridad, entre otros; cada plataforma de TI que soporte una función crítica de negocio, debería contar con una estrategia de recuperación.

Complementariamente a las alternativas previamente indicadas, existen varios métodos de recuperación que deberían aplicarse según se requiera:

- Utilización de cluster's, ya sea bajo la configuración activo-activo o activo-pasivo.
- Arreglo redundante de discos independientes (RAID), protege los datos almacenados frente a fallos físicos a nivel de disco duro.
- En redes de comunicaciones, proporcionar redundancia a nivel de enlaces, equipos de red, recuperación de voz, entre otros.

Una adecuada estrategia de recuperación es aquella que con un costo y tiempo de recuperación aceptable, es razonable comparada al impacto y probabilidad de ocurrencia conforme lo determinado en el BIA. Es recomendable que la selección de las estrategias de recuperación sea debidamente documentada

---

[9] Según (CISA Review Manual 2012), la definición es:

- **Cold Sites**, son instalaciones que cuentan únicamente con el ambiente básico están listos para recibir el equipamiento de TI, comunicaciones, programas, datos u otro soporte de oficina.
- **Mobile Sites**, son instalaciones empacadas y modulares que se colocan en vehículos de transporte y se mantienen listos para instalarse en una ubicación a especificar al momento de la activación.
- **Warm Sites**, son instalaciones con el espacio y la infraestructura básica que incluye algunos o todos los equipos requeridos de TI y comunicaciones. Los programas actuales y los datos se deben cargar antes de que se puedan reanudar las operaciones.
- **Hot Sites**, son instalaciones con el espacio y la infraestructura básica, disponen de todos los equipos de TI y comunicaciones que se requieren para respaldar las aplicaciones críticas. Los costos asociados son altos, pero el funcionamiento de las aplicaciones críticas lo justifican.
- **Mirrored Sites**, son sitios completamente redundantes con replicación de datos en tiempo real desde el sitio de producción.
- **Acuerdos Recíprocos**, son convenios entre dos o más organizaciones con equipos o aplicaciones únicos. En caso de una emergencia, los participantes del acuerdo se comprometen a brindar asistencia mutua.

para cada actividad crítica, así como también, debería ser acordada por la Alta Gerencia de la organización.

Entregable: E08 Definición de la Estrategia de Recuperación de Desastres

3.3.2.5 F2.i – Implementación de Procedimientos de Recuperación

Componente relacionado: I. Establecer los Procedimientos de Recuperación.

Descripción del proceso: 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 plan de recuperación de desastres (DRP) está conformado por un conjunto de procesos y procedimientos interrelacionados, cuyo propósito es ofrecer una respuesta rápida al desastre y a los esfuerzos de recuperación; los citados procedimientos deben documentarse y escribirse en un lenguaje simple, que sea entendible para todos los equipos de recuperación y en ningún caso deberían sustituir la aplicación del sentido común.

Las actividades del proceso de recuperación dependen del tipo de desastre, por tanto, el contenido del plan es una recopilación simplificada y a un alto nivel de la secuencia para cada evento de desastre principal, que a su vez mantiene referencias a procedimientos específicos de reparación. Los escenarios típicos que el plan debería cubrir son los siguientes: casos de pérdida: conectividad de red, sistemas clave de TI, centro de datos, datos críticos o de alguna oficina, entre otros, (Erbschloe, 2003) -paso 5-.

Otro aspecto importante a realizarse en esta fase es la conformación de los equipos de trabajo y asignación de sus responsabilidades, a continuación se listan los equipos de trabajo que según (CISA Review Manual 2012) son comunes y que constan en un DRP:

- Equipo de respuesta a incidentes, son los responsables de analizar y acotar el impacto que una incidencia puede provocar en la organización.
- Equipo de manejo de emergencia, son los responsables de la coordinación de las actividades de todos los equipos de recuperación y tomar las decisiones clave. Se encargan de la activación del plan.
- Equipo de software y aplicaciones, encargados del restablecimiento de los sistemas de base y programas de aplicación.
- Equipo de recuperación de redes, responsables del restablecimiento de las comunicaciones; y, del acceso al sitio de recuperación del sistema (en caso de tenerlo).
- Equipo de pruebas de recuperación, encargados de probar todos los planes desarrollados y evaluar los resultados.
- Equipo de capacitación, responsables de impartir la capacitación a todos los involucrados sobre los procesos y procedimientos de recuperación de desastres.

En su estructura de base, el DRP debería comprender al menos los siguientes componentes:

- Declaración del desastre, que incluye: los criterios para la activación del plan, esquema de escalamiento, relación con otros planes (en caso de existir), los nombres de los responsables, los equipos de recuperación y listas de contactos.
- Un esquema que explique de manera secuencial y estructurada el proceso de recuperación a llevarse a cabo.
- Uno o varios procedimientos específicos de recuperación, organizados por áreas, sistemas de TI o componentes particulares.
- Un listado de los proveedores con sus respectivos números de contacto, direcciones, servicios que prestan, coberturas, entre otros.

Entregable: E09 Plan de Recuperación de Desastres

3.3.2.6 F2.j - Capacitación y Pruebas

Componente relacionado: J. Capacitar y Ejecutar Pruebas.

Descripción del proceso: Todos los equipos de trabajo deben ser adecuadamente capacitados y concienciados acerca de los diferentes conceptos que contempla la recuperación de desastres (riesgos, medidas preventivas, detección de incidencias, procedimientos de recuperación, entre otros). En lo relacionado al alcance de la capacitación, ésta debería abarcar a proveedores o en general a terceros con los que la organización mantiene relaciones de negocio. Los empleados que no sean miembros de algún equipo de trabajo, también deben ser informados sobre las implicaciones de los procesos de recuperación de desastres (The Art of Service, 2009).

Por lo anotado, es importante para la organización identificar los requerimientos de capacitación en función de los diferentes grupos objetivo y definir la estrategia de comunicación más adecuada.

La fase de pruebas contiene principalmente las actividades más importantes que requieran comprobación y certeza en su funcionamiento; dentro de un ambiente que represente de mejor manera las condiciones que serían aplicables en una emergencia verdadera. Es primordial que las pruebas se lleven a cabo por las personas que serían responsables de esas actividades en una situación real de desastre y en intervalos de tiempo planificados.

Las pruebas contemplan al menos las siguientes actividades:

1. Verificar la eficacia del DRP.
2. Evaluar el desempeño de los equipos de trabajo involucrados.
3. Evaluar la coordinación entre el equipo de recuperación de desastres y los proveedores externos.
4. Evaluar la habilidad y capacidad de la opción de recuperación establecida para realizar el procesamiento recomendado.

Al término de cada prueba se deberá crear y mantener la documentación respectiva, a fin de que sirva como evidencia histórica para el análisis y diagnóstico del plan, así como también, el soporte para la toma de medidas correctivas necesarias.

Entregable: E10 Plan de Capacitación del DRP

E11 Plan de Pruebas del DRP

3.3.3 Fase 3 (F3): Verificar

Después que el plan y procedimientos de recuperación de desastres de la organización han sido desarrollados, implementados y probados por parte del Equipo de Recuperación de Desastres, dicho equipo ingresa a una nueva etapa de operación denominada "modo de mantenimiento", en donde sus esfuerzos se orientan a mantener actualizado el plan con los cambios que se podrían dar en la estructura organizacional, procesos de negocio y la incorporación de nuevas tecnologías. Su principal proceso se encuentra indicado en la **Tabla 11**.

Tabla 11. Fase 3 - Verificar

CÓDIGO	PROCESO FASE 3
F3.k	Auditorías Internas

3.3.3.1 F3.k - Auditorías Internas

Componente relacionado: K. Realizar Auditorías.

Descripción del proceso: El Coordinador de Recuperación de Desastres debe administrar las auditorías internas (NORMA ISO 22301, 2012) a intervalos planificados para determinar si el DRP:

- Se ajusta a los requerimientos de recuperación de desastres de la organización.
- Se ha implementado y mantiene de manera eficaz.

Para el efecto se deberá establecer un plan de auditoría que permita definir objetivos, alcance, responsabilidades y requisitos para su realización e informar de los resultados.

Entregable: E12 Plan de Auditoría

3.3.4 Fase 4 (F4): Actuar

La organización deberá mejorar continuamente la eficacia de su DRP, mediante la aplicación constante de su política y objetivos de recuperación de desastres, los resultados de las pruebas y de las auditorías. La **Tabla 12** muestra el proceso perteneciente a esta fase.

Tabla 12. Fase 4 - Actuar

CÓDIGO	PROCESO FASE 4
F4.I	Acciones de Mejora

3.3.4.1 F4.I - Acciones de Mejora

Componente relacionado: L. Propiciar la Mejora Continua.

Descripción del proceso: El plan de recuperación de desastres deberá ser mantenido a través de un ciclo de mejora continua (Erbschloe, 2003) -paso 8-, algunos factores que pueden afectar en su funcionamiento son:

- Cambios a nivel organizativo o de personal.
- Actualizaciones a nivel de infraestructura de TI.
- Adquisición o desarrollo de nuevas aplicaciones/sistemas.

- Cambios en la estrategia de negocio de la organización, que pueden alterar la prioridad de las aplicaciones críticas o promocionar a este nivel otras aplicaciones.
- Revisión de la estrategia de recuperación.

En el caso de que se evidencien cambios que afecten a la organización y por ende a los 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 sus procedimientos. De esta forma, la organización puede disponer de ciertas garantías sobre la eficacia de su plan de recuperación.

Entregable: E13 Plan de Acciones de Mejora

3.4 Documentos Entregables

En la ejecución del marco de referencia propuesto para la planificación de recuperación de desastres, cada proceso de la fase PHVA genera sus respectivos documentos que evidencian los resultados obtenidos, estos entregables constituyen a su vez la información de entrada para la realización del siguiente proceso, dichos documentos se listan en la **Tabla 13**.

Tabla 13. Entregables del Marco de Referencia Propuesto

PROCESOS DEL MARCO DE REFERENCIA PROPUESTO	CÓDIGO	ENTREGABLES
F1.a – Ambiente de la Empresa	E01	Diagnóstico de Situación Actual
F1.b – Nombrar el Coordinador de Recuperación de Desastres	E02	Organización Equipo de Recuperación de Desastres
F1.c – Crear la Política de Recuperación de Desastres	E03	Política de Recuperación de Desastres
F1.d – Planificación del Proyecto	E04	Plan del Proyecto para Recuperación de Desastres
F2.e – Análisis de Impacto de Negocio (BIA)	E05	Análisis de Impacto de Negocio
F2.f – Análisis de Riesgos	E06	Análisis de Riesgos
F2.g – Medidas Preventivas	E07	Plan de Medidas Preventivas de Recuperación de Desastres
F2.h – Estrategia de Recuperación	E08	Definición de la Estrategia de Recuperación de Desastres

F2.i – Implementación de Procedimientos de Recuperación	E09	Plan de Recuperación de Desastres
F2.j – Capacitación y Pruebas	E10	Plan de Capacitación del DRP
	E11	Plan de Pruebas del DRP
F3.k – Auditorías Internas	E12	Plan de Auditoría del DRP
F4.l – Acciones de Mejora	E13	Plan de Acciones de Mejora del DRP

Los entregables previamente indicados, son diligenciados en la aplicación del caso de estudio a realizarse en el Capítulo IV.

4 Capítulo IV: Caso de Estudio, Plan de Recuperación de Desastres para el Sistema de Medición Comercial de la Dirección de Sistemas de Información del CENACE

Este capítulo presenta la aplicación del marco de referencia propuesto para el Sistema de Medición Comercial (SIMEC) perteneciente a la Dirección de Sistemas de Información (DSI) del Centro Nacional de Control de Energía (CENACE) del Ecuador. Para facilitar la comprensión del lector acerca del caso de estudio, se inicia con una breve descripción del Sector Eléctrico Ecuatoriano, el rol que cumple el CENACE, su estructura organizacional y cadena de valor, para finalmente abordar el proceso de Medición Comercial que es soportado por el Sistema SIMEC.

La aplicación del marco de referencia para la planificación de recuperación de desastres en el SIMEC, posibilitará la obtención de una propuesta de su DRP. Finalmente, dicha experiencia permitirá la obtención y evaluación de los resultados de la aplicación del caso de estudio.

4.1 Ambiente de la Empresa

4.1.1 El Sector Eléctrico Ecuatoriano y el CENACE

El Sector Eléctrico del Ecuador fue reestructurado a fin de permitir su modernización mediante la participación del sector privado. Este proceso se inició con la vigencia de la Ley de Régimen del Sector Eléctrico (LRSE) en 1996 y tiene el objetivo de crear un mercado eléctrico desregulado y competitivo, descentralizando la estructura vertical y separando las actividades de generación, transmisión y distribución. Sin embargo, el nuevo esquema no se puso en vigencia sino hasta abril de 1999, fecha en la cual se dio inicio de

las operaciones del Mercado Eléctrico Mayorista (MEM)[10] con cambios significativos en las prácticas operativas y comerciales. En la **Figura 5** se muestra la estructura del Sector Eléctrico Ecuatoriano.

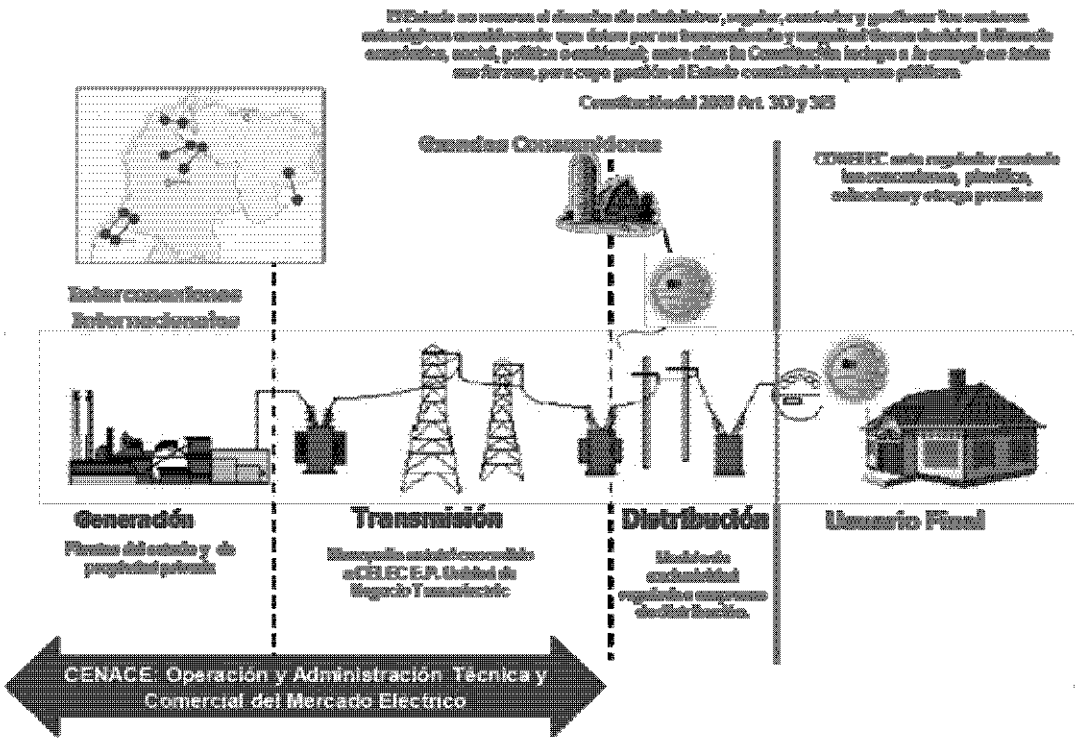


Figura 5. Marco Legal y Estructura del Sector Eléctrico Ecuatoriano
Fuente: CENACE

El sector eléctrico nacional está estructurado de la siguiente manera (Ley de Régimen del Sector Eléctrico, Reglamento y Legislación Conexa, 2007):

a) El Consejo Nacional de Electricidad

b) El Centro Nacional de Control de la Energía

c) Las empresas eléctricas concesionarias de generación

d) La Empresa Eléctrica Concesionaria de Transmisión; y,

e) Las empresas eléctricas concesionarias de distribución y comercialización.

[10] El MEM se define como el sitio donde converge la oferta y la demanda para la compra y venta de energía. Está constituido por Generadores, Transmisor, Distribuidores y Grandes Consumidores.

En la **Figura 6** se muestra la estructura del MEM.

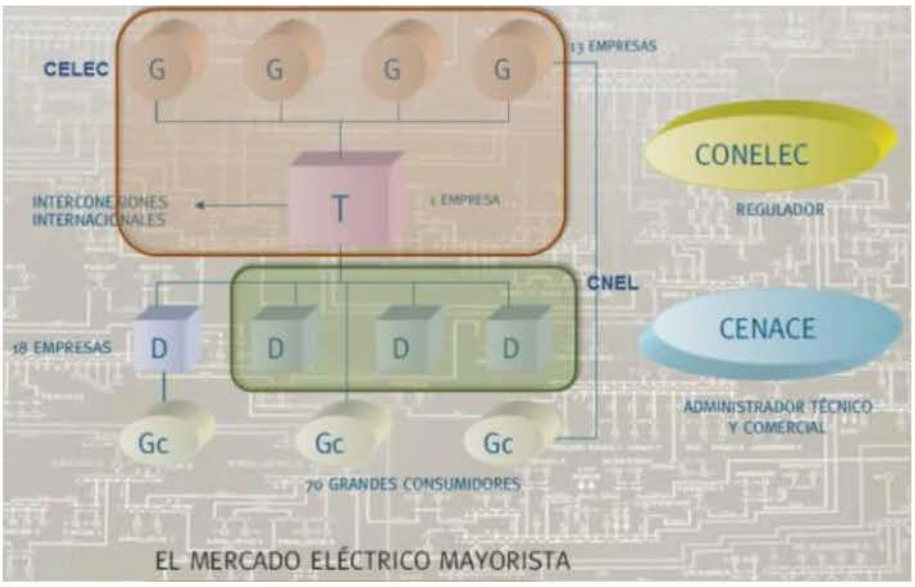


Figura 6. Estructura del Mercado Eléctrico Mayorista
Fuente: CENACE

4.1.2 El Centro Nacional de Control de Energía – CENACE

El CENACE fue creado en la Ley de Régimen de Sector Eléctrico publicada en el Registro Oficial, suplemento 43 del 10/oct/1996, y su estatuto aprobado mediante acuerdo ministerial 151 del 27/oct/1998; como una Corporación Civil de derecho privado, sin fines de lucro, cuyos miembros incluyen a todas las empresas de generación, transmisión, distribución y los grandes consumidores.

Sus funciones se relacionan con la coordinación de la operación del Sistema Nacional Interconectado (SNI)[11] y la administración de las transacciones técnicas y financieras del Mercado Eléctrico Mayorista (MEM) del Ecuador, conforme a la normativa promulgada para el Sector Eléctrico (ley, reglamentos y procedimientos).El CENACE está dirigido por un Directorio formado por:

[11] El SNI está integrado por los elementos del sistema eléctrico conectados entre sí, el cual permite la producción y transferencia de energía eléctrica entre centros de generación, centros de consumo y nodos de interconexión internacional, dirigido a la prestación del servicio público de suministro de electricidad.

1.- Un Delegado Permanente del Presidente de la República quien lo preside;

2.- Dos Delegados de las empresas concesionarias de generación;

3.- Dos Delegados de las empresas concesionarias de distribución;

4.- Un Delegado de la empresa concesionaria de transmisión; y

5.- Un Delegado por los grandes consumidores.

De acuerdo a la LRSE las funciones específicas del CENACE son:

a. La planificación operativa del sistema;
b. La coordinación y control, en tiempo real, tanto de la operación como del mantenimiento del Sistema Nacional Interconectado, SNI;
c. La administración técnica – financiera de las transacciones que se realicen en el Mercado Eléctrico Mayorista, debiendo resguardar las condiciones de eficiencia, calidad, confiabilidad y seguridad de la operación del SNI.
d. La coordinación entre las Empresas de Generación, Transmisión y Distribución o Grandes Consumidores, así como entre los importadores y exportadores de energía, en las distintas actividades que estos tienen que realizar;
e. La operación, mantenimiento y desarrollo de sistemas e infraestructura de supervisión y control de su propiedad.
f. Generar y difundir toda la información operativa.

4.1.3 Misión, Visión y Valores del CENACE

4.1.3.1 Misión

La Corporación CENACE administra con seguridad, calidad y economía, tanto el **funcionamiento técnico** del Sistema Nacional Interconectado e interconexiones internacionales, como el **aspecto comercial del sistema eléctrico ecuatoriano**, incluyendo las transacciones internacionales de electricidad, cumpliendo la normativa para satisfacer a sus clientes.

Esto se consigue mediante la **gestión de un talento humano** calificado y comprometido, a la **disponibilidad de los sistemas tecnológicos de información** y al mejoramiento continuo del **Sistema de Gestión de la Calidad** (Plan Estratégico CENACE 2013).

4.1.3.2 Visión

Ser un organismo líder en la administración operativa y comercial del sector eléctrico ecuatoriano e interconexiones internacionales, que asegure una alta calidad, confiabilidad, y economía del suministro de electricidad, en concordancia con el modelo del desarrollo social y económico del país incluyendo la integración regional.

4.1.3.3 Valores

- Transparencia, es aplicar la Ley de Régimen del Sector Eléctrico y su normativa asociada de manera precisa y permanente ejecutando los procedimientos de los procesos respectivos, brindando acceso a la información al sector eléctrico, facilitando la realización de auditorías y propiciando la participación proactiva de los integrantes del MEM.

- Ética Profesional, es actuar en concordancia con los códigos de ética profesional aplicables, ejerciendo sus responsabilidades con honestidad, objetividad y diligencia a fin de conseguir un desempeño laboral que precautele el prestigio institucional y personal.

- Responsabilidad, es responder con integridad por las actividades propias en los procesos y por las del personal que está a su cargo, a fin de conseguir la eficacia y eficiencia en los resultados contemplados en el Sistema de Gestión de Calidad.

- Lealtad y Compromiso, es demostrar fidelidad y pertenencia a la Corporación, identificándose y contribuyendo al cumplimiento de su misión, visión, valores y objetivos.

4.1.4 Estructura Organizacional y Funcionamiento del CENACE

La naturaleza de las responsabilidades del CENACE ha demandado una estructura organizacional plana, basada en procesos, la misma que cuenta, para establecer un círculo virtuoso de mejoramiento de la calidad, con un Sistema de Gestión de la Calidad (SGC) basado en la norma ISO 9001:2008. En la **Figura 7** se muestra la actual estructura organizacional del CENACE.

Figura 7. Estructura Organizacional del CENACE
Fuente: CENACE

La estructura descrita cuenta con el soporte legal del Área de Asesoría Jurídica de la Corporación.

La cadena de valor agrupa los procesos del CENACE en diez macro procesos, de los cuales cinco están orientados a la administración técnica y comercial del

SNI y del MEM; y, cinco son facilitadores. En la **Figura 8** se muestra los procesos de la cadena de valor del CENACE.

Figura 8. Cadena de Valor del CENACE
Fuente: CENACE

4.1.4.1 La Dirección de Sistemas de Información

La Dirección de Sistemas de Información (DSI) es la responsable de ejecutar el mantenimiento, supervisión y actualización permanente del sistema tecnológico de alta especialización que soporta el circuito técnico – transaccional del MEM, observando apropiados índices de desempeño y disponibilidad. La DSI está estructurada conforme se indica en la **Figura 9**.

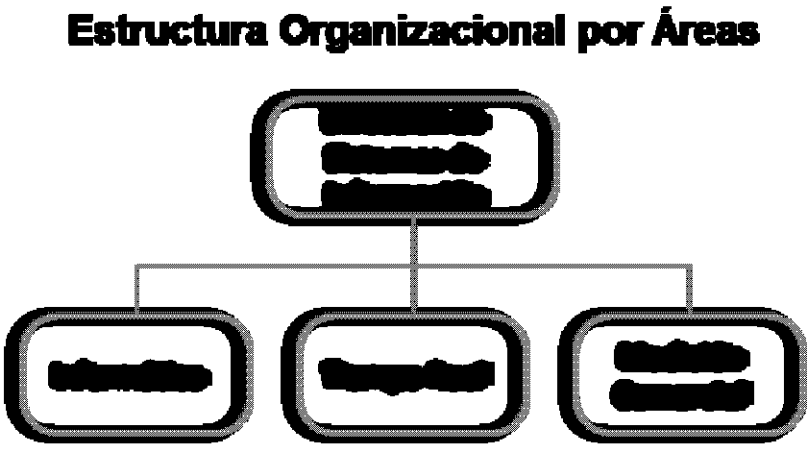


Figura 9. Estructura Organizacional DSI
Fuente: CENACE

La DSI está encargada de la gestión de dos macro procesos de la cadena de valor:

- Administrar el Sistema Informático de Gestión
- Administrar el Sistema de Tiempo Real

4.1.4.2 El Sistema de Información de Gestión – SIG

El Sistema de Información de Gestión (SIG) es la denominación genérica que se adoptó al interior del CENACE para caracterizar a la infraestructura que proporciona los servicios de información fundamentales como: esquemas de seguridad y acceso, mensajería, navegación a Internet, portales de información, integración de aplicaciones, entre otros (Testimonios de Sueños y Realidades, 2013). Adicionalmente, el SIG constituye la arquitectura de información y de aplicaciones de la Corporación que sustentan los procesos para la administración del MEM "fuera de línea", integrados en un Circuito Transaccional Técnico Económico como se muestra en la **Figura 10**. La gestión del SIG está a cargo del Área Informática.

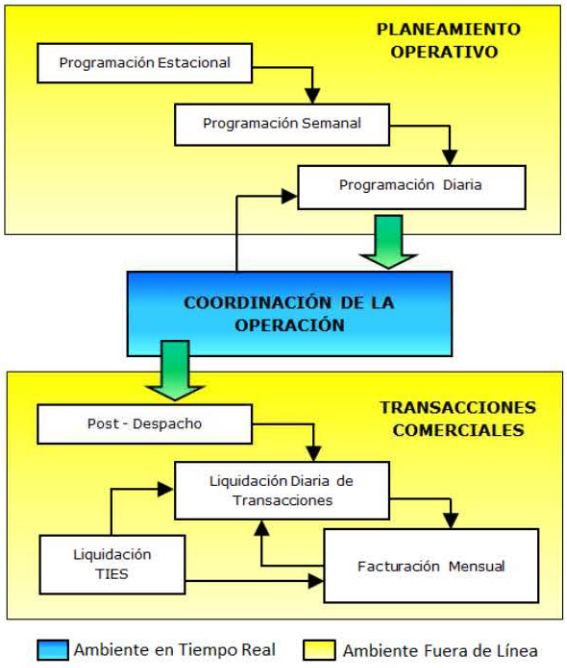


Figura 10. Circuito Transaccional Técnico Económico
Fuente: CENACE

Cabe anotar que la coordinación de la operación del SNI es en "tiempo real" a través del Sistema SCADA/EMS[12] gestionado por el Área de Tiempo Real.

Los principales sistemas informáticos que están bajo la gestión técnica de la DSI se encuentran listados en la **Tabla 14**.

Tabla 14. Sistemas Informáticos Gestionados por la Dirección de Sistemas de Información

PROCESO PRIMARIO	SISTEMAS TÉCNICOS
Planeamiento Operativo	Sistema ePSR – SIPLAN.
Coordinación de la Operación	Sistema de Gestión de Energía – SIMAE/EMS. Sistema de Validación de Información Operativa – SIVO. Bitácora Operativa del SNI - BOSNI.
Transacciones Comerciales	Sistema de Información del Mercado Eléctrico Mayorista – SIMEM. Sistema de Medición Comercial – SIMEC. Sistema Integrado de Gestión Finaciera/Administrativa – ERP.

Fuente: CENACE

Para el caso de estudio a desarrollarse en el ítem 4.2, el análisis se centrará en el sistema fuera de línea denominado Sistema de Medición Comercial (SIMEC) y que es administrado por el Área de Medición Comercial de la DSI.

4.2 Delimitación del Alcance del DRP

4.2.1 El Sistema de Medición Comercial – SIMEC

El SIMEC permite gestionar la medición de los registros cuarto-horarios[13] de energía y otros parámetros eléctricos, en los puntos de generación/entrega del SNI. La información generada en el SIMEC constituye el principal insumo para los procesos de liquidación y facturación del Mercado Eléctrico Mayorista Ecuatoriano.

Funcionalmente, el SIMEC incorpora los siguientes componentes:

---

[12] EMS - Sistema de Administración de Energía (Energy Management System en inglés), es un sistema computarizado dotado de inteligencia artificial, es decir software, para la supervisión y coordinación operativa en tiempo real (instante a instante) de toda la infraestructura de generación, transmisión e interconexiones del país.

[13] Cada quince minutos se obtienen las mediciones de energía en cuatro cuadrantes energía activa/reactiva – entrante/saliente

a) Adquisición y gestión de la información de puntos de medición, mediante:

- Recepción de la información remitida por parte de los Agentes del MEM, en un Portal Web, relativa a los registros cuarto-horarios de energía y su respectivo cualificador, obtenidos mediante una aplicación denominada Terminal Portátil de Lectura (TPL)[14].
- Telemedición de los datos almacenados en los medidores/registradores, mediante conexiones programadas y a través de Internet.
- Gestión remota de los medidores/registradores, para propósitos de sincronización remota y ajuste de parámetros de los transformadores de potencial y corriente.

b) Procesamiento de la Información, a través de mecanismos de priorización de las fuentes de información, chequeos de validez y estimación de información faltante.
c) Almacenamiento y recuperación de información, en un sistema de base de datos relacional que posibilita mantener un inventario de toda la infraestructura de medición de MEM y el expediente histórico de todos los registros de puntos de medición, para efectos de análisis y generación de reportes.

Todos los componentes previamente indicados están integrados a través de un sistema informático que incluye: sistemas operativos, plataforma de virtualización, bases de datos, servidores de aplicaciones y software de gestión de red, la **Figura 11** muestra la Arquitectura Funcional del SIMEC.

[14] TPL, es un software multiprotocolo con capacidad de conexión y descarga local/remota a medidores/registradores y generación de archivos de salida autoetiquetados mediante codificación de identificación unívoca al punto de medición y firma digital.

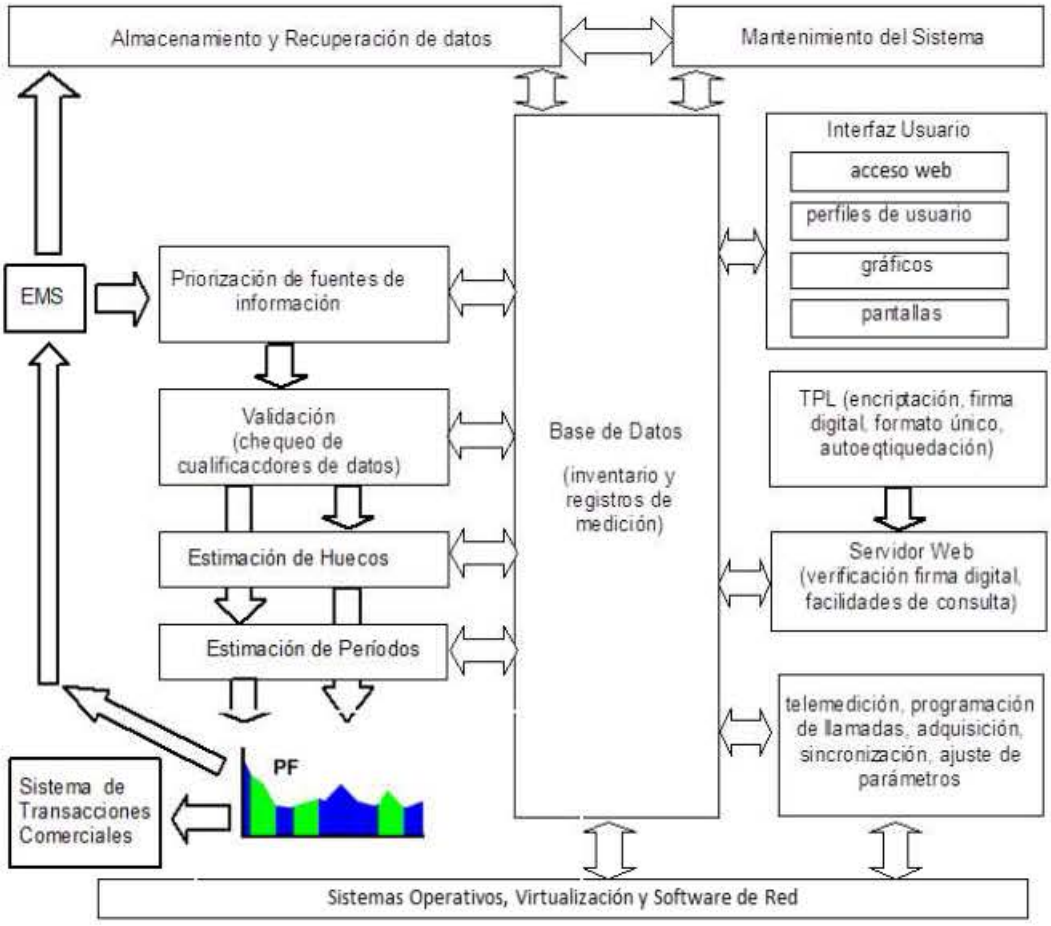


FIgura 11. Arquitectura Funcional del SIMEC
Fuente: CENACE

Una vez conocida la funcionalidad del SIMEC, su importancia en los procesos de la cadena de valor del CENACE; y, con base al marco de referencia previamente analizado, corresponde la aplicación a manera ejemplificativa de los procesos de la planificación de recuperación de desastres aplicados a dicho sistema indicados en el siguiente acápite.

4.2.2 Planificación de Recuperación de Desastres para el SIMEC

En la presente sección de procede con la aplicación del marco de referencia propuesto para la formulación de un DRP aplicado al SIMEC, considerando a dicho sistema como un elemento independiente de otros sistemas de TI de la Corporación CENACE.

Para el desarrollo de las fases del DRP, la estrategia a seguir consistirá en describir las actividades realizadas durante cada proceso de la planificación, y como resultado de su aplicación se obtendrán los documentos entregables que fueron identificados en la sección 3.4.

4.2.2.1 Fase 1 – Planificar

Proceso: F1.a Ambiente de la Empresa

Actividades: La recopilación de la información que permitió conocer, estudiar y analizar la situación del sector eléctrico ecuatoriano, la naturaleza y funcionamiento del CENACE, se encuentran ampliamente documentadas en varias fuentes de información como: la Ley del Régimen del Sector Eléctrico, el Plan Estratégico del CENACE año 2013 y "Testimonios de Sueños y Realidades" que es la memoria institucional del CENACE editada en el año 2013. Los citados documentos fueron consultados en el Centro de Documentación e Información (CDI) que es un servicio que provee el CENACE a la comunidad.

La elaboración del documento SITUACIÓN ACTUAL DEL CENACE se realizó con el soporte del Área de Análisis y Control de la Corporación.

Tiempo empleado: 16 horas.

Entregable:

E01	DIAGNÓSTICO DE SITUACIÓN ACTUAL DEL CENACE

I. El Sector Eléctrico Ecuatoriano
II. El Centro Nacional de Control de Energía – CENACE
III. Misión, Visión y Valores del CENACE
IV. Estructura Organizacional y Funcionamiento del CENACE

El desarrollo de cada uno de los ítems previamente indicados se encuentra detallado en la sección 4.1 del presente trabajo.

Proceso: F1.b Nombrar el Coordinador de Recuperación de Desastres

Actividades: La organización del equipo de recuperación de desastres se llevó a cabo en coordinación directa con el Director de Sistemas de Información, quien asumió de manera natural la Coordinación de Recuperación de Desastres de la Corporación, como responsable de la planificación, diseño y seguimiento de las políticas y lineamientos para la administración de la plataforma tecnológica del CENACE; y en su calidad de integrante del Comité Ejecutivo.

Bajo este mismo esquema, la conformación del Equipo de Recuperación de Desastres se realizó en base a las actividades que actualmente desempeñan los Funcionarios de la DSI, según el manual de responsabilidades y perfiles de competencia de la Corporación.

Tiempo empleado: 6 horas.

Entregable:

E02	ORGANIZACIÓN EQUIPO DE RECUPERACIÓN DE DESASTRES DEL CENACE

A. COMITÉ EJECUTIVO

Está conformado por los siguientes miembros:

Tabla 15. Miembros del Comité Ejecutivo

NOMBRE	CARGO
Ing. Gabriel Argüello R.	Director Ejecutivo
Ing. Max Molina	Director de Planeamiento
Ing. José Medina	Director de Operaciones
Ing. Fabián Novoa	Director de Transacciones Comerciales
Ing. Gonzalo Uquillas	Director de Sistemas de Información
Ing. Lupita Romero	Directora de Administración y Finanzas
Ing. Linda Chimborazo	Jefe de Análisis y Control

Fuente: CENACE

B. COORDINADOR DE RECUPERACIÓN DE DESASTRES

El Coordinador de Recuperación de Desastres de la Corporación CENACE es el Ing. Gonzalo Uquillas, Director de Sistemas de Información.

C. EQUIPO DE RECUPERACIÓN DE DESASTRES (SUGERIDO)

Está conformado por los siguientes integrantes:

Tabla 16. Miembros del Equipo de Recuperación de Desastres

NOMBRE	FUNCIÓN
Ing. Jorge Aguilar	Especialista de Medición Comercial
Ing. Anita Álvarez	Administración Base de Datos
Ing. Hugo Paredes	Administración de Aplicaciones e Infraestructura
Ing. Juan Vallecilla	Administración de Infraestructura de Red
Ing. Wilson Marcayata	Administración Servicios Auxiliares
Ing. Andrés Narváez	Coordinación Área de Tiempo Real
Ing. Marco Bautista	Coordinación Área de Informática

Fuente: CENACE

Proceso: F1.c Crear la Política de Recuperación de Desastres

Actividades: La propuesta inicial de la Política de Recuperación del CENACE se desarrolló mediante un taller de trabajo con el Director de Sistemas de Información y los Coordinadores de la DSI, seguidamente, se contó con la retroalimentación y comentarios por parte del Equipo de Recuperación de Desastres.

Al momento, la referida política se encuentra en una fase de revisión y validación por parte del Área de Análisis y Control previo a llevarlo a consideración de la Dirección Ejecutiva.

Tiempo empleado: 24 horas.

Entregable:

E03 POLÍTICA DE RECUPERACIÓN DE DESASTRES DEL CENACE

A. GENERALIDADES

La información es un recurso que, como el resto de los activos, tiene valor para el CENACE y por consiguiente debe ser debidamente protegida.

El Plan de Recuperación de Desastres protege la Información de una amplia gama de amenazas, a fin de asegurar el funcionamiento de los sistemas de información, la integridad y disponibilidad de los datos, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del CENACE.

Es importante que los principios de la Política de Recuperación de Desastres sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades del CENACE y de los Directores de Área para la difusión, consolidación y cumplimiento de la presente Política.

B. OBJETIVOS

El Comité Ejecutivo ha establecido la política interna de recuperación de desastres de CENACE, como se indica a continuación:

- Proteger los recursos de información del CENACE y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- El Plan de Recuperación de Desastres de CENACE deberá contemplar todos los elementos esenciales y críticos de infraestructura, sistemas computacionales y las redes de comunicación, de acuerdo con las actividades críticas de su cadena de valor.
- CENACE se responsabilizará que la gestión de riesgos se lleva a cabo periódicamente para determinar los requisitos del Plan de Recuperación de Desastres.
- CENACE procurará que el Plan de Recuperación de Desastres se mantenga actualizado, revisado, probado y se mejorará de forma periódica ante cambios significativos en procesos, procedimientos, personas, tecnología o estructura organizativa.
- CENACE propiciará que todo el personal del TI esté informado de las responsabilidades que le correspondan dentro del contexto de la Recuperación de Desastres, mediante sesiones de capacitación, difusión y pruebas del Plan de Recuperación de Desastres.

C. ALCANCE

Esta Política se aplica en todo el ámbito de la Dirección de Sistemas de Información de la Corporación CENACE con sus respectivos recursos.

D. RESPONSABILIDADES

El Director Ejecutivo y el Director de Sistemas de Información son responsables de la implementación de esta Política de recuperación de desastres dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

Las máximas autoridades del CENACE aprueban esta Política y son responsables de la autorización de sus modificaciones.

El **Comité Ejecutivo** del CENACE, procederá a revisar y proponer al Director Ejecutivo del CENACE para su aprobación la Política de Recuperación de Desastres y las funciones generales en esta materia; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la recuperación de desastres; aprobar las principales iniciativas para incrementar la seguridad de la información; promover la difusión y apoyo para las pruebas de recuperación de desastres dentro del CENACE.

El **Coordinador de Recuperación de Desastres** será el responsable de coordinar las acciones del Comité Ejecutivo y de impulsar la elaboración, implantación y cumplimiento de la presente Política.

El **Equipo de Recuperación de Desastres** cumplirá la función de cubrir los requerimientos de recuperación de desastres establecidos en la presente política, para los recursos de TI del CENACE.

Proceso: F1.d Planificación del Proyecto

Actividades: La planificación del proyecto de recuperación de desastres se realizó con la participación del Director de Sistemas de Información en su calidad de coordinador de recuperación de desastres, con el Coordinador del Área de Informática como miembro del equipo de recuperación de desastres y cumpliendo el rol del analista del proyecto. La estructuración del plan se la realizó considerando el formato manejado al interior del CENACE para la gestión de proyectos establecidos por parte del Área de Análisis y Control.

Tiempo empleado: 8 horas.

Entregable:

E04	PLAN DEL PROYECTO PARA LA RECUPERACIÓN DE DESASTRES PARA EL SISTEMA SIMEC

A. INFORMACIÓN GENERAL

Nombre del Proyecto:	IMPLEMENTACIÓN DEL DRP PARA EL SIMEC	**Fecha de Preparación:**	2013-10-02
Participantes:	Equipo de Recuperación de Desastres	**Auspiciado por:**	Ing. Gabriel Argüello Ing. Gonzalo Uquillas
Elaborado por:	Ing. Marco Bautista		
Versión del documento:	1.0		

B. LISTA DE LAS PRINCIPALES ACTIVIDADES DEL PROYECTO

Tabla 17. Listado de Actividades del Proyecto

ACTIVIDAD MACRO	SUBACTIVIDADES
Fase 1 – Planificar	Crear equipo DRP – SIMEC Designar Coordinador de Recuperación de Desastres Coordinar reuniones de trabajo con Director DSI e Ingenieros de Proceso de Medición Comercial. Adquirir suministros de oficina.
Fase 2 – Hacer	Elaborar el análisis de impacto de Negocio – SIMEC Elaborar el análisis de riesgos – SIMEC

	Crear el plan de medidas preventivas Definir la estrategia de recuperación de desastres Crear el plan de recuperación de desastres Elaborar el plan de pruebas DRP Elaborar el plan de capacitación DRP Salida a producción
Fase 3 - Verificar	Elaborar el plan de auditoría del DRP
Fase 4 – Actuar	Elaborar el plan de acciones de mejora del DRP
Cierre del proyecto	Entrega de toda la documentación

Fuente: CENACE

C. LISTA DE LOS HITOS DEL PROYECTO

Tabla 18. Listado de Hitos del Proyecto

No.	HITO	DESCRIPCIÓN
1	Reunión de "kick off" del proyecto.	Acta de inicio del proyecto.
2	Política de recuperación de desastres aprobada.	Acta de aprobación de la política DRP.
3	Culminación del análisis BIA y Riesgos	Informe BIA y análisis de riesgos
4	Definición estrategia DRP - SIMEC	Acta selección de estrategia DRP
5	Capacitación DRP	Acta de validación de capacitación
6	Pruebas DRP	Acta de validación de pruebas
7	Salida a producción	Acta de entrega/recepción, suscripción de contratos cliente/proveedor

Fuente: CENACE

4.2.2.2 Fase 2 – Hacer

Proceso: F2.e Análisis de Impacto de Negocio (BIA)

Actividades: El análisis BIA se lo realizó aplicando las siguientes acciones:

- Aplicación del "cuestionario-BIA" (Anexo 1) al Director de Sistemas de Información.
- Revisión de los documentos del proceso Administrar la Información del SMC con un ingeniero encargado de la Administración del Sistema de Medición Comercial.
- En el ámbito normativo, se requirió la revisión de la Regulación No. CONELEC 005/006 SISTEMA DE MEDICIÓN COMERCIAL DEL MERCADO ELÉCTRICO MAYORISTA (MEM).
- Revisión de los compromisos de envío y recepción de información de medidas de energía, estipulados en el Contrato Cliente/Servidor suscrito entre la Dirección de Sistemas de Información y la Dirección de Transacciones Comerciales.

Una vez analizada la información fuente, fue factible la identificación del nivel de criticidad del sistema y la determinación del RTO y el RPO objetivos del SIMEC.

Tiempo empleado: 40 horas.

Entregable:

E05	ANÁLISIS DE IMPACTO DE NEGOCIO DEL SISTEMA SIMEC

A. GENERALIDADES

La Corporación CENACE cuenta con un modelo organizativo basado en el diseño y trabajo con procesos, desde el año 2003 mantiene la certificación ISO 9001 para su Sistema de Gestión de Calidad.

Según el plan de calidad[15] aplicado por la Dirección de Sistemas de Información, dentro del macroproceso **P.10 Administrar el Sistema de Tiempo Real**, consta el proceso **P.10.3 Administrar el Sistema de Medición Comercial**, que a su vez hace referencia al subproceso **P.10.3.2 Administrar la Información del SMC** con su respectivo procedimiento **PR-DSI-S01 Administración de la Información del Sistema de Medición Comercial.** Dicho procedimiento contempla desde el punto de vista funcional, todas las acciones a realizarse por parte de los Administradores del Sistema SIMEC para la gestión de la información de energía.

La sede principal del CENACE se encuentra ubicada en la Panamericana Sur Km 0 y Av. Atacazo, Parroquia Cutuglahua, Sector Santa Rosa.

B. PROCESOS Y SISTEMAS DE INFORMACIÓN

En la siguiente tabla se muestra un listado de los procesos de negocio[16] de CENACE con sus respectivas Direcciones y sistemas de información que los sustentan:

Tabla 19. Procesos, Sistemas Tecnológicos y Calificación de Criticidad

DIRECCIÓN	PROCESO	SISTEMA	CRITICIDAD*
TRANSACCIONES COMERCIALES	P.5 Administrar y Liquidar las Transacciones del MEM y de las TIE	SIMEM	Alto
		SVM	Bajo
		HIS - EMS	Bajo
SISTEMAS DE INFORMACIÓN	P.10.3 Administrar el Sistema de Medición Comercial	SIMEC	Alto

* El nivel de criticidad se define como: alto, medio y bajo

Fuente: CENACE

Según el diagrama de procesos, el resultado del **P.10.3 Administrar el Sistema de Medición Comercial** que es la provisión de los registros de

[15] Documento que relaciona los procesos, requisitos de la norma ISO 9001 y los procedimientos e instructivos aplicados.

[16] Listado reducido de procesos dado el alcancel del caso de estudio.

energía cuarto-horaria, constituye uno de los principales e indispensables insumos para la ejecución del proceso **P.5 Administrar y Liquidar las Transacciones del MEM y de las TIE**. Ante la incompleta o inexistente información fuente, los procesos de liquidación y facturación simplemente no pueden ejecutarse, de allí que, el sistema SIMEC es considerado como un componente de alta criticidad dentro del portafolio de servicios que actualmente dispone el CENACE.

C. EVALUACIÓN RTO Y RPO

Desde el punto de vista normativo, 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.

Bajo esta premisa, la siguiente tabla muestra los resultados de RTO y RPO objetivos para el SIMEC.

Tabla 20. Resultados RTO y RPO del SIMEC

DIRECCIÓN	DIRECTOR	PROCESO	RTO	RPO	COMENTARIO
DSI	Ing. Gonzalo Uquillas	Administrar el Sistema de Medición Comercial	24 horas	24 horas	Una no-disponibilidad mayor genera: • Pérdida de credibilidad y desconfianza de parte de los Agentes del MEM. • Deterioro de la imagen del CENACE ante las Autoridades del Sector.

Fuente: CENACE

Para el caso del RPO, el tiempo de 24 horas fue analizado, validado y ratificado por el Director de Sistemas de Información en su calidad de responsable del proceso de Administración del Sistema de Medición Comercial, y corroborado por los Ingenieros responsables de su ejecución, a su vez el RPO mantiene concordancia con los requerimientos actuales de funcionamiento del MEM.

Por otra parte, el RTO también fue definido por un consenso entre el Director de Sistemas de Información y los Ingenieros responsables del proceso, en un valor de 24 horas, basados en que la frecuencia de obtención de datos de energía en todos los medidores/registradores del SNI es diaria. Cabe indicar que el RTO establecido para el SIMEC está por debajo del valor máximo tolerable de no-disponibilidad de SIMEC determinado en tres días.

D. CONCLUSIONES

- El SIMEC es un sistema computacional indispensable para la ejecución del proceso para la gestión de las medidas de energía de los puntos de generación/entrega del SNI. Ante la falta o incompleta información de medición comercial, los procesos de liquidación y facturación de Mercado Eléctrico Mayorista no se pueden llevar a cabo.

- Para el CENACE, el proceso Administrar el Sistema de Medición Comercial está catalogado como crítico y de alta prioridad de recuperación ante un evento de no-disponibilidad.

Proceso: F2.f Análisis de Riesgos

Actividades: Para el análisis de riesgos se estructuró el siguiente plan de acción:

- Desarrollo de la evaluación cualitativa de riesgos aplicado al SIMEC utilizando para el efecto el toolkit facilitado en el Anexo 2, y con el soporte del Área de Análisis y Control del CENACE.
- Según corresponda, para las actividades de identificación de: activos, amenazas, vulnerabilidades y cálculo de riesgo, se contó con la participación activa de los miembros del equipo de recuperación de desastres encargados de la gestión de infraestructura, redes, aplicaciones, bases de datos y manejo del SIMEC.

Al finalizar la aplicación del toolkit, se logró obtener la categorización de los activos del SIMEC con su respectivo nivel de riesgo.

Tiempo empleado: 48 horas.

Entregable:

E06 ANÁLISIS DE RIESGOS PARA EL SISTEMA SIMEC

A. GENERALIDADES

Se entiende por análisis de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la normal operación del CENACE.

El CENACE debe tener conocimiento actualizado sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.
- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.
- Activos físicos: equipamiento informático (servidores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.
- Servicios: informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Para el análisis de riesgos del Sistema SIMEC se ha tomado el marco metodológico de la norma ISO/IEC 27005, apoyada para temas específicos en NIST-800-30 y MAGERIT; dando como resultado un marco de análisis hibrido y adaptado a los propósitos específicos para el caso de estudio en tratamiento. En el proceso de análisis de riesgos se utilizó el toolkit "Curso Gestión de Riesgos ISO 27005", incluido en el Anexo 2.

B. IDENTIFICACIÓN DE ACTIVOS

En la **Tabla 21** se muestra el inventario de activos correspondientes al Sistema SIMEC con su respectiva valoración:

Tabla 21 Inventario de Activos de Información SIMEC

CODIGO	ACTIVOS	CATEGORIA	DESCRIPCIÓN	UBICACIÓN	RESPONSABLE/ DUEÑO	CONF.	INT.	DISP.	CONSECUENCIA OPERACIONAL	CONSECUENCIA REPUTACIONAL	CONSECUENCIA ECONÓMICA	CONSECUENCIA REGULATORIA	CONSECUENCIA FINAL	VALOR DEL ACTIVO
A1	Enlace WAN entre CENACE y CELEC EP - TRANSELECTRIC	Servicios	Servicio ofrecido por TRANSELECTRIC para el acceso por fibra óptica a los medidores/registradores en el SNI.	CENACE - SUBESTACION SANTA ROSA	JV	3	3	3	4	2	1	4	4	36
A2	Firewall Data Center CHECK POINT	Red	Elemento de seguridad para el control y segmentación de tráfico a nivel de red para el SIMEC.	SEDE CENACE	JV	2	2	3	4	2	1	3	4	28
A3	Servidores de Base de Datos (HP BL460c GT CTO Blade)	Hardware	Servidores físicos donde reside las bases de datos del SIMEC	SEDE CENACE	HP	2	3	3	4	2	1	3	4	32
A4	Servidores de Virtualización (HP BL620c GT CTO Blade)	Hardware	Servidores físicos donde reside la plataforma de virtualización del SIMEC	SEDE CENACE	HP	2	3	3	3	2	1	3	3	24
A5	Servidor de IHM (HP BL460c G7 CTO Blade)	Hardware	Servidor físico para la aplicación IHM Web del SIMEC, que permite a los operadores del sistema acceder a la aplicación cliente CENTAX de Producción a través del navegador de Internet	SEDE CENACE	HP	2	2	3	3	2	1	3	3	21
A6	Cabina de Discos - EVA P6350	Hardware	Almacenamiento físico para todos los servidores del SIMEC	SEDE CENACE	HP	2	3	3	4	2	1	4	4	32
A7	Enclousure - C7000 - SIMEC	Hardware	Chasis blade para el alojamiento de los servidores físicos del SIMEC	SEDE CENACE	HP	2	3	3	4	2	1	3	4	32
A8	Base de Datos SIMEC (Oracle 11g)	Software	Base de datos en la cual se soporta el funcionamiento del sistema SIMEC	SEDE CENACE	MB	3	3	3	4	3	1	4	4	36
A9	Red LAN (Switch de Data Center CISCO NEXUS 2000 – C2232PP)	Red	Componentes de networking para la red del SIMEC	SEDE CENACE	JV	3	2	3	4	2	1	4	4	32
A10	GPS - Arbiter Systems	Hardware	Dispositivo para la sincronización de los medidores/registradores	SEDE CENACE	JV	2	2	3	3	2	1	2	3	21

A11	Ingenieros de Sistemas	Personas	Ingenieros del área de sistemas encargados de la administración técnica y soporte del SIMEC	SEDE CENACE	HP, MB	1	2	2	1	3	2	2	3	15
A12	Datacenter del CENACE	Sitio	Centro de datos de CENACE donde residen los servidores y elementos de networking	SEDE CENACE	WM	3	3	3	4	2	1	4	4	36
A13	Información del SIMEC (base de datos)	Información	Información del SIMEC almacenada en la base de datos Oracle 11g	SEDE CENACE	MB	3	3	3	4	3	3	4	4	36
A14	Enlaces WAN entre CENACE y otras redes	Servicios	Servicio ofrecido por otros carriers para el acceso a los medidores/registradores que están fueran de la WAN de TRANSELECTRIC	VARIAS CIUDADES ECUADOR	JV	2	3	3	3	2	1	3	3	24
A15	Sistemas Operativos de Servidores: Windows 2008, Red Hat Linux, Vmware	Software	Sistemas operativos que se ejecutan los distintos servidores del SIMEC		HP	2	2	3	3	2	1	3	3	21
A16	Portal SIMEC	Software	Portal web en donde los Agentes de MEM gestionan la información de sus puntos de medidas.	SEDE CENACE	HP	2	3	3	4	3	3	4	4	32
A17	Capa media: Oracle Forms & Reports 11g Web Server, JBOSS Enterprise Application Server	Software	Servidor de forms, reports y servidor de aplicsciones del SIMEC	SEDE CENACE	HP	2	2	3	3	2	1	3	3	21
A18	Software CENTAX 2.1	Software	Software del sistema SIMEC	SEDE CENACE	ME, JA	3	3	3	4	3	3	4	4	36
A19	Ingenieros de Operaciones	Personas	Ingenieros encargados de la operación funcional del SIMEC	SEDE CENACE / INSTALACIONES EN CAMPO	ME, JA	2	3	3	1	3	2	2	3	24
A20	Estaciones de trabajo de los Ingenieros de Operaciones (Hardware)	Hardware	Estaciones de trabajo físicas donde trabajan los Ingenieros de Operaciones	SEDE CENACE	ME, JA	2	3	3	3	2	1	3	3	24
A21	Estaciones de trabajo de los Ingenieros de Operaciones (Sistema Operativo Windows 7)	Software	Sistema Operativo residente en las estaciones de trabajo de los Ingenieros de Operaciones	SEDE CENACE / INSTALACIONES EN CAMPO	HP	2	2	2	3	2	1	3	3	18

A22	Área de Operaciones del SIMEC en el CENACE	Sitio	Sitio físico donde laboran los Ingenieros de Operaciones del SIMEC	SEDE CENACE	WM	1	2	2	3	2	1	3	3	15
A23	Acceso a Internet	Servicios	Servicio de navegación corporativo	SEDE CENACE	JV	1	2	3	3	2	2	1	3	18
A24	Correo Electrónico	Servicios	Servicio de correo electrónico corporativo	SEDE CENACE	MCH	2	2	2	3	2	2	1	3	18
A25	Impresora de red HP	Hardware	Impresora de red para uso de la DSI	SEDE CENACE	HP	2	2	1	2	1	1	1	2	10
A26	Terminal Portátil de Lectura (TPL)	Software	Software para la adquisición en sitio de los registros de energía de los medidores/contadores.	AGENTES MEM	ME, JA	2	3	3	4	3	3	4	4	32
A27	Estaciones de trabajo de los Ingenieros de Sistemas (Windows 7 y herramientas ofimáticas)	Software	Sistema Operativo residente en las estaciones de trabajo de los Ingenieros de Sistemas	SEDE CENACE	HP	2	1	1	3	2	1	3	3	12
A28	Servicio Telefónico (fijo y celular)	Servicios	Interacción con los Agentes del MEM		JV	2	2	2	2	1	1	1	2	12
A29	Servidor de antivirus	Hardware	Antivirus McAfee	SEDE CENACE	MCH	3	2	3	3	2	1	2	3	24
A30	Servidor de Directorio Activo (HP BL460c G7 CTO Blade)	Hardware	Servicio de directorio activo corporativo	SEDE CENACE	MCH	2	2	3	3	2	1	2	3	21

Notas:

1. **CONF.** = Confidencialidad (C): Bajo(1), Medio(2) y Alta (3).
2. **INT.** = Integridad (I): Bajo(1), Medio(2) y Alta (3).
3. **DISP.** = Disponibilidad (D): Bajo(1), Medio(2) y Alta (3).
4. **CONSECUENCIA OPERACIONAL**: Insignificante(1), Menor(2), Moderado(3) y Mayor(4).
5. **CONSECUENCIA REPUTACIONAL**: Insignificante(1), Menor(2), Moderado(3) y Mayor(4).
6. **CONSECUENCIA ECONÓMICA**: Insignificante(1), Menor(2), Moderado(3) y Mayor(4).
7. **CONSECUENCIA REGULATORIA**: Insignificante(1), Menor(2), Moderado(3) y Mayor(4).
8. **CONSECUENCIA FINAL**, valor máximo de: Consecuencia Operacional, Consecuencia Reputacional, Consecuencia Económica y Consecuencia Regulatoria.
9. **VALOR DEL ACTIVO**, está dado por la siguiente formula: Valor del Activo = (C+I+D) x Consecuencia; donde: C=Confidencialidad, I= Integridad y D= Disponibilidad

Fuente: CENACE

C. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

La **Tabla 22** muestra la relación identificada entre los activos, amenazas y las vulnerabilidades correspondientes, cuyo resultado se resume en el campo *Valor del Factor de Exposición (FE)* que representa la probabilidad de ocurrencia que dichas amenazas exploten la vulnerabilidad en cuestión.

Tabla 22 Amenazas y Vulnerabilidades SIMEC

ACTIVOS		FACTOR DE EXPOSICIÓN			
		Análisis de Vulnerabilidades (V) y el conjunto de Amenazas (T) que podrían explotar la vulnerabilidad identificada*			
Código de Activo	Activo	Código de la Vulnerabilidad	Vulnerabilidad	Código de la amenaza	Valor del Factor de Exposición (FE)**
A1	Enlace WAN entre CENACE y CELEC EP - TRANSELECTRIC	V37	Adquisición, Mantenimiento y seguimiento al funcionamiento	T8, T10, T19, T42, T43,	3
A2	Firewall ASA 5520	V41	Uso, fortaleza, complejidad, calidad y gestión de contraseñas de acceso a elementos de red	T34, T48, T49, T50, T51, T58, T78,	2
A3	Servidores de Base de Datos (HP BL460c G7 CTO Blade)	V34	Otorgamiento y Cambio controlado de usuarios a equipos (PCs, Servidores) y medios	T22, T42, T45, T52, T70,	2
A4	Servidores de Virtualización (HP BL620c G7 CTO Blade)	V34	Otorgamiento y Cambio controlado de usuarios a equipos (PCs, Servidores) y medios	T22, T42, T45, T52, T70,	2
A5	Servidor de IHM (HP BL460c G7 CTO Blade)	V34	Otorgamiento y Cambio controlado de usuarios a equipos (PCs, Servidores) y medios	T22, T42, T45, T52, T70,	2
A6	Cabina de Discos - EVA P6350	V25	Almacenamiento, ubicación, fijación, exposición	T1, T2, T3, T4, T5, T6, T7, T8, T9, T14, T20, T21, T70,	2
A7	Enclousure - C7000 – SIMEC	V25	Almacenamiento, ubicación, fijación, exposición	T1, T2, T3, T4, T5, T6, T7, T8, T9, T14, T20, T21, T70,	2
A8	Base de Datos SIMEC (Oracle 11g)	V72	Encripción por parte del software (encripción de la aplicación o del motor de base de datos), gestión de las llaves de cifrado	T34, T51, T58, T59, T66, T67, T68, T70, T83, T86, T102	3
A9	Red LAN (Switch de Data Center CISCO NEXUS 2000 – C2232PP)	V55	Uso, fortaleza, complejidad, calidad y gestión de contraseñas de acceso a elementos de red	T34, T48, T49, T50, T51, T58, T78,	2
A10	GPS - Arbiter Systems	V42	Tiempo de sincronización	T25, T26, T27, T61,	1
A11	Ingenieros de Sistemas	V18	Personal capacitado, entrenado o con experiencia en los procedimientos operativos y herramientas de la organización	T22, T23, T24, T35, T40, T45	2
A12	Datacenter del CENACE	V10	Ubicación del sitio	T1-T5, T6-T9, T21, T71, T72	3
A13	Información del SIMEC (base de datos)	V50	Falta de cifrado en el canal (lo cual permite ver información sensible como contraseñas, datos de tarjetahabiente, información sensible), gestión de llaves de cifrado en los elementos de red	T34, T50, T54, T60, T62,	3
A14	Enlaces WAN entre CENACE y otras redes	V37	Adquisición, Mantenimiento y seguimiento al funcionamiento	T8, T10, T19, T42, T43,	2
A15	Sistemas Operativos de Servidores: Windows 2008, Red Hat Linux, Vmware	V34	Otorgamiento y Cambio controlado de usuarios a equipos (PCs, Servidores) y medios	T22, T42, T45, T52, T70,	3

A16	Portal SIMEC	V63	Control de Acceso (Restricciones en el acceso al software y mecanismos de autenticación), Políticas de Control de Acceso	**T22, T23, T24, T25, T28, T34, T36, T46, T48, T49, T50, T51, T52, T53, T58, T62, T64, T67, T69,**	**2**
A17	Capa media: Oracle Forms & Reports 11g Web Server, JBOSS Enterprise Application Server	V34	Otorgamiento y Cambio controlado de usuarios a equipos (PCs, Servidores) y medios	**T22, T42, T45, T52, T70,**	**2**
A18	Software CENTAX 2.1	V65	Cambios controlados, aprobados, autorizados, evaluados	**T11, T12, T28, T29, T34, T36, T37, T43, T49, T51, T57, T58, T62, T67, T68, T76, T77, T83, T87, T88, T89**	**2**
A19	Ingenieros de Operaciones	V18	Personal capacitado, entrenado o con experiencia en los procedimientos operativos y herramientas de la organización	**T22, T23, T24, T35, T40, T45**	**2**
A20	Estaciones de trabajo de los Ingenieros de Operaciones (Hardware)	V34	Otorgamiento y Cambio controlado de usuarios a equipos (PCs, Servidores) y medios	**T22, T42, T45, T52, T70,**	**2**
A21	Estaciones de trabajo de los Ingenieros de Operaciones (Sistema Operativo Windows 7)	V34	Otorgamiento y Cambio controlado de usuarios a equipos (PCs, Servidores) y medios	**T22, T42, T45, T52, T70,**	**2**
A22	Área de Operaciones del SIMEC en el CENACE	V25	Almacenamiento, ubicación, fijación, exposición	**T1, T2, T3, T4, T5, T6, T7, T8, T9, T14, T20, T21, T70,**	**2**
A23	Acceso a Internet	V56	Separación de las redes confiables de las no confiables (Control de conexión entre redes por intermedio de Firewalls de red). Conectividad del sistema de información (Sistema aislado, conectado a un conjunto reducido y controlado de redes, conectado a un amplio colectivo de redes conocidas, conectado a Internet)	**T32, T33, T34, T56, T57, T58, T62, T78, T80, T83, T85, T87, T97,**	**2**
A24	Correo Electrónico	V67	Uso y manipulación apropiada y controlada (Procedimientos y políticas de uso aceptable) de herramientas, utilerías, software, navegación en internet, etc.	**T22, T23, T24, T25, T26, T28, T29, T36, T46, T51, T52, T53, T64, T67,**	**2**
A25	Impresora de red HP	V46	Uso y manipulación apropiada y controlada (Procedimientos y políticas de uso aceptable)	**T22, T23, T45, T49, T52,**	**3**
A26	Terminal Portátil de Lectura (TPL)	V65	Cambios controlados, aprobados, autorizados, evaluados	**T11, T12, T28, T29, T34, T36, T37, T43, T49, T51, T57, T58, T62, T67, T68, T76, T77, T83, T87, T88, T89**	**2**
A27	Estaciones de trabajo de los Ingenieros de Sistemas (Windows 7 y herramientas ofimáticas)	V34	Otorgamiento y Cambio controlado de usuarios a equipos (PCs, Servidores) y medios	**T22, T42, T45, T52, T70,**	**2**
A28	Servicio Telefónico (fijo y celular)	V45	Conexión autorizada	**T27, T34, T54, T59, T62, T78,**	**2**
A29	Servidor de antivirus	V17	Concientización, capacitación, formación en seguridad de la información	**T21, T22, T24, T31, T35, T52, T53, T54, T66, T74, T75,**	**3**
A30	Servidor de Directorio Activo (HP BL460c G7 CTO Blade)	V34	Otorgamiento y Cambio controlado de usuarios a equipos (PCs, Servidores) y medios	**T22, T42, T45, T52, T70,**	**1**

* El catálogo de amenazas y vulnerabilidades se encuentra en el Anexo 3.

** Factor de Exposición (FE), especifica la probabilidad de ocurrencia que dichas amenazas exploten la vulnerabilidad en cuestión, los posibles valores son: Insignificante(1), Menor(2), Moderado(3) y Mayor(4)

Fuente: CENACE

D. CÁLCULO DEL RIESGO

Finalmente, el riesgo es calculado para cada uno de los activos del Sistema SIMEC, conforme se evidencia en la **Tabla 23:**

Tabla 23. Cálculo del Riesgo SIMEC

CÓDIGO DE ACTIVO	ACTIVO	VALOR DE ACTIVO (VA)	VALOR DEL FACTOR DE EXPOSICIÓN (FE)	CÁLCULO DEL RIESGO (R) R=(VA*FE)	NIVEL DEL RIESGO*
A1	Enlace WAN entre CENACE y CELEC EP - TRANSELECTRIC	36	2	72	Riesgo Alto
A2	Firewall ASA 5520	28	2	56	Riesgo Medio
A3	Servidores de Base de Datos (HP BL460c G7 CTO Blade)	32	2	64	Riesgo Medio
A4	Servidores de Virtualización (HP BL620c G7 CTO Blade)	24	2	48	Riesgo Medio
A5	Servidor de IHM (HP BL460c G7 CTO Blade)	21	2	42	Riesgo Medio
A6	Cabina de Discos - EVA P6350	32	2	64	Riesgo Medio
A7	Enclousure - C7000 - SIMEC	32	2	64	Riesgo Medio
A8	Base de Datos SIMEC (Oracle 11g)	36	3	108	Riesgo Alto
A9	Red LAN (Switch de Data Center CISCO NEXUS 2000 – C2232PP)	32	2	64	Riesgo Medio
A10	GPS - Arbiter Systems	21	1	21	Riesgo Bajo
A11	Ingenieros de Sistemas	15	2	30	Riesgo Bajo
A12	Datacenter del CENACE	36	2	72	Riesgo Alto
A13	Información del SIMEC (base de datos)	36	3	108	Riesgo Alto
A14	Enlaces WAN entre CENACE y otras redes	24	2	48	Riesgo Medio
A15	Sistemas Operativos de Servidores: Windows 2008, Red Hat Linux, Vmware	21	3	63	Riesgo Medio
A16	Portal SIMEC	32	2	64	Riesgo Medio
A17	Capa media: Oracle Forms & Reports 11g Web Server, JBOSS Enterprise Application Server	21	2	42	Riesgo Medio
A18	Software CENTAX 2.1	36	3	108	Riesgo Alto
A19	Ingenieros de Operaciones	24	2	48	Riesgo Medio
A20	Estaciones de trabajo de los Ingenieros de Operaciones (Hardware)	24	2	48	Riesgo Medio
A21	Estaciones de trabajo de los Ingenieros de Operaciones (Sistema Operativo Windows 7)	18	2	36	Riesgo Medio
A22	Área de Operaciones del SIMEC en el CENACE	15	2	30	Riesgo Bajo
A23	Acceso a Internet	18	2	36	Riesgo Medio
A24	Correo Electrónico	18	2	36	Riesgo Medio
A25	Impresora de red HP	10	3	30	Riesgo Bajo
A26	Terminal Portátil de Lectura (TPL)	32	2	64	Riesgo Medio
A27	Estaciones de trabajo de los Ingenieros de Sistemas (Windows 7 y herramientas ofimáticas)	12	2	24	Riesgo Bajo
A28	Servicio Telefónico (fijo y celular)	12	2	24	Riesgo Bajo
A29	Servidor de antivirus	24	3	72	Riesgo Alto
A30	Servidor de Directorio Activo (HP BL460c G7 CTO Blade)	21	1	21	Riesgo Bajo

* La matriz de riesgos aplicada en el análisis se encuentra documentada en el Anexo 3.

Fuente: CENACE

Proceso: F2.g Medidas Preventivas

Actividades: El plan de medidas preventivas fue diseñado por el equipo de recuperación de desastres bajo la dirección del Coordinador del Área Informática, para posteriormente poner el citado plan a consideración del Director de Sistemas de Información.

La mayor parte de las actividades preventivas identificadas presuponen únicamente, la inversión de horas de soporte para la infraestructura de base del SIMEC por parte de la empresa encargada.

Tiempo empleado: 8 horas.

Entregable:

E07	PLAN DE MEDIDAS PREVENTIVAS DE RECUPERACIÓN DE DESASTRES PARA EL SISTEMA SIMEC

A. GENERALIDADES

Una vez obtenidos los resultados del BIA y el análisis de riesgos aplicados al Sistema SIMEC, es factible la identificación y aplicación de medidas preventivas que permitan reducir la probabilidad de interrupciones en el normal funcionamiento del SIMEC y minimizar el impacto que puede provocar en el CENACE la no-disponibilidad del citado sistema.

B. PLAN DE ACCIÓN

Según el análisis de riesgos se tiene:

Tabla 24. Activos y Niveles de Riesgos en Medidas Preventivas

CÓDIGO DE ACTIVO	ACTIVO	NIVEL DEL RIESGO
A3	Servidores de Base de Datos (HP BL460c G7 CTO Blade)	Riesgo Medio
A4	Servidores de Virtualización (HP BL620c G7 CTO Blade)	Riesgo Medio
A5	Servidor de IHM (HP BL460c G7 CTO Blade)	Riesgo Medio

A6	Cabina de Discos - EVA P6350	Riesgo Medio
A7	Enclousure - C7000 - SIMEC	Riesgo Medio
A12	Datacenter del CENACE	Riesgo Alto
A15	Sistemas Operativos de Servidores: Windows 2008, Red Hat Linux, Vmware	Riesgo Medio
A16	Portal SIMEC	Riesgo Medio
A29	Servidor de antivirus	Riesgo Alto

Fuente: CENACE

El plan de acción contempla las siguientes actividades:

Tabla 25. Medidas Preventivas SIMEC

ÍTEM	ACTIVIDAD	CÓDIGO ACTIVO	TRATAMIENTO RIESGO	RESPONSABLE	PLAZO
1	Actualización del firmware de servidores, almacenamiento y chasis blade del SIMEC.	A3, A4, A5, A6 y A7	Modificar el nivel de riesgo a "Bajo"	HP	1 mes
2	Mejorar la condiciones de temperatura y humedad del Datacenter CENACE, mediante la incorporación de dos unidades adicionales de aire acondicionado	A12	Modificar el nivel de riesgo a "Medio"	WM	4 meses
3	Actualizar e instalar los parches a nivel de sistema operativo Windows y Red Hat Linux de los servidores del SIMEC	A15	Modificar el nivel de riesgo a "Bajo"	MCH	1 mes
4	Establecer un enlace de comunicaciones redundante con un proveedor distinto para la publicación de los Portales Web del SIMEC.	A16	Modificar el nivel de riesgo a "Bajo"	JV	1 mes
5	Instalación de un software antivirus en todos los servidores del SIMEC que tienen el sistema operativo Microsoft.	A29	Modificar el nivel de riesgo a "Bajo"	MCH	1 mes

Fuente: CENACE

Proceso: F2.h Estrategia de Recuperación

Actividades: Para la definición de la estrategia de recuperación de desastres del SIMEC, se consideró el siguiente procedimiento:

- Identificación de los activos con nivel del riesgo de tipo "alto/crítico"; determinación del RTO y RPO objetivos del SIMEC.
- Revisión de la arquitectura actual del SIMEC, considerando los métodos de recuperación como: clusters, RAID´s, infraestructura redundante y respaldos de información.
- Visualización de la situación objetivo para el SIMEC, en base a sus requerimientos operativos y de la disponibilidad de sus servicios de información.

En el análisis previo participaron el equipo de recuperación de desastres y el Director de Sistemas de Información.

Tiempo empleado: 48 horas.

Entregable:

E08	DEFINICIÓN DE LA ESTRATEGIA DE RECUPERACIÓN DE DESASTRES PARA EL SISTEMA SIMEC

A. GENERALIDADES

En base a la aplicación del BIA y el análisis de riesgos aplicados al sistema SIMEC, se tienen los siguientes resultados:

- BIA -> RTO: 24 horas; RPO: 24 horas.
- Análisis de Riesgos -> Activos de mayor nivel de riesgo:

Tabla 26. Activos y Niveles de Riesgos en Estrategia de Recuperación

CÓDIGO DE ACTIVO	ACTIVO	NIVEL DEL RIESGO
A1	Enlace WAN entre CENACE y CELEC EP - TRANSELECTRIC	Riesgo Alto
A8	Base de Datos SIMEC (Oracle 11g)	Riesgo Alto
A12	Datacenter del CENACE	Riesgo Alto
A13	Información del SIMEC (base de datos)	Riesgo Alto
A18	Software CENTAX 2.1	Riesgo Alto

Fuente: CENACE

La mejor estrategia de recuperación será aquella que cumpla los tiempos estipulados de RTO y RPO; y, minimice el nivel de riesgo identificado para los principales activos del SIMEC.

B. SITUACIÓN ACTUAL

Al momento el Sistema SIMEC cuenta con los siguientes métodos de recuperación 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 **Figura 12** se muestra la arquitectura física y virtual del SIMEC.

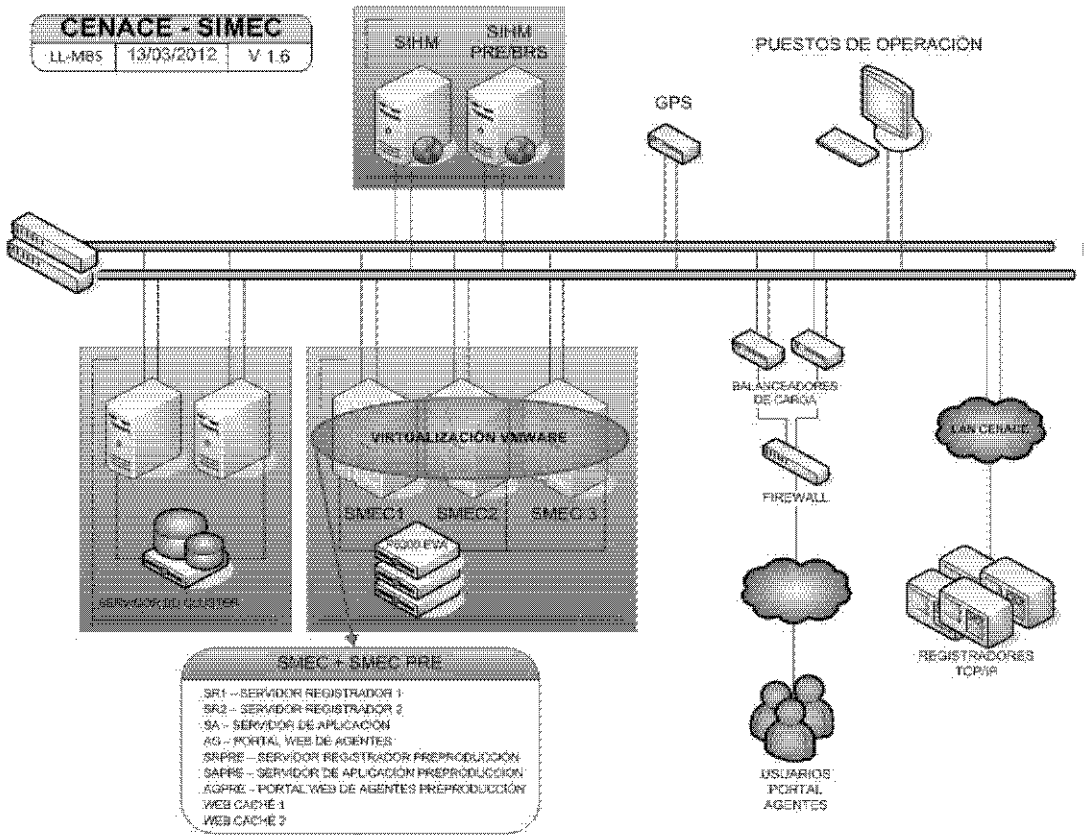


Figura 12. Arquitectura Física y Virtual SIMEC
Fuente: CENACE

- Almacenamiento de Datos, el SIMEC guarda toda su información en una solución de almacenamiento de la gama corporativa de Hewlett Packard P6350 EVA, posibilitando la creación de arreglos de discos virtuales que manejan redundancia del tipo 0, 1, 5 y 6.

- Respaldo y restauración, para el efecto el sistema SIMEC forma parte de la Solución de Respaldo Corporativo del CENACE que cuenta con una infraestructura de hardware y software para crear tareas automatizadas para la obtención backups de bases de datos, sistemas de archivos y configuraciones adicionales a través de una red de SAN (Storage Area Network). Los principales componentes de hardware son: un robot de cintas (HP MSL 6030), sistema de respaldos a discos D2D[17] y switch´s de fibra como se observa en la **Figura 13.**

[17] Disk-to-disk, sistema de respaldo de información a disco que permite optimizar el tiempo de procesamiento para la obtención de respaldo y la restauración de información.

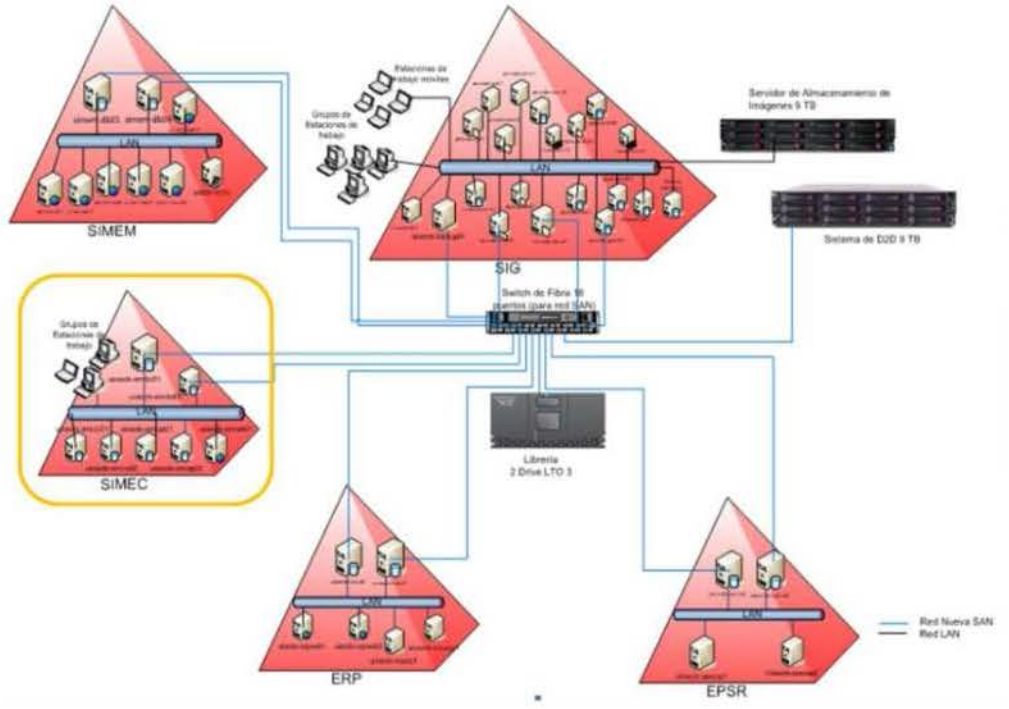


Figura 13. Solución de Respaldo Corporativo del CENACE
Fuente: CENACE

El proceso para la obtención de los backups del SIMEC se ejecuta de manera diaria bajo dos modalidades, full e incremental, la **Figura 14** ilustra dicho esquema.

TIPO DE RESPALDO	FRECUENCIA	FECHA DE OBTENCIÓN	RETENCIÓN EN D2D	RETENCIÓN EN CINTA	OBSERVACIONES
INCREMENTAL/ DIFERENCIAL	DIARIO	DOMINGO A VIERNES	1 semana	-	
FULL	SEMANAL	SABADO	2 semanas	-	
FULL (copia a cinta física)	QUINCENAL		-	13 semanas	Se enviará el juego de cintas del mes previo al WTC
FULL(copia a cinta física)	ANUAL	Primera semana del mes de enero del año en curso	-	3 años	Se enviará el juego de cintas al WTC

Figura 14. Esquema de Retención de Información D2D y Cintas Físicas
Fuente: CENACE

- 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.

C. SITUACIÓN OBJETIVO

En una primera fase, la definición de la estrategia de recuperación para el SIMEC ha considerado prioritariamente los siguientes activos: A8, A13 y A18 que se encuentran identificados en la **Tabla 26** con el nivel de riesgo "Alto". Desde el punto de vista del tratamiento del riesgo, el objetivo perseguido es modificar su nivel a la calificación "Medio". Los activos A1 y A12 serán tratados en una segunda fase de evaluación, por presentar valores menores en el factor de exposición.

Los métodos de recuperación del SIMEC identificados en la sección B, como son: implementación de cluster´s, arreglos de discos virtuales, respaldo y restauración de información, han permitido al SIMEC cumplir adecuadamente con los niveles de operación y disponibilidad, que permiten la obtención, procesamiento y entrega de la información de los registros de energía para los procesos de liquidación y facturación, conforme los índices de gestión establecidos.

En base a lo expuesto previamente, el Director de Sistemas de Información y el equipo de recuperación de desastres acuerdan ratificar la estrategia de recuperación de desastres con la que actualmente cuenta el SIMEC, considerando adicionalmente, que los métodos de recuperación están alineados con los valores de RTO y RPO previamente identificados en el análisis BIA.

Proceso: F2.i Implementación de Procedimientos de Recuperación

Actividades: La elaboración del plan de recuperación de desastres constituyó una de las actividades más importantes y demandantes para el equipo de recuperación de desastres bajo la dirección del Coordinador del Área Informática, su desarrollo se basó en los siguientes lineamientos:

- Definición de objetivos y alcance del DRP.
- Organización de equipos de trabajo y responsabilidades.
- Establecimiento del árbol de llamadas, contactos internos de CENACE y proveedores externos.
- Identificación de los procedimientos de respaldos de información aplicados al SIMEC.
- Desarrollo de una propuesta del proceso de para la declaración y activación del DRP para el SIMEC.
- Elaboración de los procedimientos de recuperación del SIMEC.

El plan de recuperación de desastres obtenido para el SIMEC se encuentra en la etapa de revisión por parte del Director de Sistemas de Información.

Tiempo empleado: 48 horas.

Entregable:

E09	PLAN DE RECUPERACIÓN DE DESASTRES PARA EL SISTEMA SIMEC

A. INTRODUCCIÓN

El presente documento describe el Plan de Recuperación de Desastres (DRP) que está orientado a mantener en un único repositorio la información necesaria, a fin de que la Corporación CENACE pueda enfrentar un evento de desastre en sus instalaciones, dado que no dispone de un sitio alterno.

1. Objetivo

El DRP del CENACE para el Sistema SIMEC, tiene por objetivo delinear los pasos principales que se deben realizar durante una interrupción del sistema, para retornar a sus operaciones normales tan pronto como sea posible.

2. Alcance

El DRP del CENACE toma en consideración las siguientes componentes del SIMEC:

- Infraestructura de Servidores y Almacenamiento
- Base de Datos
- Servidores de Capa Media
- Software Centax y aplicaciones complementarias
- Sistema de backup
- Consolas de Operación

El presente documento no considera componentes que no son de TI, personal y los relacionados con la infraestructura física del edificio de la Corporación.

3. Control de Cambios

El siguiente cuadro muestra el control de cambios del documento:

Tabla 27. Control de Cambios Documento DRP

REVISIÓN	FECHA	AUTOR	CAMBIOS
1.0	15-01-2014	Marco Bautista	Versión inicial del DRP - SIMEC

Fuente: CENACE

B. EQUIPOS Y RESPONSABILIDADES

En el caso de un evento de desastre, los siguientes equipos de trabajo se requerirán para asistir al Área de Informática de la Dirección de Sistemas de Información, en sus esfuerzos para retornar a la funcionalidad normal del SIMEC. Los equipos de trabajo son:

1. **Equipo de respuesta a incidentes**

Rol y Responsabilidades:

- Analizar y acotar el impacto de una incidencia.
- Reportar las incidencias graves al equipo de manejo de emergencia.

Datos de contacto:

Tabla 28. Datos de Contacto Equipo de Respuesta a Incidentes

NOMBRE	ROL/CARGO	TELÉFONO OFICINA	TELÉFONO DOMICILIO	TELÉFONO MÓVIL
Ing. Hugo Paredes	Administrador de Aplicaciones e Infraestructura	2992062	22456245	0996035125
Ing. Jorge Aguilar	Especialista Medición Comercial	2992055	22678245	0996035125
Ing. Wilson Marcayata	Administrador Sistemas Auxiliares	2992045	22848865	0996035125

Fuente: CENACE

2. **Equipo de manejo de emergencia**

Rol y Responsabilidades:

- Determinar la magnitud y la clase del evento de desastre.
- Ser el único punto de contacto y supervisar todos los equipos de recuperación de desastres.
- Determinar los sistemas y procesos que han sido afectados por el desastre.
- Determinar los pasos iniciales necesarios a ser realizados por los equipos de recuperación de desastres.
- Observar que todas las decisiones adoptadas respeten el DRP y sus políticas establecidas por la Corporación CENACE.
- Crear un informe detallado de todas las medidas adoptadas en el proceso de recuperación de desastres.
- Notificar a las partes interesadas una vez que el desastre fue superado y la funcionalidad del SIMEC normalizada.

Datos de contacto:

Tabla 29. Datos de Contacto Equipo de Manejo de Emergencia

NOMBRE	ROL/CARGO	TELÉFONO OFICINA	TELÉFONO DOMICILIO	TELÉFONO MÓVIL
Ing. Gonzalo Uquillas	CIO / DRP Líder	2992048	22456550	0996035126
Ing. Andrés Narváez	Coordinador STR	2992052	23674243	0996035125
Ing. Marco Bautista	Coordinador AINF	2992060	23450045	0996035127

Fuente: CENACE

3. Equipo de software y aplicaciones

Rol y Responsabilidades:

- Determinar las aplicaciones que no funcionan adecuadamente.
- Si múltiples aplicaciones están afectadas, el equipo determinará la prioridad de recuperación en la forma y orden que generen el menor impacto.
- Aplicar el procedimiento de recuperación de sistema operativo, componentes de virtualización y software de aplicación.
- Aplicar el procedimiento de restauración de la base de datos utilizando sus respectivos backups.

Datos de contacto:

Tabla 30. Datos de Contacto Equipo de Software y Aplicaciones

NOMBRE	ROL/CARGO	TELÉFONO OFICINA	TELÉFONO DOMICILIO	TELÉFONO MÓVIL
Ing. Anita Álvarez	Administrador Base de Datos	2992060	23458755	0999719468

Fuente: CENACE

4. Equipo de recuperación de redes

Rol y Responsabilidades:

- Evaluar los daños específicos de cualquier infraestructura de red y proveer la conectividad de voz y datos incluyendo las conexiones de LAN y WAN.

- Priorizar la recuperación de los servicios de red en la forma y orden que generen el menor impacto.
- En el caso que los servicios de red sean provistos por un proveedor externo, el equipo coordinará las acciones con el proveedor para la recuperación de estos servicios.

Datos de contacto:

Tabla 31. Datos de Contacto Equipo de Recuperación de Redes

NOMBRE	ROL/CARGO	TELÉFONO OFICINA	TELÉFONO DOMICILIO	TELÉFONO MÓVIL
Ing. Juan Vallecilla	Administrador de Redes	2992050	22456244	0996035130

Fuente: CENACE

C. ÁRBOL DE LLAMADAS

En un evento de recuperación de desastres, el CENACE hará uso del esquema de notificación indicado en el **Figura 15** para asegurar que los Funcionarios de la Dirección de Información sean contactados en el momento requerido.

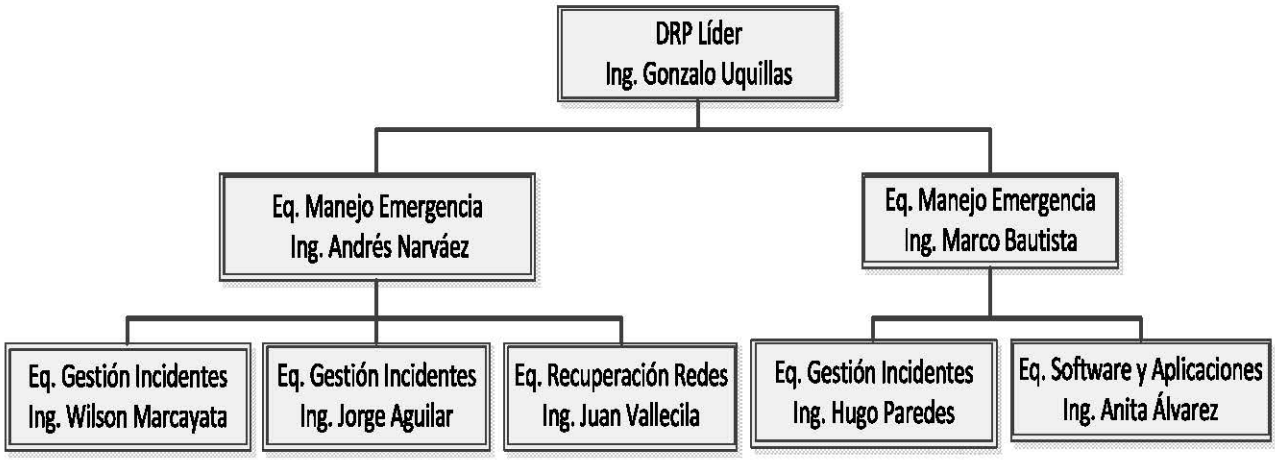


Figura 15. Árbol de Llamadas DSI
Fuente: CENACE

Información de Proveedores Externos:

Tabla 32. Datos de Contacto Proveedores Externos

PROVEEDOR	DATOS DE CONTACTO	
NUCLEO DF	Servicio	Soporte SIMEC
	Nombre Administrador	Ing. Roberto García
	No. Contrato	13001103
	Teléfono Soporte	00 34 91 807 39 01
	Teléfono Oficina	00 34 91 803 18 10
	Teléfono Movil	00 34 617 328 483
	e-mail	roberto.garcia@nucleodf.com.es
REFUNDATION	Servicio	Soporte Bases de Datos, Plataforma Virtual y Sistemas Operativos Linux
	Nombre Administrador	Ing. Paola Pullas
	No. Contrato	13000120
	Teléfono Soporte	26037651
	Teléfono Oficina	26037652
	Teléfono Móvil	0986947240
	e-mail	paola.pullas@refundation.com
MAINT	Nombre Administrador	Ing. Edison Pardo
	No. Contrato	13000018
	Teléfono Soporte	22447929
	Teléfono Oficina	22442710
	Teléfono Móvil	0984911076
	e-mail	epardo@maint.com.ec
Soporte HP	Teléfono Soporte	1999119 18007112884
	No. Carepack	2054366626
Soporte ORACLE	No. Contrato	5514438
	Acceso metalink	https://support.oracle.com/
Servicio de Taxi	Servicio	Transporte
	Nombre Contacto	Sr. Luis Velastegui
	Teléfono Móvil	0998880679

Fuente: CENACE

D. DATOS Y BACKUPS

La gestión de los backups del Sistema SIMEC se lo realiza en función de lo estipulado en el instructivo IT-DSI-AINF-15 Respaldo de información de la plataforma de servidores mediante la utilización de la Solución Corporativa de Almacenamiento y Respaldo de Información del CENACE. En la siguiente tabla se muestra el detalle de la información respaldada, frecuencia y tipo.

Tabla 33. Esquema Backups SIMEC

SISTEMA	SERVIDORES	TIPO	INFORMACIÓN A RESPALDAR	FRECUENCIA	TIPO DE RESPALDO
SIMEC	uiosede-smcbd01	CLUSTER WINDOWS CON ORACLE	UIOSEDE-SMCBD01\D$\CENTAX	MENSUAL	FULL
			UIOSEDE-SMCBD01\D$\ORACLE		
			System State		
	uiosede-smcbd02	CLUSTER WINDOWS CON ORACLE	UIOSEDE-SMCBD02\D$\CENTAX	MENSUAL	FULL
			UIOSEDE-SMCBD02\D$\ORACLE		
			System State		

	uiosede-smcbdcl	MAQUINA VIRTUAL DEL CLUSTER	UIOSEDE-SMCBDCL\Q$	Diario	FULL+INCREMENTAL
	uiosede-smcbd		CENTAX (Base de datos)		
	uiosede-smcco01	CLUSTER WINDOWS	UIOSEDE-SMCCO01\D\CENTAX	MENSUAL	FULL
			UIOSEDE-SMCCO01\D\ORACLE		
			System State		
	uiosede-smcco02	CLUSTER WINDOWS	UIOSEDE-SMCCO02\D\CENTAX	MENSUAL	FULL
			UIOSEDE-SMCCO02\D\ORACLE		
			System State		
	uiosede-smccocl	MAQUINA VIRTUAL DEL CLUSTER	Z:\Compartido	MENSUAL	FULL
			Q:\		
	uiosede-smcap01	CLUSTER WINDOWS	D:\CENTAX	MENSUAL	FULL
			D:\JBOSS-4.0.5.GA		
			D:\JBOSS-EAP-4.3		
			D:\ENTERPRISEPLATAFFORM-4.2.0.GA_CP02		
			D:\SAM		
			System State		
	uiosede-smcap02	CLUSTER WINDOWS	D:\CENTAX	MENSUAL	FULL
			D:\JBOSS-4.0.5.GA		
			D:\JBOSS-EAP-4.3		
			D:\ENTERPRISEPLATAFFORM-4.2.0.GA_CP02		
			D:\SAM		
			System State		
	uiosede-smcapcl	MAQUINA VIRTUAL DEL CLUSTER	Q:\	MENSUAL	FULL
	uiosede-smcapas		Z:\Oracle		
	uiosede-smcapfs		Y:\COMPARTIDO		
	uiosede-smcwb01	WEB SERVER WINDOWS IIS	D:\	MENSUAL	FULL
			System State		

Fuente: CENACE

E. GESTIÓN PARA LA RECUPERACIÓN DE DESASTRES

Ante la ocurrencia de un evento de desastre en la Corporación CENACE, la prioridad será asegurar que todos los funcionarios se encuentren sanos y salvos, para lo cual es necesario observar el Plan de Emergencia y Contingencia del CENACE.

Independientemente del tipo de desastre, el tratamiento del mismo se divide en los siguientes pasos:

1. Declaración del desastre

El CENACE iniciará su preparación en base a las fuentes primarias de información de los siguientes medios:

- Reportes de primera mano de parte del Equipo de respuesta a incidentes.

- Sistema de alarmas y monitoreo
- Personal de seguridad
- Usuarios finales
- Proveedores

Los criterios bajo los cuales el DRP Líder procederá con la activación del DRP son:

- Corrupción de la base de datos del SIMEC.
- Daño grave en los componentes de hardware (servidores/almacenamiento).

Una vez que el DRP Líder ha determinado que ha ocurrido un evento disruptivo, él convocará al Comité de Ejecutivo para determinar la factibilidad de la activación del DRP. En caso de la activación, el DRP Líder dará instrucciones al Equipo de manejo de emergencia para iniciar el contacto con las autoridades y todos los equipos de recuperación de desastres.

2. Activación del DRP

Luego que el DRP Líder ha declarado formalmente que un desastre se ha producido, inmediatamente iniciará con la activación del DRP a través de la ejecución del árbol de llamadas de recuperación de desastres. Una vez que los equipos de recuperación de desastres (Ref. Sección B) han sido notificados, su accionar estará orientado conforme al siguiente esquema indicado en la **Figura 16**.

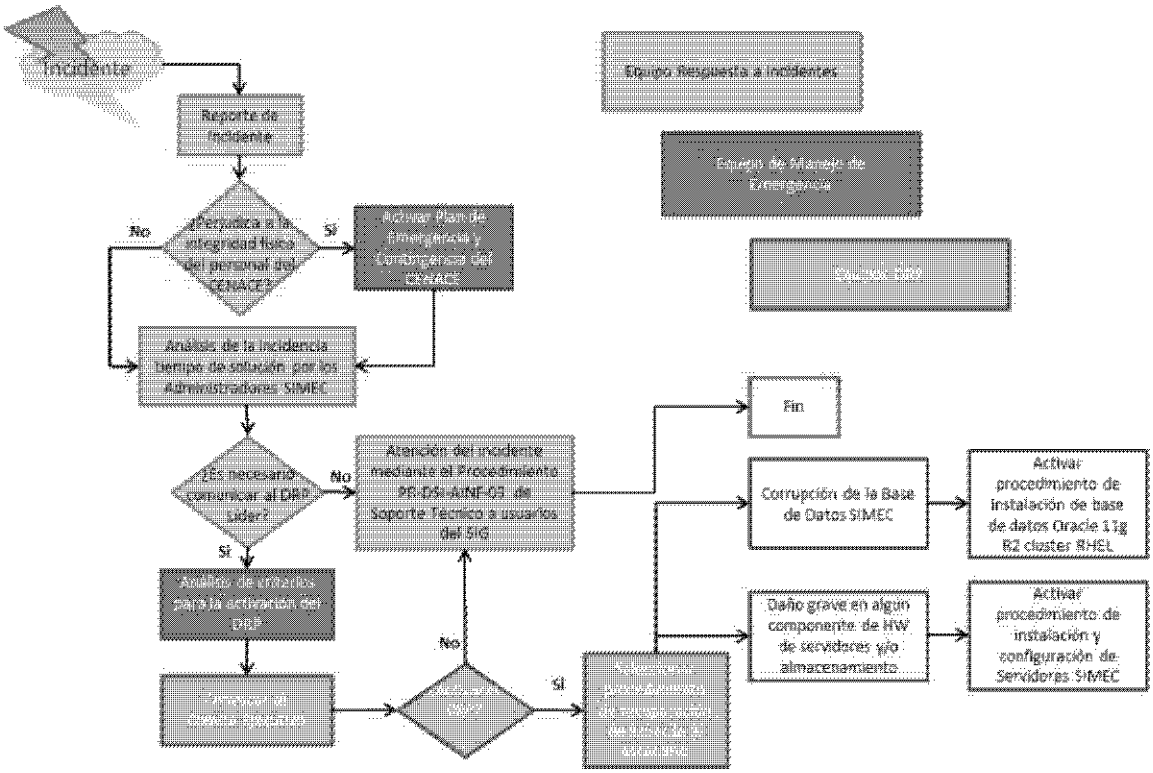


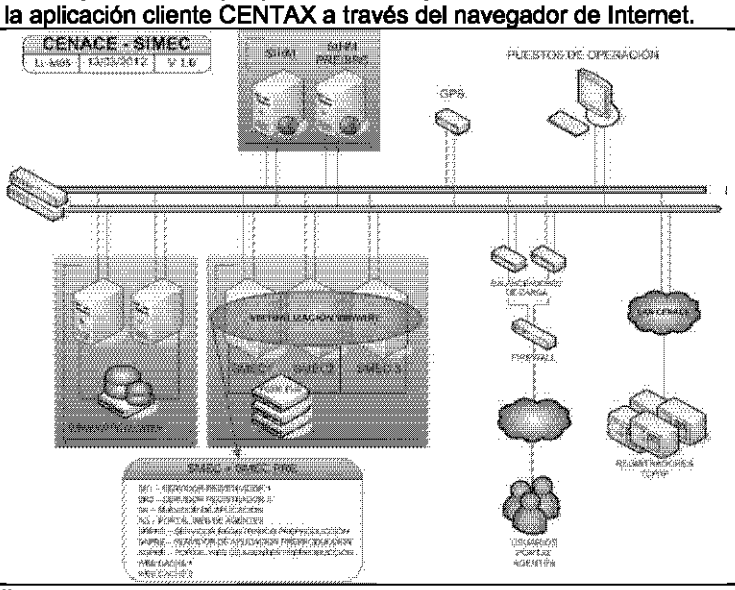
Figura 16. Secuencia de Actividades Ante la Ocurrencia de un Evento Disruptivo
Fuente: CENACE

3. Procedimientos de Recuperación

Esta sección contiene la información necesaria para retornar a la operación normal los servicios y sistemas de información del CENACE, para el caso particular del Sistema de Medición Comercial SIMEC, se han identificado los siguientes componentes y escenarios para su recuperación:

Tabla 34. Procedimientos de Recuperación SIMEC

Sistema	**Sistema de Medición Comercial – SIMEC**
Descripción	Gestionar la medición de los registros cuarto-horarios de energía y otros parámetros eléctricos, en los puntos de generación/entrega del SNI.
Nombre del Proveedor	NUCLEO df Duro Felguera
Versión	SIMEC – CENTAX versión 2.0
RTO	24 horas
RPO	24 horas

Componentes / Especificaciones	• **Servidores de BBDD:** cluster compuesto por dos servidores físicos (SBD1 y SBD2) con sistema operativo Red Hat Enterprise Linux 6 64 bits y una cabina de discos EVA P6350 HP compartida, donde reside la base de datos Oracle. • **Servidor SIMEC/SA:** servidor virtual donde se ejecutan las aplicaciones propias del sistema (instaladores, inventario SIMEM, mantenimiento histórico SIMEM, recuperación de medidas del STR, autómata cálculos, informesWeb). • **Servidores SIMEC/SR:** dos servidores virtuales SR-1 y SR-2 para la aplicación Servidor de Registradores. • **Servidores SIMEC/AG:** dos servidores con sistema operativo MS Windows 2008 Standard Edition de 64 bits para la aplicación Web del Portal SIMEC para los agentes MEM. • **Servidores SIMEC/Web Cache:** dos servidores Web con sistema operativo MS Windows 2008 R2 Server Edition 64 bits, donde residen los servidores Web (Apache http Server) que redireccionan las conexiones de los agentes a través de Internet a los servidores de aplicaciones del Portal de Agentes SIMEC. • **Servidor SIMEC/SIHM:** servidor físico para la aplicación IHM Web del CS de producción, que permite a los operadores del sistema acceder a la aplicación cliente CENTAX a través del navegador de Internet.
Arquitectura	
Sitio Alterno	No dispone
Estrategia de Backup	Refiérase a la Sección D. Datos y Backups
Procedimientos*	**Escenario 1:** Daño grave en los componentes de hardware (servidores/almacenamiento). Refiérase al documento "Procedimiento de Instalación y Configuración de Servidores SIMEC".
	Escenario 2: Mal funcionamiento de sistema operativos de servidores. Refiérase al documento "Procedimiento de Instalación y Configuración de Sistemas Operativos SIMEC".
	Escenario 3: Corrupción de la base de datos del SIMEC. Refiérase al documento "Procedimiento de Instalación Bases de Datos Oracle 11g R2 Cluster RHEL".
	Escenario 4: Pérdida de los servidores de aplicaciones, registradores, IHM, portal Agentes. Refiérase al documento "Procedimiento de Instalación y Configuración del Sistema SIMEC".
	Escenario 5: Pérdida de servidor de aplicaciones WebCache. Refiérase al documento "Procedimiento de Instalación WebCache".

***** La documentación de los procedimientos fue revisada, se encuentra actualizada y es utilizada por los equipos de trabajo del DRP.

Fuente: CENACE

Proceso: F2.j Capacitación y Pruebas

Actividades: El proceso de capacitación del DRP para el SIMEC fue planificado por el Coordinador del Área Informática considerando la impartición de dos talleres, Visión General y Funcionamiento del DRP; y, Revisión de los Procedimientos de Recuperación SIMEC.

El taller Revisión de los Procedimientos de Recuperación SIMEC, fue impartido por el Coordinador del Área Informática a los Ingenieros de infraestructura, bases de datos y networking del equipo de recuperación de desastres. Mientras que el segundo taller, dirigido a los Ingenieros de la DSI se encuentra pendiente de su ejecución para una fecha posterior.

Tiempo empleado: 10 horas.

Entregable:

E10 PLAN DE CAPACITACIÓN DEL DRP PARA EL SISTEMA SIMEC

A. PROPÓSITO

El objetivo del presente documento es describir el Plan de Capacitación establecido por la Dirección de Sistemas de Información para el DRP del SIMEC.

Básicamente el citado plan consiste en un listado con cada uno de los cursos a impartirse, el número de días previsto, las fechas programadas, el lugar del evento, los objetivos a cubrir y el número de asistentes esperado.

B. DESCRIPCIÓN DE LOS TALLERES DE CAPACITACIÓN

1. Visión General y Funcionamiento del DRP para el sistema SIMEC

- Objetivo del curso: Presentación divulgativa sobre el marco de referencia para la Planificación de Recuperación de Desastres. Es un curso eminentemente teórico.

- Temario:
  - ✓ Sensibilización, qué es un: incidente, desastre, tipos, causas, impactos, importancia de contar con un DRP?.
  - ✓ Objetivos y alcance del DRP – SIMEC
  - ✓ Conformación de grupos de recuperación
  - ✓ Funciones y responsabilidades
  - ✓ Estrategias de recuperación
  - ✓ Declaración del Desastre
  - ✓ Actividades de Recuperación
  - ✓ Activación del Plan de recuperación
  - ✓ Pruebas y Mantenimiento del DRP

- Número de asistentes esperado: 6
- Prerrequisitos de los asistentes: Conocimientos básicos en seguridad de la información y análisis de riesgos.
- Material: Diapositivas powerpoint
- Duración: 4 horas.
- Dirigido a: Ingenieros de la Dirección de Sistemas de Información.
- Lugar: Auditorio Corporación CENACE

2. Revisión de los Procedimientos de Recuperación aplicados al SIMEC

- Objetivo del curso: Conocimiento y aplicación de los procedimientos para el restablecimiento de servidores y base de datos del SIMEC. Componente práctica del curso 80%.
- Temario:
  - ✓ Revisión del proceso de recuperación de desastres.
  - ✓ Asignación de responsabilidades
  - ✓ Ejecución de procedimientos para recuperación de servidores y bases de datos.
- Número de asistentes esperado: 3

- Prerrequisitos de los asistentes: Conocimientos de hardware, sistemas operativos, bases de datos.
- Material: Diapositivas powerpoint
- Duración: 6 horas.
- Dirigido a: Ingenieros de Infraestructura y Administradores de Bases de Datos.
- Lugar: Laboratorio de DSI - Corporación CENACE

Proceso: F2.j Capacitación y Pruebas

Actividades: El proceso de pruebas del DRP para el SIMEC, fue planificado por el equipo de recuperación de desastres y ejecutado por el equipo de software y aplicaciones con el soporte especializado de ORACLE en sitio. Las pruebas se llevaron a cabo en el entorno de producción del SIMEC bajo condiciones controladas.

La ejecución del plan de pruebas propuesto fue autorizada por el Director de Sistemas de Información.

Tiempo empleado: 8 horas.

Entregable:

E11 PLAN DE PRUEBAS DEL DRP PARA EL SISTEMA SIMEC

A. PROPÓSITO

Validar que los procedimientos establecidos para la recuperación de la base de datos del SIMEC sean eficaces, a fin de que los equipos de recuperación puedan restablecer los servicios de información del SIMEC dentro de los períodos de tiempos acordados.

B. ALCANCE DE LA PRUEBA

Las pruebas de funcionamiento de la base de datos del SIMEC se realizarán utilizando los servidores indicados en la siguiente tabla, mismos que se encuentran en el ambiente de producción y forman parte del dominio llamado CENACE.CORP.

Tabla 35. Servidores de Base de Datos SIMEC

NOMBRE	DESCRIPCIÓN DE ROLES	IP
QCSIMECFXBD1	Servidor de base de datos activo	10.2.3.14
QCSIMECFXBD2	Servidor de base de datos pasivo	10.2.3.15

Fuente: CENACE

C. ESTRATEGIA DE LA PRUEBA

Las pruebas serán desarrolladas por el equipo de software y aplicaciones del SIMEC, bajo la coordinación del equipo de manejo de emergencia, en las instalaciones de la sede principal de la Corporación CENACE.

Para el desarrollo de las pruebas, se crearán los escenarios necesarios en el entorno de producción del SIMEC, bajo condiciones controladas que no afecten su integridad y posterior operación.

A continuación se listan los casos de prueba con su respectiva secuencia:

Tabla 36. Casos de Prueba SIMEC

CÓDIGO PRUEBA	DESCRIPCIÓN
TS_PE_DB.0001. Configuración en mirror del Sistema Operativo	**Prueba a realizar:** El sistema estará configurado para soportar la posible pérdida de un disco duro, sin que conlleve la no-disponibilidad de sus servicios. Para ello se realizará las siguientes actividades: • Apagar el servidor • Extraer un disco duro • Iniciar el servidor y comprobar su correcto funcionamiento. • Introducir el disco que fue extraído luego de transcurridos aproximadamente 5 minutos. • Verificar la replicación de datos en el disco extraído. **Resultado esperado:** El sistema realiza la correcta replicación de los datos perdidos al reponer el disco duro defectuoso. **Resultado de la prueba:** La configuración en mirror del Sistema Operativo funcionó satisfactoriamente. **Fecha de evaluación:** 2014-02-07

TS_PE_DB.0002. Sistema de red Redundante	**Prueba a realizar:** El sistema soportará la pérdida de conexión de un nivel de la red, sin que conlleve la no-disponibilidad del servicio ante una posible pérdida de conectividad con una parte del sistema de comunicaciones. Los pasos que se realizarán son: • Desconectar un cable en la tarjeta de red activa. • Verificar la conectividad de red entre servidores. **Resultado esperado:** El sistema opera normalmente sin presentar intermitencias de conexión de red. **Resultado de la prueba:** La configuración de red redundante funcionó satisfactoriamente, el sistema no presentó intermitencias ante la desconexión de uno de sus puertos de red. **Fecha de evaluación:** 2014-02-07
TS_PE_DB.0003. Configuración del Cluster de Red Hat Linux	**Prueba a realizar:** El sistema estará preparado para realizar un correcto balanceo del servicio de cluster de la Base de Datos ante una posible caída de uno de sus nodos host. Para ello se realizará las siguientes actividades: • Apagar controladamente el servidor activo. • Verificar en la consola de administración del cluster la migración del servicio de Base de Datos al servidor pasivo. • Encender el servidor • Devolver el servicio de Base de Datos al servidor encendido a través de la consola de administración del cluster. **Resultado esperado:** El sistema es capaz de balancear el servicio de la base de datos en configuración cluster entre sus dos servidores host. **Resultado de la prueba:** La configuración de cluster de Red Hat Linux respondió satisfactoriamente ante el apagado de uno de sus servidores host. **Fecha de evaluación:** 2014-02-07
TS_PE_DB.0004. Redundancia de Fuentes de Alimentación	**Prueba a realizar:** El sistema soportará un posible fallo de una fuente de alimentación eléctrica sin que conlleve la pérdida de los servicios. Los pasos que se realizarán son: • Desconectar un cable de alimentación eléctrica. • Verificar que la fuente redundante conserva la operación del servidor. • Validar que el servidor se mantenga operativo. **Resultado esperado:** El sistema opera normalmente sin presentar interrupciones eléctricas. **Resultado de la prueba:** La configuración redundante de fuentes de alimentación funcionó satisfactoriamente, el sistema no fue afectado por ninguna interrupción eléctrica.

	Fecha de evaluación: 2014-02-07
TS_PE_DB.0005. Recuperación de datafiles de la Base de Datos Oracle	**Prueba a realizar:** El sistema será afectado por la pérdida de varios datafiles de la Base de Datos debido a un daño en una de sus unidades lógicas. Para ello se realizará las siguientes actividades • Eliminar manualmente varios datafiles (sistema y datos) de la Base de Datos. • Reconstruir los datafiles eliminados a partir del último backup. • Verificar el estado consistente de la Base de Datos de acuerdo a la información del último respaldo. **Resultado esperado:** La Base de Datos puede ser abierta en un estado consistente con la información registrada en su último backup. **Resultado de la prueba:** El Equipo de Respuesta a Incidentes detectó una falla a nivel de Base de Datos que no permitió la operación normal del SIMEC, debido a la gravedad del daño, se procedió a reportar el incidente al Equipo de Manejo de Emergencia. Por la naturaleza del evento disruptivo, el DRP Líder activó el Plan de Recuperación de Desastres del SIMEC, mediante la ejecución del respectivo árbol de llamadas. Para el caso, el Coordinador del Área Informática contactó al Equipo de Software y Aplicaciones, y al proveedor externo de soporte ORACLE. Para el escenario identificado, se aplicó el "Procedimiento de Instalación Bases de Datos Oracle 11g R2 Cluster RHEL", que permitió el restablecimiento de la Base de Datos del SIMEC en un tiempo de 8 horas, siendo éste menor al valor del RTO definido para el sistema. **Observaciones:** El caso de prueba desarrollado asumió lo siguiente: • El caso de prueba es un criterio de activación del DRP. • El Comité Ejecutivo determinó la necesidad de activar el DRP. • Para el desarrollo de este caso de prueba fue necesario contar con el soporte externo de ORACLE en las instalaciones del CENACE. **Fecha de evaluación:** 2014-02-07

Fuente: CENACE

4.2.2.3 Fase 3 – Verificar

Proceso: F3.k Auditorías Internas

Actividades: La ejecución de la primera auditoría al DRP del SIMEC se realizó con el apoyo de un representante del Área de Análisis y Control como auditor, mientras que el Coordinador del Área Informática y el equipo de recuperación de desastres como auditados.

El primer ejercicio de auditoría se realizó en base a los procedimientos establecidos para auditorías en el Sistema de Gestión de la Calidad del CENACE. Los resultados obtenidos fueron plasmados en el respectivo informe para la revisión del Director de Sistemas de Información.

Tiempo empleado: 6 horas.

Entregable:

E12 PLAN DE AUDITORÍA DEL DRP PARA EL SISTEMA SIMEC

CORPORACION CENTRO NACIONAL DE CONTROL DE ENERGÍA PLAN DE AUDITORÍA 2014-01			
Nombre:	Ing. Linda Chimborazo		
Cargo:	Análisis y Control	Correo electrónico	lchimborazo@cenace.org.ec
Alcance: Determinar la conformidad del Plan de Recuperación de Desastres con los requerimientos del CENACE basados en el BIA, Análisis de Riesgos y estrategia de recuperación de desastres aplicados para el Sistema de Medición Comercial "SIMEC".			
Criterios de Auditoría	Documentación del Plan de Recuperación de Desastres del SIMEC y sus respectivos procedimientos.		
Tipo de Auditoría:	☐ PRE – AUDITORIA	☐ EXTRAORDINARIA	▣ SEGUIMIENTO
Reunión de Apertura:	2014 02 24	Hora:	08:00h
Reunión de Cierre:	2014 02 24	Hora:	16:30 h
Auditor Líder:	Ing. Michelle Nieto (MN)	Correo electrónico	mnieto@cenace.org.ec
Auditor:	N/A	Auditor	N/A
Experto técnico:	Ing. Diego Pullas		
Fecha:	2014 02 24		

FECHA	HORA	PROCESO / ACTIVIDAD / REQUISITO POR AUDITAR	AUDITOR	CARGO Y NOMBRE
2014 02 24	08:00 h	Reunión de apertura	MN	DRP Líder y Equipos de Trabajo: respuesta a incidentes, manejo de emergencia, recuperación de redes, software y aplicaciones.
	8:30 h	Conformación de equipos y responsabilidades	MN	DRP Líder
	10:30 h	Revisión árbol de llamadas	MN	DRP Líder, Equipo de Manejo de Emergencia.
	11:00 h	Revisión instructivo backups	MN	Equipo software y aplicaciones
	14:30 h	Gestión para la recuperación de desastres	MN	DRP Líder y Equipos de Trabajo: respuesta a incidentes, manejo de emergencia, recuperación de redes, software y aplicaciones.
	15:30 h	Revisión procedimientos	MN	Equipos de Trabajo: respuesta a incidentes, manejo de emergencia, recuperación de redes, software y aplicaciones.
Observaciones:				
Objetivos de la Auditoría: 1.1 Determinar la conformidad del DRP con los criterios de auditoría. 1.2 Determinar la eficaz implementación y mantenimiento del DRP. 1.3 Identificar oportunidades de mejora en el DRP				
Nota: Durante la auditoría se utilizará el método PHVA en cada proceso, con base a un muestreo selectivo de actividades y documentos.				

CORPORACION CENTRO NACIONAL DE CONTROL DE ENERGÍA

INFORME DE AUDITORÍA

2014-01

1. Introducción: La auditoría cubrió la totalidad de temas asociados al Plan de Recuperación de Desastres implantado actualmente en el Sistema de Medición Comercial del CENACE.

2. Hallazgos y Recomendaciones:
   - Documentación: No existe la información referente a los procedimientos para la recuperación del enlace de comunicaciones con la red WAN de CELEC EP – TRANSELECTRIC.
   - Seguimiento: El DRP del SIMEC no ha sido socializado con todos los Funcionarios de la Dirección de Sistemas de Información.
     Se verificó los resultados de las pruebas realizadas al DRP.
   - Proceso de Auditoría: El auditor realizó su preparación de auditoría en instalaciones fuera del CENACE, que permitió una mejor preparación de la misma. El tiempo destinado para la auditoría resultó muy corto.

3. Resultados Numéricos:

Resultados	DSI		TOTAL
	Acciones de Corrección	Acciones de Prevención	
Nuevas	1	2	3
Cerradas	0	0	0
En proceso	0	0	0
Nuevas Observaciones	3		3

4. Conclusiones:
   - Preparar un plan de acción con la DSI para solventar las acciones de corrección y prevención identificadas en la presente auditoría.
   - Diseñar un programa de auditorías de alcance anual que permita abordar diferentes estrategias de revisión y pruebas del DRP.

Auditor Líder:	
	Ing. Michelle Nieto

4.2.2.4 Fase 4 – Actuar

Proceso: F4.I Acciones de Mejora

Actividades: El plan de acciones de mejora ha sido elaborado por el Coordinador del Área Informática, con la información de los resultados alcanzados en el primer ejercicio de auditoría y las pruebas del DRP del SIMEC.

El plan identificado constituye un ejemplo propositivo que deberá ser validado y autorizado por el Director de Sistemas de Información.

Tiempo empleado: 4 horas.

Entregable:

E13	PLAN DE ACCIONES DE MEJORA DEL DRP PARA EL SISTEMA SIMEC

CORPORACION CENTRO NACIONAL DE CONTROL DE ENERGÍA PLAN DE ACCIONES DE MEJORA DEL PLAN DE RECUPERACIÓN DE DESASTRES PARA EL SIMEC
1. Introducción: En base a los resultados de la auditoría interna, los resultados de las pruebas y condiciones del entorno del CENACE, a continuación se plantea las siguientes iniciativas de mejora del Plan de Recuperación de Desastres para el SIMEC.
2. Actividades: 2.1 Conocimiento del DRP del SIMEC en la DSI. Dado que el alcance inicial de la capacitación cubrió únicamente a los Equipos de Trabajo del DRP del SIMEC, se preparará un evento de capacitación para todos los Funcionaros de la DSI para su socialización. Responsable: Ing. Marco Bautista. Plazo: primer semestre 2014. 2.2 Seguridad de la Información. En vista que el manejo y gestión de activos es un componente clave para la gestión de riesgos de una organización; y por otra parte, existe una disposición gubernamental respecto al uso de las normas técnicas INEN-ISO/IEC 27000. La Dirección de Sistemas de Información emprenderá con un proceso para la conceptualización y diseño para la implementación de la citada norma en el CENACE. Responsable: Ing. Gonzalo Uquillas. Plazo segundo semestre 2014.

4.2.3 Evaluación de Resultados

Una vez que concluida la aplicación del caso de estudio del plan de recuperación de desastres para el Sistema de Medición Comercial "SIMEC", en base al marco de referencia propuesto, los resultados obtenidos son los siguientes:

a) Fase 1 Planificar, se logró la creación de una propuesta de Política de Recuperación de Desastres para el CENACE que marca los lineamientos y objetivos a aplicarse por la Corporación en materia de eventos de desastre; dicha política estableció los requisitos para la creación del Comité, Coordinador y el Equipo de Recuperación de Desastres cuya responsabilidad la asumió el Comité Ejecutivo, Director de Sistemas de Información e Ingenieros de la Dirección de Sistemas de información respectivamente.

   La planificación del proyecto DRP para el SIMEC, se planteó y desarrolló en base a las mejores prácticas para el desarrollo de proyectos utilizados en el CENACE.

b) Fase 2 Hacer, la culminación de las actividades de la fase de planificación, permitió el desarrollo de las actividades de la fase dos, iniciando con el Análisis de Impacto de Negocio para el SIMEC que identificó al citado sistema como crítico y de alta prioridad de recuperación, debido a que soporta un proceso sustantivo de la cadena de valor del CENACE; el análisis BIA también permitió determinar los valores para el RTO y RPO de veinte y cuatro horas. A continuación, se realizó el Análisis de Riesgos para el SIMEC que bajo un marco metodológico seleccionado, permitió la obtención de los activos del SIMEC con su respectiva valoración, la identificación de amenazas y vulnerabilidades de los activos identificados, para finalmente obtener el nivel de riesgo al que están expuestos los

activos, que se resumen en 6 de riesgo alto, 17 de riesgo medio y 7 de riesgo bajo.

Como primera acción a ejecutarse con los resultados del BIA y análisis de riesgos del SIMEC se obtuvo el Plan de Medidas Preventivas de Recuperación de Desastres para el SIMEC, que abarcó seis actividades proactivas cuya implementación es de corto plazo y con el uso de recursos propios de la Corporación.

El principal resultado de la aplicación del BIA y análisis de riesgos del SIMEC es la Definición de la Estrategia de Recuperación de Desastres para el SIMEC, determinándose que en la situación actual y en una primera fase, el sistema dispone de métodos de recuperación como: cluster´s, arreglos de discos y sistemas de backup´s que han permitido mantener adecuados niveles de disponibilidad y operación del sistema, por tanto, la estrategia de recuperación fue ratificada por parte del nivel Directivo debido a que los límites establecidos para el RTO y RTO previamente identificados, son perfectamente alcanzables y factibles en su cumplimiento.

La siguiente actividad consistió en el desarrollo del Plan de Recuperación de desastres para el SIMEC, que en su parte medular contempló los componentes indicados a continuación: objetivo, alcance, identificación de equipos de trabajo y responsabilidades, identificación del árbol de llamadas, proceso de backups, la declaración y activación del DRP; y, finalmente la creación de los procedimientos específicos de recuperación del SIMEC aplicados en 5 escenarios disruptivos. En el contexto general, también se observó la relación del DRP del SIMEC con otros planes como el Plan de Emergencia y Contingencia del CENACE.

Luego de la creación del DRP, se procedió con la creación del Plan de Pruebas del DRP del SIMEC, que de manera ejemplificativa fue aplicado al procedimiento de instalación y restauración de la base de datos del SIMEC,

con resultados satisfactorios. Seguidamente se presentó el Plan de Capacitación del DRP del SIMEC con dos cursos, uno de temática teórica y el segundo de carácter práctico que se impartió al equipo de recuperación de desastres.

c) Fase 3 Verificar, en esta fase se abordó de manera específica un Plan de Auditoría del DRP del SIMEC, basado en la información documentada del DRP. Resultó clave el apoyo que brindó el Área de Análisis y Control del CENACE para la ejecución de la citada auditoría en base a su experiencia como auditores de calidad de la norma ISO 9001:2008. Los resultados obtenidos en la auditoría se plasmaron en su respectivo informe.

d) Fase 4 Actuar, Finalmente la aplicación de la última fase del marco de referencia permitió obtener el Plan de Acciones de Mejora del DRP del SIMEC, que en base a los resultados previamente conseguidos de las fases anteriores (auditorías y pruebas), se logró determinar en principio dos actividades de mejora para acometerse en un corto plazo al interior del CENACE.

5 Capítulo V: Conclusiones y Recomendaciones

5.1 Conclusiones

- 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 y sobre todo con el apoyo y compromiso de la Alta Gerencia.

- Por su naturaleza, el CENACE cumple funciones únicas en el Sector Eléctrico Ecuatoriano y emitidas por Ley, su accionar tiene como base un fuerte componente tecnológico con servicios y sistemas de información con que demandan una operación las 24 horas del día, los 365 días del año, por tanto, es imperativo para la Corporación la adopción de estrategias alternativas para mejorar la disponibilidad y continuidad de sus servicios de información.

- La plataforma tecnológica del CENACE está constituida por sistemas tecnológicos en "tiempo real" y "fuera de línea"; sin ser necesaria la operación de un sistema con datos en tiempo real, la calificación de criticidad de un determinado sistema está dado por el uso y aporte a un proceso

crítico de negocio. El CENACE cuenta con varios sistemas tecnológicos fuera de línea que son considerados críticos para el desarrollo de sus procesos y generación de sus servicios de información a sus clientes.

- 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.

- La aplicación del marco de referencia para la planificación de recuperación de desastres propuesto, permitió de una manera simple, efectiva, sistemática y detallada, obtener el Plan de Recuperación de Desastres para el SIMEC, incluyendo su modelo de operación y con el sustento de los principales documentos de soporte de dicho plan.
- El presente trabajo de investigación constituye un primer paso de lo que sería la aplicación de un plan de recuperación de desastres para toda la Corporación CENACE, 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 del CENACE.

- Los conceptos esgrimidos en el marco de referencia propuesto, han sido complementados y reforzados en el caso de estudio, en donde, a través de formatos y toolkits, los entregables en cada una de las fases son fácilmente realizables.

- La aplicación de las cuatro fases del marco de referencia para la recuperación de desastres propuesto, involucra la creación/eliminación y actualización de documentos en cada una de ellas, por tanto, se requiere contar con un sistema de gestión de documentos para el DRP del SIMEC.

- La Corporación CENACE no cuenta con un plan de recuperación de desastres global que involucre a todos los procesos de la cadena de valor con sus respectivos servicios/sistemas de TI; la estrategia y plan elaborados para el SIMEC, basados en los métodos de protección como arreglos de discos, clusters de aplicaciones, redundancia de comunicaciones y respaldos de información han proporcionado resultados satisfactorios y son factibles de ampliarse a otros sistemas.

- El marco de referencia propuesto en la presente tesis pretende constituirse en una guía referencial para la Planificación de Recuperación de Desastres, que ayude en la identificación de equipos de trabajo, sus responsabilidades, los procesos y procedimientos de recuperación, sus mecanismos de verificación y mejora continua; contribuyendo de esta manera a las organizaciones para contar con una herramienta que permita mejorar las condiciones de fiabilidad, seguridad y disponibilidad de los servicios críticos de TI.

5.2 Recomendaciones

- El marco de referencia propuesto para la Planificación de Recuperación de Desastres y aplicado en el CENACE, deberá ser revisado y aprobado por parte de su Comité Ejecutivo (Directores y Jefes de Área), a fin de que su aplicación y uso en toda la Corporación sea de manera obligatoria.

- Se deberá emprender en una campaña para crear una cultura de recuperación de desastres en el CENACE, para lo cual, es necesario capacitar y concienciar a todos los colaboradores sobre aspectos relacionados con la planificación de recuperación y continuidad del negocio.

- Debido a que el DRP es un documento "vivo", se recomienda la creación de un Equipo de Recuperación de Desastres permanente que bajo la dirección

de su Coordinador, sea el encargado de mantenerlo actualizado y mejorado continuamente.

- La ejecución de las actividades como el BIA y Análisis de Riesgos son los elementos clave para la determinación de los procesos críticos y la identificación de los activos que hay que proteger en el DRP, por tanto, se recomienda considerar el apoyo de especialistas externos (consultores) en el manejo de seguridad de la información y gestión de riesgos.

- El DRP es un instrumento manejado íntegramente en el ámbito de TI, sin embargo, desde el punto de vista empresarial, la recuperación de desastres deberá ser complementada con un Plan de Emergencia y Contingencia (seguridad de las personas) y un Plan de Continuidad de Negocios (operación funcional).

- Será necesario completar la segunda fase para el tratamiento de los riesgos identificados en el SIMEC, a fin de complementar la actual estrategia y plan de recuperación de desastres.

- Partiendo del peor escenario disruptivo, que puede ser la pérdida del sitio sede de operación del SIMEC, sería recomendable para la Corporación CENACE elaborar un nuevo análisis de riesgos que permita evolucionar la estrategia de recuperación de desastres a soluciones como un Hot Site, Mirrored Site o alternativamente el uso de tecnologías emergentes conocidas bajo el nombre de recuperación como servicio (Recovery as a Service - RaaS); a fin de otorgar mayores de niveles de confiabilidad y disponibilidad del citado sistema.

Referencias

Areitio, J. (2008). Seguridad de la Información Redes, Informática y Sistemas de Información. Madrid: Paraninfo.

Centro Nacional de Control de Energía. (2013). Plan Estratégico CENACE 2013. Quito.

Centro Nacional de Control de Energía. (2013). Testimonios de Sueños y Realidades. Quito.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). MAGERIT - Metodología de Análsis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones Públicas.

EC-Council. (2010). Introduction to Disaster Recovery & Business Continuity. Disaster Recovery & Business Continuity. USA.

Erbschloe, M. (2003). Guide to Disaster Recovery. Boston: THOMSON Course Technology.

Fackler, M. (29 de abril de 2013). Flow of Tainted Water Is Latest Crisis at Japan Nuclear Plant. The New York Times, pág. 2.

INTECO. (2010). Guía práctica para PYMES: cómo implantar un Plan de Continuidad de Negocio. Guía práctica para PYMES: cómo implantar un Plan de Continuidad de Negocio. Madrid.

ISACA. (2012). CISA Review Manual 2012. Rolling Meadows, IL 60008: ISACA.

ISACA. (2012). COBIT 5 Enabling Processes. USA: ISBN 978-1-60420-241-0.

ISO. (2012). NORMA ISO 22301. Switzerland: ISO copyright office.

ITIL V3 Foundation. (2009). The Art of Service. Brisbane.

L., M. A. (2010). ITIL Foundations v3 Plus - Manual de Estudiante. Quito.

Nickolett, C., & Schmidt, J. (2001). Business Continuity Planning Description and Framework., (pág. 10).

Publicaciones, C. d. (2007). Ley de Régimen del Sector Eléctrico, Reglamento y Legislación Conexa. Quito.

Ragheb, M. (2011). FUKUSHIMA EARTHQUAKE AND TSUNAMI STATION BLACKOUT ACCIDENT.

Superintendencia de Bancos y Seguros del Ecuador. (20 de Octubre de 2005). Codificación Resoluciones SBS y Junta Bancaria del Ecuador. Recuperado el 25 de Abril de 2014, de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_V.pdf

Universidad de Toronto. (2011). Disaster Recovery Plan. Recuperado el 1 de Agosto de 2013, de http://www.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm#plan)

Wallace, M., & Webber, L. (2011). The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets. New York: AMACOM.

Anexos

Anexo 1

ANÁLISIS DE IMPACTO DE NEGOCIO - CUESTIONARIO	
ORGANIZACIÓN:	
ÁREA/DEPARTAMENTO DE NEGOCIO:	
NOMBRE DEL DIRECTOR DEL ÁREA/DEPARTAMENTO:	
DESCRIPCIÓN DEL OBJETO DEL ÁREA/DEPARTAMENTO EN LA ORGANIZACIÓN:	
NOMBRE DE LA PERSONA ENTREVISTADA:	CARGO:

LISTA DE PROCESOS DEL ÁREA/DEPARTAMENTO:

N°	PROCESOS

ÁREA/DEPARTAMENTO DE NEGOCIO:	PROCESO DE NEGOCIO N°: ___
DESCRIPCIÓN:	
PERSONA ENTREVISTADA:	CARGO:
SISTEMA QUE LO SOPORTA:	ADMINISTRADOR DEL SISTEMA:

ACTIVIDADES	PRIORIDAD DE RECUPERACIÓN		
	ALTA	MEDIA	BAJA

DESCRIPCIÓN DEL SISTEMA: (Incluir arquitectura, diagramas de sistemas, etc.)

1. IDENTIFICAR PUNTOS DE CONTACTO FUNDAMENTALES DEL SISTEMA	ROL CRÍTICO	RECURSO
Internos: (Identificar personas o departamentos de la organización que dependen o apoyan al sistema)		
Externos: (Identificar personas o departamentos fuera de la organización que dependen o apoyan al sistema)		

2.- IDENTIFICAR EL TIEMPO DE RECUPERACIÓN OBJETIVO: (Identificar el período máximo aceptable de indisponibilidad del recurso)

RECURSO	TIEMPO ADMISIBLE DE INTERRUPCIÓN

3.- IDENTIFICAR EL PUNTO DE RECUPERACIÓN OBJETIVO: (Punto de recuperación de la información requerida para continuar con el proceso después de la interrupción)

RECURSO	PUNTO DE RECUPERACIÓN OBJETIVO

4.- PRIORIZAR LA RECUPERACIÓN DE RECURSOS: (Indicar la prioridad asociada a la recuperación de un recurso específico, considerando el impacto de interrupciones y tiempos de interrupción permisibles establecidos en la Sección 5.)

RECURSO	PRIORIDAD DE RECUPERACIÓN		
	ALTA	MEDIA	BAJA

Anexo 2 - Formato para la Evaluación Cualitativa de Riesgos

EVALUACIÓN DE RIESGOS

Inventario de Activos de Información - Sistema ABC															
Código	Activos	Categoría	Descripción	Ubicación	Responsable/Dueño	Cont.	Int.	Disp.	Consecuencia Operacional	Consecuencia Reputacional	Consecuencia Económica	Consecuencia Regulatoria	Consecuencia Final	Valor del activo

Amenazas y Vulnerabilidades - Sistema ABC					
Activos		Factor de Exposición			
		Análisis de Vulnerabilidades (V) y el conjunto de Amenazas (T) que podrían explotar la vulnerabilidad identificada*			
Código de Activo	Activo	Código de la Vulnerabilidad	Vulnerabilidad	Código de la amenaza	Valor del Factor de Exposición (FE)

Cálculo del Riesgo - Sistema ABC					
Código de Activo	Activo	Valor de Activo (VA)	Valor del Factor de Exposición (FE)	Cálculo del Riesgo (R) R=(VA*FE)	Nivel del riesgo*

Anexo 3 - Catálogo de Vulnerabilidades y Amenazas

CATÁLOGO DE VULNERABILIDADES

Código	Vulnerabilidad	Amenazas relacionadas
Vulnerabilidades Específicas por Activo o grupo de Activos		
Activos tipo SITIO/AMBIEN	**Las vulnerabilidades se dan en términos de falta, ausencia, insuficiencia, mala, inadecuada, débil y/o carencia de algo (protección o control)**	**Amenazas relacionadas**
V1	Protección física en el área de trabajo (frente a desastres naturales)	T1-T5, T6-T9, T21, T47, T66, T71, T72
V2	Control de Acceso al Sitio (Puertas, llaves, candados, cercas, etc.)	T59, T71, T72
V3	Control de visitantes al sitio	T59, T71, T72
V4	Abastecimiento de Energía Eléctrica	T13
V5	Abastecimiento de Agua y otros suministros de servicios públicos: agua, gas	T18
V6	Abastecimiento de aire acondicionado	T14
V7	Mantenimiento Preventivo del sitio	T1-T5, T6-T9, T21
V8	Almacenamiento de material volatil/ inflamable a granel	T1, T6, T71
V9	Prevención y Detección contra incendio	T1, T6, T71
V10	Ubicación del sitio	T1-T5, T6-T9, T21, T71, T72
V11	Monitoreo de los accesos a los sitios	T59, T70, T71, T72,
V12	Protección contra emanación electromagnética	T20
Activos tipo PERSONA	**Las vulnerabilidades se dan en términos de falta, ausencia, insuficiencia, mala, inadecuada, débil y/o carencia de algo (protección o control)**	**Amenazas relacionadas**
V13	Personal de respaldo capacitado o con conocimientos mínimos para llevar a cabo tareas en la organización.	T44, T73
V14	Procesos, procedimientos de reclutamiento/selección de personal. Nota: las amenazas supuestas a través del control inadecuado de reclutamientos son extensas. Las amenazas listadas son ejemplos. Trabajo bajo presión	T22, T30, T34, T45, T46, T47, T52, T62, T65, T70, T71, T72, T74, T91, T99
V15	Definición de roles, perfiles, responsabilidades	T30, T35, T36, T39
V16	Exclusión/Inclusión en listas de distribución de documentos	T34, T38, T39, T62, T66, T70, T79,
V17	Concientización, capacitación, formación en seguridad de la información	T21, T22, T24, T31, T35, T52, T53, T54, T66, T74, T75,
V18	Personal capacitado, entrenado o con experiencia en los procedimientos operativos y herramientas de la organización	T22, T23, T24, T35, T40, T45
V19	Políticas, Normas, Estándares, Procedimientos documentados, aprobados, divulgados. Nota: las amenazas supuestas a través de éste control son extensas. Las amenazas listadas son ejemplos.	T22, T45, T46, T48, T51, T52, 753, T54, T59, T70, T74, T75, T78, T82, T84, T91, T94, T95, T100
V20	Revocación de derechos de acceso	T34, T35, T36, T39, T48, T51, T52, T59, T63, T64, T65, T66, T67,
V21	Medio ambiente de trabajo cómodo, agradable, confiable en términos de ruido, olor, iluminación, clima, etc.	T22, T34, T65, T66, T71, T73, T74, T75
V22	Recursos y demás herramientas para llevar a cabo las actividades (Horas de trabajo compatibles)	T22, T31, T35, T36, T38, T39, T43, T45, T46, T47, T50, T51, T54, T59,
V23	Acuerdos de Confidencialidad, responsabilidades, acuerdos contractuales	T22, T24, T35, T45, T46, T39, T52, T53, T66, T70, T75, T99
Activos tipo HARDWARE	**Las vulnerabilidades se dan en términos de falta, ausencia, insuficiencia, mala, inadecuada, débil y/o carencia de algo (protección o control)**	**Amenazas relacionadas**
V24	Adquisición, Mantenimiento y seguimiento al funcionamiento	T8, T10, T19, T42, T43,
V25	Almacenamiento, ubicación, fijación, exposición	T1, T2, T3, T4, T5, T6, T7, T8, T9, T14, T20, T21, T70,
V26	Compatibilidad, Capacidad, requerimientos, compatibilidades y especificaciones definidas	T10, T16, T19, T43, T69,
V27	Control de Acceso	T21, T23, T45, T51, T54, T59, T62, T69, T70, T71, T72, T96, 798,
V28	Procedimiento de Descarte y reemplazo de Equipos y/o medios	T34, T62, T70, T80, T96,
V29	Tiempo de sincronización	T25, T26, T27, T61,
V30	Suministro continuo y eficiente de energía eléctrica	T13
V31	Control de Configuración	T28, T29, T49, T69,
V32	Conexión autorizada	T27, T31, T34, T43, T54, T59, T62, T78,
V33	Uso y manipulación apropiada y controlada (Procedimientos y políticas de uso aceptable)	T22, T23, T45, T49, T52,
V34	Otorgamiento y Cambio controlado de usuarios a equipos (PCs, Servidores) y medios	T22, T42, T45, T52, T70,
V35	Inventario, Etiquetado, control de entrada y salida de elementos	T70
V36	Ausencia de controles para equipos fuera de las instalaciones de la organización (Personal Firewall y Cifrado)	T34, T39, T66, T80

Activos tipo RED	Las vulnerabilidades se dan en términos de falta, ausencia, insuficiencia, mala, inadecuada, débil y/o carencia de algo (protección o control)	Amenazas relacionadas
V37	Adquisión, Mantenimiento y seguimiento al funcionamiento	T8, T10, T19, T42, T43,
V38	Almacenamiento, ubicación, fijación, exposición	T1, T2, T3, T4, T5, T6, T7, T8, T9, T14, T20, T21, T70,
V39	Compatibilidad, Capacidad, requerimientos, compatibilidades y especificaciones definidas	T10, T16, T19, T43, T69
V40	Control de Acceso	T23, T45, T51, T54, T59, T62, T69, T70, T71, T72, T96, 798,
V41	Uso, fortaleza, complejidad, calidad y gestión de contraseñas de acceso a elementos de red	T34, T48, T49, T50, T51, T58, T78,
V42	Tiempo de sincronización	T25, T26, T27, T61,
V43	Suministro continuo y eficiente de energía eléctrica	T13
V44	Control y administración de configuraciones (Líneas base de configuración)	T28, T29, T34, T37, T41, T49, T51, T52, T62, T63, T69, T88, T89
V45	Conexión autorizada	T27, T34, T54, T59, T62, T78,
V46	Uso y manipulación apropiada y controlada (Procedimientos y políticas de uso aceptable)	T22, T23, T45, T49, T52,
V47	Protección contra emanación electromagnética	T20
V48	Mecanismos de Monitoreo (Logs en los elementos de red)	T27, T33, T34, T43, T48, T49, T50, T54, T57, T58, T60, T61, T69, T78, T85, T87, 790
V49	Mecanismos de Monitoreo (mecanismos de IPS/IDS)	T27, T33, T34, T43, T48, T49, T50, T54, T57, T58, T60, T61, T69, T78, T85, T87, 790
V50	Falta de cifrado en el canal (lo cual pérmite ver información sensible como contraseñas, datos de tarjetahabiente, información sensible), gestión de llaves de cifrado en los elementos de red	T34, T50, T54, T60, T62,
V51	Líneas de comunicación protegidas (conexiones físicas en el cableado, blindaje de los cables,	T9, T15, T20, T32, T33, T34, T56, T57, T60, T62, T69, T78, T85, T87,
V52	Identificación remitente y receptor	T27, T32, T33, T34, T50, T51, T57, T58, T61, T78,
V53	Uso y manipulación apropiada y controlada (Procedimientos y políticas de uso aceptable)	T22, T23, T45, T49, T52,
V54	Autenticación de usuarios para conexiones externas	T34, T50, T56, T58, T85,
V55	Uso, fortaleza, complejidad, calidad y gestión de contraseñas de acceso a elementos de red	T34, T48, T49, T50, T51, T58, T78,
V56	Separación de las redes confiables de las no confiables (Control de conexión entre redes por intermedio de Firewalls de red). Conectividad del sistema de información (Sistema aislado, conectado a un conjunto reducido y controlado de redes, conectado a un amplio colectivo de redes conocidas, conectado a Internet)	T32, T33, T34, T56, T57, T58, T62, T78, T80, T83, T85, T87, T97,
V57	Seguridad en Comunicaciones inalámbricas (uso de protocolos de seguridad inlámbricos)	T34, T58, T59, T60, T62, T78, T87
V58	Puntos de acceso protegidos (Puertos públicos)	T34, T58, T59, T60, T62, T78, T87
V59	Inventario, Etiquetado, control de entrada y salida de elementos	T70
Activos tipo SOFTWARE	**Las vulnerabilidades se dan en términos de falta, ausencia, insuficiencia, mala, inadecuada, débil y/o carencia de algo (protección o control)**	**Amenazas relacionadas**
V60	Capacidad, requerimientos, compatibilidades y especificaciones definidas	T11, T12, T43, T69,
V61	Pruebas de seguridad y funcionales antes de su despliegue (sea por cambios, actualizaciones, parches, etc.)	T11, T12, T28, T29, T34, T37, T40, T41, T48, T49, T50, T51, T57, T58, T67, T76, T77, T83, T87, T88, T89,
V62	Interfase de usuario adecuada, amigable, intuitiva	T22, T23, T28, T36, T46,
V63	Control de Acceso (Restricciones en el acceso al software y mecanismos de autenticación), Políticas de Control de Acceso	T22, T23, T24, T25, T28, T34, T36, T46, T48, T49, T50, T51, T52, T53, T58, T62, T64, T67, T69,
V64	Sistema aislado a nivel de red de otros sistemas de información no complementarios	T34, T58, T62, T83, T85, T87, T97,
V65	Cambios controlados, aprobados, autorizados, evaluados	T11, T12, T28, T29, T34, T36, T37, T43, T49, T51, T57, T58, T62, T67, T68, T76, T77, T83, T87, T88, T89
V66	Desarrollo seguro de software	T11, T12, T29, T37, T58, T61, T67, T68, T69, T76, T77,

V67	Uso y manipulación apropiada y controlada (Procedimientos y políticas de uso aceptable) de herramientas, utilerías, software, navegación en internet, etc.	T22, T23, T24, T25, T26, T28, T29, T36, T46, T51, T52, T53, T64, T67,
V68	Uso, fortaleza, complejidad, calidad y gestión de contraseñas de acceso al software	T34, T48, T49, T50, T51, T58, T78,
V69	Tiempo de inactividad y tiempo de conexión de las sesiones	T34, T36, T46, T48, T49, T50, T58, T62, T67,
V70	Documentación, procedimientos, manuales y licencias del software	T22, T23, T24, T25, T26, T28, T29, T41, T46,
V71	Administración e instalación oportuna de parches, service pack, hot fixes, etc	T11, T12, T31, T34, T37, T41, T55, T58, T83,
V72	Encripción por parte del software (encripción de la aplicación o del motor de base de datos), gestión de las llaves de cifrado	T34, T51, T58, T59, T66, T67, T68, T70, T83, T86, T102
V73	Inpección de código	T34, T37, T40, T51, T55, T58, T66, T76, T77, T83, T87, T89, T99,
V74	Control en el uso de data real en ambientes previos	T29, T34, T58, T62, T63, T66, T80, T86, T87, T99
V75	Software Antimalware	T31, T51, T55, T62, T63, T65, T68, T69, T80, T83, T87
V76	Control y administración de configuraciones (Líneas base de configuración, FIM, Policy Compliance)	T12, T28, T29, T34, T37, T41, T49, T51, T52, T57, T62, T63, T67, T68, T69, T88, T89
V77	Enmascaramiento de información por parte del software a la información sensible	T34, T39, T51, T58, T62, T66, T70, T79, T80, T81, T83, T87, T96, T99,
V78	Mecanismos de Monitoreo (Logs en el software)	T27, T34, T48, T49, T50, T57, T58, T61, T90
V79	Gestión de Vulnerabilidades Técnicas (Tests de vulnerabilidades y Ethical Hacking)	T28, T29, T41, T58, T68, T83,
V80	Definición de roles, perfiles, responsabilidades	T34, T46, T48, T49, T51, T52, T53, T57, T58, T63, T64, T66, T67, T80, T83, T87, T99
p	**Las vulnerabilidades se dan en términos de falta, ausencia, insuficiencia, mala, inadecuada, débil y/o carencia de algo (protección o control)**	**Amenazas relacionadas**
V81	Almacenamiento, ubicación, fijación, exposición	T14, T34, T35, T38, T39, T59, T63, T65, T66, T70, T79,
V82	Política de Escritorio limpio	T34, T35, T38, T39, T59, T63, T65, T66, T70, T79,
V83	Copias de Respaldo	T19, T22, T35, T36, T38, T48, T63, T64, T65, T70,
V84	Procedimientos de Identificación, ubicación, detección de información, Clasificación y etiquetado de la información	T34, T35, T38, T39, T45, T51, T66, T79, T80, T81, T96, T99
V85	Procedimiento de Descarte y reemplazo de medios	T34, T70, T80, T96,
V86	Validación de datos de entrada	T12, T35, T38, T58, T63, T64,
V87	Almacenamiento de datos cifrados	T34, T39, T66, T80, T96,
V88	Control de entrada, distribución, salida	T34, T35, T38, T39, T63, T65, T66, T70, T79, T80
Activos Tipo SERVICIO	**Las vulnerabilidades se dan en términos de falta, ausencia, insuficiencia, mala, inadecuada, débil y/o carencia de algo (protección o control)**	**Amenazas relacionadas**
V89	Capacidad, requerimientos de seguridad, compatibilidades y especificaciones definidas	T17, T65, T66, T69,
V90	Monitoreo del acceso y uso del servicio	T90
V91	Continuidad del Servicio	T17, T69,
V92	Acuerdos de Confidencialidad, responsabilidades, acuerdos contractuales	T65, T66

CATÁLOGO DE AMENAZAS

Código	AMENAZA	Descripción	Propiedades de seguridad que se pueden ver afectadas por este tipo de Amenaza	Categoría de Activos afectados directamente por esta Amenaza
	Origen Natural			
T1	Desastre Natural- Fuego/Incendio	Suceso de causa directa o indirecta que pueden ocurrir sin intervención de los seres humanos . Incendios: posibilidad de que el fuego acabe con recursos del sistema.	Disponibilidad	Hardware Red Sitio
T2	Desastre Natural- Daños por Agua	Suceso de causa directa o indirecta que pueden ocurrir sin intervención de los seres humanos . Inundaciones: posibilidad de que el agua acabe con recursos del	Disponibilidad	Hardware Red Sitio
T3	Desastre Natural- Rayos, Tormenta Eléctrica	Suceso de causa directa o indirecta que pueden ocurrir sin intervención de los seres humanos . Fenómeno natural con efectos eléctricos	Disponibilidad	Hardware Red Sitio
T4	Desastre Natural- Terremoto	Suceso de causa directa o indirecta que pueden ocurrir sin intervención de los seres humanos . Fenómeno natural de movimientos fuertes de tierra	Disponibilidad	Hardware Red Sitio
T5	Desastre Natural- Huracán	Suceso de causa directa o indirecta que pueden ocurrir sin intervención de los seres humanos . Fenómeno natural	Disponibilidad	Hardware Red Sitio
	Origen Industrial			
T6	De Origen Industrial- Fuego	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas puede darse de forma accidental o deliberada. Incendios: posibilidad de que el fuego acabe con recursos del sistema.	Disponibilidad	Hardware Red Sitio
T7	De Origen Industrial- Daños por Agua	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas puede darse de forma accidental o deliberada. Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	Disponibilidad	Hardware Red Sitio
T8	Contaminación mecánica	Vibraciones, polvo, suciedad, partículas, polución, corrosión, etc.	Disponibilidad	Hardware Red Sitio
T9	Contaminación electromagnética	Interferencias de radio, campos magnéticos potentes, luz ultravioleta, ...	Disponibilidad	Hardware Red Sitio
T10	Avería, roturas, fallas en Hardware	Fallos en los equipos. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	Disponibilidad	Hardware Red
T11	Fallas lógicas (No disponibilidad del software)	Fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.	Disponibilidad	Software
T12	Fallas/Errores en el Procesamiento	El software no procesa datos correctamente	Integridad	Software
T13	Corte/Falla/picos/fluctuaciones del suministro eléctrico	Cese de la alimentación de potencia, carga electrostática, corto circuito	Disponibilidad	Hardware Red Sitio
T14	Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la acklimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, fallas de aire acondicionado, etc.	Disponibilidad	Hardware Red Sitio Información
T15	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte (cables) o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente. Daño a líneas, sobrecarga de tráfico, errores de transmisión.	Disponibilidad	Red Servicio
T16	Interrupción de otros servicios y suministros esenciales	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, plásticos, cintas, etc.	Disponibilidad	Hardware
T17	Interrupción de otros Procesos de Negocio	Otros Procesos de la organización fallan y afectan el servicio o el activo siendo analizado	Disponibilidad	Servicio
T18	Fallas y cortes en suministros de servicios públicos: agua, gas	Degradación o falla total de los servicios públicos con los que cuenta la organización.	Disponibilidad	Sitio
T19	Degradación y/o deterioro de los equipos y demás soportes o medios informáticos; Obsolescencia	Como consecuencia del paso del tiempo. Deterioro de medios de almacenamiento, deterioro de Hardware, impresoras, PCs, Servidores	Disponibilidad	Hardware Red Información
T20	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.	Confidencialidad	Hardware Red
T21	Daños Accidentales: nave aérea, colisión vehicular, material del edificio, mantenimiento edificio	Accidentes, daños por eventos fortuitos	Disponibilidad	Sitio Harware Red Personas

	Errores y fallos no intencionados			
T22	Errores de los usuarios	Fallos no intencionales causados por las personas/staff de la organización. Equivocaciones, omisiones, malos juicios de las personas cuando usan los recursos, datos, etc.	Integridad Disponibilidad	Servicios Información Software Persona Hardware
T23	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación sobre los activos de información tipo infraestructura	Disponibilidad Integridad Confidencialidad	Servicios Información Software Hardware Red Persona
T24	Mal uso de utilerías y herramientas administrativas de los sistemas operativos	Mal uso de utilerías y herramientas administrativas de los sistemas operativos, ya sea por parte de administradores, operadores o usuarios finales.	Disponibilidad Integridad Confidencialidad	Software Persona
T25	Mal uso de herramientas de auditoría	Manejo inadecuado por el personal administrativo o de auditoría de sistemas hacia las herramientas dispuestas para el monitoreo o auditoría de componentes de sistema	Disponibilidad Integridad	Software Red Hardware
T26	Errores de monitorización (log) y eventos como Borrado, destrucción, alterado y falsificación de Logs	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ... Reducción de la posibilidad de verificar eventos de seguridad importantes, tales como accesos no autorizados, errores, omisiones, etc., o de buscarlos respectivos agentes que causaron el incidente. Es provocada por falta o inconsistencia de registros de eventos, por ejemplo, los existentes en los logs de auditoría de software, en los libros de ocurrencias, etc., pudiendo resultar en repudio de los usuarios a sus acciones, ecusaciones impropias, recurrencia de incidentes u otras consecuencias	trazabilidad del servicio trazabilidad de los datos	Servicios Información Software Hardware Red
T27	Fugas/brechas no detectadas por falta de monitoreo	Inadecuado registro de actividades sobre la red y elementos de red que permitirá la fuga de información sin poder ser detectada	Confidencialidad	Red Hardware
T28	Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia el administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, protocolos y algoritmos débiles o landecuados, etc. Genrralmente se da por la falta de guías o líneas base de configuración para los componentes de sistema	Confidencialidad Disponibilidad Integridad	Servicios Información Software Hardware Red
T29	Errores en modificaciones y actualizaciones	Introducción de cambios, instalación de módulos y mejoras sin revisiones y aprobaciones, lo cual eventualmente implica fallas posteriores	Disponibilidad Integridad Confidencialidad	Servicios Información Software Hardware Red
T30	Deficiencias en la organización, asignación incorrecta o no clara de responsabilidades	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Mano de obra no preparada, Acciones descoordinadas, errores por omisión, etc.	Disponibilidad	Personas
T31	Difusión de software malicioso	Propagación inadvertida de virus, espías (spyware), gusanos, troyanos, bombas lógicas, bank trojans, Credentialed Malware, keyloggers, back doors, sniffers, RAM Scraper, etc.	Disponibilidad Integridad Confidencialidad	Software ATMs
T32	Errores de re-encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	Confidencialidad Integridad	Red
T33	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.	Integridad	Red
T34	Escapes/Fugas de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	Confidencialidad	Información Software Red
T35	Alteración de la información	Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	Integridad	Información Personas
T36	Introducción de información incorrecta	Inserción accidental de información incorrecta. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	Integridad	Software Información Personas
T37	Salida de información incorrecta o degradación de la información	La información resultante de un procesamiento en la aplicación no es lógica, y se desvía de los resultados esperados. Degradación accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	Integridad	Software
T38	Destrucción de información	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	Disponibilidad	Información
T39	Divulgación/Exposición de información	Revelación por indiscreción. Exposición de contraseña incontinencia verbal, medios electrónicos, soporte papel, etc.	Confidencialidad	Información Personas
T40	Errores de codificación en los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	Integridad Disponibilidad Confidencialidad	Software

T41	Errores de mantenimiento / actualización de programas (software). Ataques a Software por ausencia de Parches/Upgrades	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. Debido a lo no instalación de parches o hot fixes en el software, atacantes (internos y externos)y código malicioso puede explotar dicha vulnerabilidad	Integridad Disponibilidad Confidencialidad	Software
T42	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	Disponibilidad	Hardware
T43	Caída del sistema por agotamiento de recursos, Degradación por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Degradación en tiempos de respuesta, saturación de los sistemas de infoirmación.	Disponibilidad	Servicios Hardware Red
T44	Indisponibilidad o déficit del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, daño físico por atacarrte, muerte	Disponibilidad	Personas
T45	Uso inapropiado de Equipos y Medios Informáticos	Mal manejo de los elementos, mala manipulación, mala administración y mantenimiento, manipulación por visitantes, familiares	Disponibilidad	Hardware Red
T46	Uso inapropiado de Software	Mal manejo del software, como sistemas de información, sistema operativo, motores de base de datos.	Disponibilidad	Software
T47	Uso inapropiado de Instalaciones de Procesamiento de Información	Mal manejo o manipulación del entorno físico donde residen los equipos de procesamiento (Superficies, centros de cableado, datacenters)	Disponibilidad	Sitio
	Ataques intencionados			
T48	Borrado, alterado, falsificación de Logs de manera intencional	Modificación intencional y borrado de los Logs de auditoría	trazabilidad del servicio trazabilidad de los datos	Software Hardware Red
T49	Manipulación de la configuración	Fallos deliberados causados por las personas. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	Integridad Confidencialidad Disponibilidad	Software Hardware Red
T50	Suplantación de la identidad del usuario o falsificación de derechos	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	Confidencialidad Integridad	Software Red
T51	Abuso de privilegios de acceso, funciones y permisos	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	Confidencialidad Integridad	Software Hardware Red
T52	Uso no previsto o no controlado de recursos	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: Juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	Disponibilidad	Software Hardware Red
T53	Instalación y Uso de programas no autorizados o sin licencia	Utilización de aplicativos externos para fines no previstos, típicamente de interés personal. Descarga no controlada de software	Disponibilidad Integridad Confidencialidad	Software
T54	Instalación y uso de Equipos Informáticos no autorizados o sin licencia	Utilización de equipos informáticos para fines no previstos, típicamente de interés personal.	Disponibilidad Integridad Confidencialidad	Red Hardware
T55	Difusión de software malicioso	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, bank trojans, credentialed malware, back doors, keyloggers, sniffers, RAM Scraper, etc.	Disponibilidad Integridad Confidencialidad	Software ATMs
T56	[Re-]encaminamiento de mensajes y Enlaces que permanecen activos al completar comunicaciones	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe	Confidencialidad Integridad	Red Servicios
T57	Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad o confidencialidad de los datos afectados. Spoofing IP, DNS Spoofing	Integridad Confidencialidad	Software Red
T58	Acceso y uso no autorizado lógico (Hacking)	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. Hacking, SQL Injection, credenciales default, listas de acceso débiles, reglas de los firewalls débiles, robo de tokens y contraseñas	Confidencialidad Integridad	Software Hardware Red
T59	Acceso no autorizado físico	El atacante o visitante consigue acceder a las distintas áreas de la organización para extraer, manipular, dañar activos. Los visitantes o potenciales atacantes no están acompañados o identificados dentro de las áreas de la organización.	Disponibilidad Confidencialidad Integridad	Sitio Hardware Red Servicios
T60	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina "monitorización de tráfico"	Confidencialidad	Red
T61	Repudio o negación de acciones	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.	Trazabilidad del servicio	Servicios Hardware Red Información Software

T62	Interceptación de información (escucha, infiltración)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada	Confidencialidad	Red Hardware Software
T63	Modificación/Corrupción de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	Integridad	Información Software
T64	Introducción de falsa información	Inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	Integridad	Información Software
T65	Destrucción de la información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	Disponibilidad	Información
T66	Divulgación de información	Revelación de información. Revelación intencional, Exposición de contraseña, incontinencia verbal, medios electrónicos, soporte papel, etc.	Confidencialidad	Información Sitio Persona Software
T67	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. Mal manejo del software, como sistemas de información, sistema operativo, motores de base de datos.	Confidencialidad Integridad	Software
T68	Ataques por Vulnerabilidades técnicas desconocidas o para las que no existe parches	Debido a lo no instalación de parches o hot fixes, debido a que aún no existen, el software, atacantes (internos y externos)y código malicioso pueden explotar dicha vulnerabilidad	Integridad Disponibilidad Confidencialidad	Software
T69	Denegación o Pérdida del servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. La carga de trabajo es causada por ataques internos y externos.	Disponibilidad	Servicios Hardware Red Software
T70	Robo, o Retiro no autorizado de medios, equipos, documentación	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. Robo de medios y documentos impresos. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información	Disponibilidad Confidencialidad	Hardware Red Información
T71	Ataque destructivo	Vandalismo, actos de terrorismo, bomba, sabotaje, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. Explosivos, artefacto incendiario, químico, uso de armas, EMP, manipulación de Hardware	Disponibilidad	Hardware Red Sitio
T72	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.	Disponibilidad Confidencialidad	Hardware Red Sitio
T73	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos ...	Disponibilidad	Personal
T74	Extorsión, Coacción, Chantaje, soborno	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	Confidencialidad Integridad	Personal
T75	Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	Confidencialidad Integridad	Personal
T76	Errores intencionales de codificación en los programas (software)	Defectos en el código que dan pie a una operación fraudulenta por parte del atacante (Ejemplo: Puerta trasera)	Integridad Disponibilidad Confidencialidad	Software
T77	Introducción de Código no autorizado o no probado o no revisado	Actualización en el ambiente de producción de código que puede dar pie a una operación fraudulenta por parte del atacante (Ejemplo: Puerta trasera)	Integridad Disponibilidad Confidencialidad	Software
T78	Uso y/o acceso de la Red de forma no autorizada	Conexiones a la red de la organización de forma oculta y no autorizada	Confidencialidad	Red
T79	Copia No Controlada de Documentos	Copia No Controlada de Documentos	Confidencialidad	Información
T80	Copia No Controlada de información digital	Copia No Controlada de información digital	Confidencialidad	Información Software
T81	Eliminación No Controlada de Documentos. *Dumpster Diving*.	Eliminación No Controlada de Documentos.	Disponibilidad Confidencialidad	Información Software
T82	No cumplimiento o no seguimiento a procedimientos internos	Situación donde los usuarios/empleados no actúan en cumplimiento con un procedimiento.	Disponibilidad Confidencialidad Integridad	Información Servicios
T83	Ataques a sitio WEB (Comercio electrónico, Web site)	Ataques relacionados con las vulnerabilidades OWASP a sitios y aplicaciones web externas	Confidencialidad Integridad Disponibilidad	Software
T84	Incumplimiento de contratos, Incumplimiento de servicios por parte de terceros	Incumplimiento de contratos, Incumplimiento de servicios por parte de terceros	Disponibilidad	Servicios
T85	Accesos no autorizados por medios de conexión o acceso remoto a la red (teleworkers, etc.)	Accesos por RAS (Remote Access Server), VPNs (Client to site) insuficientes permitirán la conexión remota de eventuales atacantes externos	Confidencialidad	Red
T86	Mezcla de ambientes operativos, pruebas y desarrollo	Mal manejo en el ciclo de desarrollo de software que permitirá eventualmente la fuga de información y fallas en el software	Confidencialidad	Software
T87	Canales Encubiertos/Ocultos	Enlaces alternos no autorizados, medios de comunicación conectados no autorizados, fuga de información oculta en mensajes autorizados (Extracción de información de forma oculta y no autorizada por la red)	Confidencialidad	Red Software

T88	Cambios no probados y no aprobados en los sistemas de información	Cambios no probados y no a probados en los sistemas de información	Confidencialidad Disponibilidad Integridad	Software
T89	Cambios no exitosos	Cambios probados y aprobados, pero que al ser llevados a producción fallaron	Disponibilidad	Software
T90	Incapacidad de proveer evidencia	Incapacidad de proveer evidencia a investigadores, encaso de fraudes y compromisos	Trazabilidad	Software Hardware Red
T91	Publicación o entrega de información incorrecta a terceros o al público	Publicación o entrega de información incorrecta a terceros o al público, uso de redes sociales.	Confidencialidad	Personas
T92	Acceso no autorizado a código fuente	Acceso no autorizado a código fuente	Confidencialidad Integridad Disponibilidad	Información Software
T93	Cambios no probados, no controlados y no aprobados en las instalaciones físicas	Cambios no probados, no controlados y no aprobados en las instalaciones físicas	Disponibilidad	Sitio
T94	Datos de fuentes no confiables	Datos de fuentes no confiables	Integridad	Información Personas
T95	Acuerdos incorrectos o incompletos de intercambio de información con terceros	Acuerdos incorrectos o incompletos de intercambio de información con terceros	Confidencialidad	Información
T96	Recuperación o reciclaje de medios descartados	Disposición final de medios o equipos informáticos de forma incorrecta o inadecuada.	Confidencialidad	Información Hardware Software
T97	Daños causados por Pen Tests	Daños causados por Pen Tests	Disponibilidad Integridad	Información Software Hardware Red
T98	Daños causados por Proveedores de Servicio	Daños causados por Proveedores de Servicio	Disponibilidad Integridad	Información Software Hardware Red
T99	Fraude	Fraude	Confidencialidad Integridad	Información
T100	Acceso no autorizado a herramientas y Logs de auditoría	Acceso no autorizado a herramientas y Logs de auditoría	Confidencialidad Integridad	Información
T101	Scam	Es un termino anglosajón que se emplea para designar el intento de estafa a través de a un correo electrónico fraudulento (o páginas web fraudulentas) Es un tipo de Ingeniería social	Confidencialidad	Información
T102	Amenazas por usar Cloud Computing y Servicios de Hosting	Amenazas emergentes en servicios SaaS, en la cual la información es puesta en un tercero.	Confidencialidad	Información

MATRIZ DE RIESGO

Matriz de Riesgos				
	FE			
VA	3-35	3-35	3-35	36-71
	3-35	36-71	36-71	72-111
	3-35	36-71	72-111	72-111
	36-71	72-111	72-111	112-144

Rango Min	Rango Max	Nivel de Riesgo	Descripción
3	35	Riesgo Bajo	La Organización acepta este nivel de Riesgo, ya que puede tener un impacto insignificante o nulo. No Requiere atención.
36	71	Riesgo Medio	La Organización podría aceptar temporalmente este nivel de Riesgo, ya que puede tener un impacto menor. Requiere atención a mediano plazo.
72	111	Riesgo Alto	La Organización no acepta este nivel de Riesgo, ya que puede tener un impacto significativo. Requiere atención a corto plazo.
112	144	Riesgo Crítico	La Organización no acepta este nivel de Riesgo, ya que puede tener un impacto muy serio. Requiere atención Inmediata.