VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER

TEMA: PLAN DE CONTINUIDAD DE NEGOCIO APLICADO AL CENTRO DE DATOS DE LA FISCALIZACIÓN DEL PROYECTO HIDROELÉCTRICO COCA CODO SINCLAIR

AUTOR: Ing. CEVALLOS AMAGUAY JHERRY FERNANDO

DIRECTOR: Mgrt. ARROYO CHANGO, RUBÉN

OPONENTE: MSc. GÓMEZ ESTEVAN

SANGOLQUÍ

2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRIA EN EVALUACIÓN Y SISTEMAS TECNOLOGICOS

CERTIFICADO

Ing. Gómez Estevan MSc

Ing. Rubén Darío Arroyo Chango MSc.

CERTIFICAN

Que el trabajo titulado PLAN DE CONTINUIDAD DE NEGOCIO APLICADO AL CENTRO DE DATOS DE LA FISCALIZACIÓN DEL PROYECTO HIDROELÉCTRICO COCA CODO SINCLAIR, realizado por el Ing. Jherry Fernando Cevallos Amaguay, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas de la Universidad de las fuerzas armadas –ESPE.

Debido a que constituye un trabajo que aporta de forma positiva a la gestión que realiza la Asociación CFE-PYPSA-CVA-ICA, contribuyendo a la mejora continua de los servicios que ofrece al desarrollo del proyecto Hidroeléctrico Coca Codo Sinclair, motivo por el cual si recomendamos su publicación.

El mencionado trabajo consta de un empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf), Autorizan a Jherry Fernando Cevallos Amaguay a que entregue al Msc. Rubén Darío Arroyo Chango, en su calidad de director de la Carrera.

Sangolquí, Abril del 2015

Mgrt. Rubén Darío Arroyo Chango
DIRECTOR

MSc. Gómez Estevan
CODIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRIA EN EVALUACIÓN Y SISTEMAS TECNOLOGICOS

AUTORÍA DE RESPONSABILIDAD

JHERRY FERNANDO CEVALLOS AMAGUAY

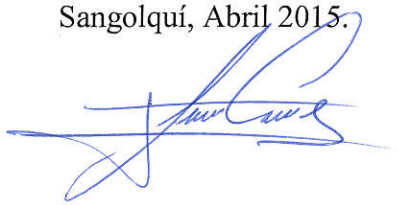
DECLARO QUE

El Trabajo de investigación denominado PLAN DE CONTINUIDAD DE NEGOCIO APLICADO AL CENTRO DE DATOS DE LA FISCALIZACIÓN DEL PROYECTO HIDROELÉCTRICO COCA CODO SINCLAIR, ha sido desarrollado respetando los derechos intelectuales de terceros, conforme las citas cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Abril 2015.



Ing. Jherry Fernando Cevallos Amaguay

AUTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRIA EN EVALUACIÓN Y SISTEMAS TECNOLOGICOS

AUTORIZACIÓN

Yo, Jherry Fernando Cevallos Amaguay

Autorizo a la Universidad de las Fuerzas Armadas – ESPE, la publicación en la biblioteca virtual de la Institución del trabajo PLAN DE CONTINUIDAD DE NEGOCIO APLICADO AL CENTRO DE DATOS DE LA FISCALIZACIÓN DEL PROYECTO HIDROELÉCTRICO COCA CODO SINCLAIR, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, Abril 2015.

Ing. Jherry Fernando Cevallos Amaguay
AUTOR

DEDICATORIA

Dedico el presente trabajo a todas las personas que me ayudaron moral y económicamente a su desarrollo, mi profunda admiración y respeto.

A mis hijos Fernanda y Adriel, quienes son mi motivación para superarme y conseguir el éxito, con el firme propósito de brindarles un futuro mejor y ser su claro ejemplo de triunfo.

A mi madre por brindarme su apoyo incondicional y formarme con valores de respeto, humildad y deseos de superación.

Al Ing. Pedro Villegas jefe del departamento de sistemas y control de software de la Asociación CFE- PYPSA-CVA-ICA por brindarme la oportunidad de desenvolverme en el ámbito profesional y permitir el desarrollo de este trabajo dentro de su departamento de labores.

AGRADECIMIENTO

Me permito expresar con profunda sinceridad las gracias a todos quienes han contribuido directa o indirectamente a la culminación del presente trabajo.

Mi agradecimiento a DIOS por darme salud y sabiduría, permitiéndome culminar esta etapa de mi vida y de esta manera crecer como ser humano y también como profesional.

A la Universidad de la Fuerzas Armadas ESPE, especialmente a los catedráticos de la Maestría de Evaluación y Auditoría en Sistemas Tecnológicos, quienes aportaron con sus conocimientos para formarme como profesional de cuarto nivel.

A mi esposa por el apoyo incondicional durante todo el transcurso de estudio de la maestría, a mis hijos por brindarme su cariño y amor, sin permitir que la distancia sea un factor de distanciamiento en los días que tenía estudio y trabajo, los cuales eran muchos.

También quiero agradecer a mis tutores: Msc. Raúl Pavón y Msc. Rubén Arroyo por compartir sus amplios conocimientos y aportaciones en el desarrollo del presente trabajo.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FÍGURAS

RESUMEN

Este trabajo se basa en el estudio del problema detectado, en la Asociación fiscalizadora del proyecto Hidroeléctrico Coca Codo Sinclair, en la cual no se cuenta con planes de continuidad de negocio. La Asociación al ser una empresa privada que se rige por sus propios reglamentos y regulaciones en cuanto funcionamiento y manejo de la seguridad de la información, por lo tanto es de su competencia y responsabilidad implementar planes que aseguren la continuidad de los procesos ante posibles interrupciones. Es por esta razón la propuesta de un plan de continuidad de negocios basados en la norma ISO 22301 -2012, que permite enfrentar desastres que puedas provocar discontinuidad en las operaciones y servicios que presta en centro de datos de la Asociación. El estudio realizado, así como el modelo de propuesta planteado demuestra que el plan de continuidad de negocios puede implementarse y operarse.

PALABRAS CLAVES:

PLAN DE CONTINUIDAD DE NEGOCIO
SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIOS
NORMA ISO 22301
SEGURIDAD SOCIAL
SEGURIDAD DE LA INFORMACIÓN

ABSTRACT

This work is based on the study of the problem identified in the audit Association Coca Codo Sinclair hydroelectric project in which you do not have business continuity plans. The Association being a private company which is governed by its own rules and regulations regarding the operation and management of information security, so it is your duty and responsibility to implement plans to ensure the continuity of proceedings before any interruptions.

This is why a proposed plan business continuity based on ISO 22301 -2012, which can cope with disasters that can cause disruption in operations and services provided in the data center of the Association. The study and the proposed model raised demonstrates that business continuity plan can be implemented and operated.

KEYWORDS:

BUSINESS CONTINUITY PLAN
BUSINESS CONTINUITY MANAGEMENT SYSTEM
STANDARD ISO 22301
SOCIETAL SECURITY
INFORMATION SECURITY

PLAN DE CONTINUIDAD DE NEGOCIO APLICADA AL CENTRO DE DATOS DE LA FISCALIZACIÓN DEL PROYECTO HIDROELÉCTRICO COCA CODO SINCLAIR.

El presente trabajo se basa en el desarrollo plan de continuidad de negocio aplicado al centro de datos de la fiscalización del proyecto hidroeléctrico Coca codo Sinclair, A fin de que pueda ser acogido por esta Asociación para asegurar la información y con ello la continuidad de los procesos que sostienen las actividades de servicios de la Asociación.

La Investigación ha sido estructurada en cinco capítulos.

En el capítulo I, se analizan los antecedentes investigativos planteando el tema y problema a investigar, se formula el problema, se justifica y se detalla la importancia del mismo, se plantea el Objetivo general y los objetivos específicos.

En el capítulo II, se analiza la fundamentación filosófica de varios autores sobre el tema tratado, así mismo se sustenta atreves del marco conceptual con la definición de términos básicos que respaldan la investigación y el planteamiento de los objetivos.

En el capítulo III, Se plantea la metodología a utilizar, defendiendo bajo criterios las herramientas adecuadas para su utilización en la recolección de información y métodos a emplearse.

En el capítulo IV, se describe la situación actual de la Asociación, evaluación de criterios liderazgo, planificación, se aplica las herramienta de recolección de información la entrevista y encuesta y el procesamiento de los resultados, identificación de los principales riesgos naturales y a su análisis respectivo.

En el capítulo V, contiene el desarrollo de la gestión de continuidad de negocios utilizando la norma seleccionada, conociendo el contexto de la Asociación, estructura orgánica, análisis de impacto con la descripción de los procesos e identificación de las actividades críticas, evaluación de riesgos, definiendo así el modelo y la propuesta con el desarrollo de los planes de continuidad, de evacuación y recuperación con estrategias y políticas establecidas.

En el capítulo VI, se detallan las conclusiones y recomendaciones del presente trabajo, basadas en los objetivos propuestos.

CAPITULO I

INTRODUCCIÓN

La información es el activo más importante que puede poseer una organización, se debe mantener disponible, íntegra, fiable y oportuna, para llevar adelante sus negocios permitiendo a la organización competir en el mercado, aumentando su credibilidad y competitividad.

En la actualidad es inaceptable que una organización no cuente con un sistema de información, por pequeño que sea, por lo tanto deben existir métodos que lo resguarden de manera física y lógica. Los sistemas almacenan gran cantidad de datos siendo vulnerables a una variedad de tumultos, que parten desde leves interrupciones como: falta de dispositivos de almacenamiento, cortes al suministro eléctrico, etc. La pérdida total que puede proceder de diferentes fuentes como acciones violentas o desastres naturales.

Considerables vulnerabilidades pueden ser mitigadas a través soluciones operativas o de técnicas de gestión, es prácticamente imposible eliminar por completo todos los riesgos, por este motivo las tecnologías de información requieren una solución a la necesidad de proteger sus recursos y dar continuidad a las operaciones primordiales. Como respuesta a esto se tiene las normas internacionales ISO 22301 y el estándar BCLS 2000 de la organización DRI International, el cual rige sus principios en tomar decisiones correctas al momento de sufrir un desastre, de tipo natural o alguno imprevisto.

La normas ISO 22301 (Gestión de Continuidad de Negocio) ocupa un espacio determinante en tecnologías de información (TI), siendo un pilar primordial al momento de cumplir sus objetivos, obteniendo como resultados la reduciendo riesgos con la definición de niveles de seguridad de acuerdo a los estándares y mejores prácticas.

"El Proyecto Hidroeléctrico Coca Codo Sinclair, de 1500 Mv declarado de Alta Prioridad Nacional por el Consejo Nacional de Electricidad, CONELEC, mediante Resolución No. 001/08, tomada en sesión realizada el 31 de enero de 2008"., Por esta razón es significativo la recopilación de información diaria de actividades, ya que un futuro será necesaria su revisión para posibles auditorías y procedimientos en general.

La presente investigación busca definir políticas de planificación de contingencia, análisis de impacto al negocio, identificar controles preventivos, desarrollo de estrategias de recuperación y plan de continuidad de negocio que servirá de guía para la implementación en actividades de Fiscalización y Gerenciamiento de grandes proyectos Hidroeléctricos (generación mayor a 1000 Mv)

1.1 Antecedentes

La Asociación fiscalizadora CFE-PYPSA-CVA-ICA se encuentra laborando en el Ecuador, desde el año 2011. Al principio sus trabajos se centralizaron en el campamento "San Rafael", perteneciente al Proyecto Hidroeléctrico Coca Codo Sinclair EP, ubicando allí el servidor principal que contiene información relevante de todos los frentes de trabajo, conjuntamente con los softwares de control de proyecto que permite llevar un registro de las actividades realizadas y el cronograma. En la actualidad se encuentra trabajando en el campamento con nombre "La Loma" desde junio del 2014, teniendo servidores que contienen software de control de proyectos, software de cronograma de proyecto, aplicaciones internas y unidades de red compartidas. Dicho campamento se encuentra a pocos kilómetros de distancia del conocido "Volcán El Reventador", siendo este el principal riesgo inherente por su constante actividad.

El Centro de Datos de la Asociación se encuentra vulnerable debido a la zona geográfica donde está albergada, se tiene como acontecimientos naturales anteriores, el terremoto del año 1987 el cual destruyó el campamento de la empresa Francesa "Rodio", que centralizaba sus trabajos de estudios de factibilidad del Proyecto

Hidroeléctrico Coca Codo Sinclair, teniendo grandes pérdidas humanas y la pérdida en la totalidad de los recursos y activos del mencionado campamento que se ubicaba en el mismo lugar que actualmente labora la Asociación.

1.2 Problema

Es importante que en una organización existan los recursos necesarios para la continuidad de un negocio como son: personal competente, servicios de soporte, recursos de formación, toma de conciencia en la organización, comunicaciones, control de la información, control de documentación, prevención de riesgos y control de riesgos. Estas son observaciones no contempladas por la organización encargada de la fiscalización del Proyecto Hidroeléctrico Coca Codo Sinclair, por lo tanto no se ha realizado ninguna evaluación de riesgos ni de impacto al negocio, consecuentemente no se ha aplicado ningún procedimiento ni estrategia de continuidad de negocios con capacidad de dar respuestas de recuperación ante un posible daño o pérdida de la misma, además no cuenta con: políticas, estrategias, valores y objetivos de gestión de riesgos vinculados a la organización, tampoco existe liderazgo y compromiso de la dirección para tomar acciones, vigilar y dotar de recursos necesarios para la organización, a fin de garantizar la seguridad de la información.

Las instalaciones de la organización se encuentra geográficamente en un sitio propenso a desastres naturales como son: la erupción del Volcán el Reventador, emanación de ceniza, sismos, inundación por crecida del río Coca, deslizamientos en masa, asentamientos, derrames de petróleo y gasolinas, lo que corresponde, es estar preparados para minimizar el impacto que generan las posibles interrupciones; por lo tanto, es vital, plantear un sistema de gestión de continuidad de negocios que permita crear una organización más resistente, con planificación y control, con capacidad de responder en forma efectiva y proteger los intereses, preservando y mejorando su imagen corporativa, reduciendo los costos globales, asegurando el cumplimiento de las actividades y creando un clima de confianza con los empleados, proveedores y cliente.

1.3 Justificación

En la actualidad las organizaciones están expuestas a riesgos constantes que se presentan en diferentes situaciones, causando grandes consecuencias, esto por no tener una organización definida y encaminada en prevenir y enfrentar un posible desastre; por tal razón, en la presente investigación se elaborará un modelo de gestión de continuidad de negocios aplicada al centro de datos de la fiscalización del Proyecto Hidroeléctrico, se dispondrá de un Plan General que cuente con: políticas, estrategias, procedimientos y liderazgo en riesgos, para con ello, minimizar el impacto, ante las posibles interrupciones, respondiendo con capacidad y eficiencia, y proteger los activos de la organización.

La necesidad de contar con un plan de continuidad de negocios aplicado a la fiscalización del proyecto hidroeléctrico es justificado por la ubicación geográfica, en la cual se encuentra localizado, pues se trata de una zona de constantes riesgos a causa de desastres naturales que a menudo ocurren en el sector, ya que alrededor del campamento donde permanece toda la información generada del proyecto, se encuentra cerca el volcán activo El Reventador; el río Coca que puede causar inundaciones ante una creciente; el Oleoducto y Poliducto que podrían ocasionar derrames de petróleo y combustibles y por último las montañas inestables que por las continuas lluvias suelen generar deslizamientos de tierra; así como los asentamientos humanos aledaños al Proyecto.

Debido a que la organización Fiscalizadora, no cuenta con un estudio ni evaluación de riesgos e impactos, tampoco ha implementado políticas y procedimientos para enfrentar un posible riesgo, esto obliga a que disponga de un modelo de gestión de continuidad de negocios que sea aplicable para precautelar la información.

1.4 Importancia

La importancia de desarrollar un plan de continuidad de negocios es salvaguardar al personal que labora en la fiscalizadora, minimizar la confusión y permitir

decisiones acertadas en tiempo de crisis, así como, reducir la dependencia de personal específico, minimizar la pérdida de datos, mantener una buena imagen pública y su reputación; igualmente, facilitar la recuperación pertinente de las funciones críticas de la fiscalización en el departamento de sistemas y control del software de forma segura y confiable, permitiendo establecer un adecuado protocolo de comunicaciones internas y externas.

La investigación y desarrollo de este Plan de continuidad de negocios que puede ser aplicado a otras organizaciones que realizan fiscalización de proyectos hidroeléctricos en el mundo, adaptando y ajustando a su realidad y necesidades, servirá de modelo estandarizado que permitirá preservar los intereses de la organización, reduciendo riesgos, costos y tiempo de inactividad, al mismo tiempo que existirá mayor eficacia operativa, protección de información almacenada, mejorará la seguridad global de la organización y evitará acciones derivadas de la responsabilidad organizacional.

1.5 Objetivos

Objetivo general

Elaborar un Plan de Continuidad de Negocio aplicada al Centro de Datos de la fiscalización del proyecto hidroeléctrico Coca Codo Sinclair.

Objetivos específicos

a) Investigar y desarrollar el marco teórico, en base a la normativa mundial existente.

b) Desarrollar la metodología de investigación a aplicar.

c) Determinar el diagnóstico situacional de la organización encargada de la fiscalización de un proyecto hidroeléctrico.

d) Desarrollar de un plan de continuidad de negocios y procedimientos de recuperación de desastres.

e) Conclusiones y recomendaciones.

CAPITULO II

MARCO TEÓRICO

2.1 Introducción a la gestión de continuidad de negocios

2.1.1 Plan de continuidad de negocios

(Bureau Veritas, 2012), Catálogo y documentos de Continuidad de Negocio, La definición de Continuidad de Negocio, es un proceso de gestión holístico que identifica las amenazas potenciales de una organización y los impactos que pueden causar en las operaciones del negocio si esas amenazas se materializan, Además proporciona un marco de trabajo para construir una organización más resistente con capacidad para responder de forma efectiva y proteger los intereses de las partes interesadas clave, su reputación, imagen de marca y actividades de valor añadido.

Un Plan de Continuidad de Negocio, está orientado en priorizar las operaciones críticas del negocio, viéndose como una herramienta de mitigación de riesgos para garantizar el funcionamiento de la organización y su continuidad, haciendo frente a sucesos inadvertidos, después de un suceso no planificado que puede provenir de varias fuentes como naturales o acciones violentas.

El rol de la continuidad de negocio (BCM por sus siglas en inglés) se basa en cómo se prepara una organización para futuros acontecimientos inesperados que puedan poner en peligro a su misión. Provee un procedimiento para construir una organización más resistente con capacidad para responder de forma efectiva ante los escenarios viables, conteniendo desde incidentes particulares como incendios, inundaciones, terremotos; además sucesos de carácter territorial, nacional o internacional incluso incidentes tales como pandemias.

Un Plan de Continuidad de Negocio se compone de varias etapas que comienzan con un análisis de los procesos que componen la organización. Este análisis servirá para prevalecer qué procesos son críticos y establecer una estrategia de recuperación ante un desastre. Por cada proceso que sea identificado se establecerá un control que permita continuar con la actividad empresarial en caso de una interrupción.

La razón principal de implementar un plan de continuidad de negocio, es enfrentar positivamente las oportunidades y amenazas que son siempre concurrentes, pudiendo desarrollarse, surgir nuevas o eclipsar, lo esencial es saber dónde ubicarlas, las organizaciones deben estar en constante alerta y orientarse en las necesidades, para con esto mantener la identidad de su organización. Con los argumentos mencionados las acciones enfatizadas al momento de hablar de Continuidad de Negocio son:

- Estructurar el plan de continuidad de negocio, alineado a las metas de la organización.
- Regirse en el marco de referencia de la norma internacional ISO 22301, Gestión de Continuidad de Negocio.
- Regirse en el estándar BCLS 2000 de la organización DRI International.
- Realizar una Evaluación de Riesgos.
- Identificar procesos críticos de las operaciones y asegurar SLA (Acuerdos de Nivel de Servicios).
- Examinar la garantía de las políticas y procedimientos, demostrar y ser optimizados
- Establecer procesos de revisión continua.

2.1.2 La Norma ISO 22301

2.1.2.1 Definición ISO 22301

(Norma ISO 22301, 2012) Sistemas de gestión de la continuidad del negocio. Seguridad de la sociedad, es la primera norma internacional para la Gestión de la Continuidad del Negocio y ha sido desarrollada para ayudar a las organizaciones a minimizar el riesgo de interrupciones. Sustituye a la norma Británica BS25999, Norma para la gestión del plan de continuidad de negocio, y que es reemplazada por la norma internacional ISO 22301.

(Norma ISO 22301, 2012) La norma ISO 22301 es una norma que puede ser utilizada por las organizaciones de todos los tamaños y tipos. Estas organizaciones serán capaces de obtener la certificación acreditada según esta norma y así demostrar a los legisladores, reguladores, clientes, posibles clientes y otras partes interesadas

que se adhieren a las buenas prácticas en (GCN). La norma ISO 22301 también permite al administrador de la continuidad del negocio demostrar a la alta dirección que se ha cumplido con una norma reconocida mundialmente.

(Norma ISO 22301, 2012) Mejora la organización pro activa de resistencia contra la interrupción de su capacidad de lograr sus objetivo clave, además proporciona un método ensayado para restaurar la capacidad de una organización para garantizar el suministro de sus productos y servicios después de una interrupción, proporcionando una capacidad demostrada para gestionar una interrupción del negocio y proteger la reputación de la organización en conformidad con las necesidades y los requisitos de las partes interesadas.

ISO 22301 es la segunda norma de sistemas de gestión publicada que ha adoptado la nueva estructura de alto nivel y el texto normalizado acordado en ISO. Esto garantizará la coherencia con todas las normas del sistema de gestión futuras y revisadas y para hacer un uso más fácil e integrarse con las normas: ISO9001 (calidad), ISO14001 (ambiental) e ISO/IEC 27001 (seguridad de la información).

2.1.2.2 Vinculación Círculo de Deming.

La principal herramienta para la mejora continua en las organizaciones es el círculo de Deming, una secuencia lógica de cuatro pasos que se deben llevar a cabo consecuentemente: planificar, hacer, verificar y actuar, que combinados con las principales etapas de gestión de continuidad de negocios permite comprender la organización, definir la estrategia, desarrollar e implementar una respuesta. ISO 22301 emplea el modelo Plan-do-Check-Act (PDCA) para organizar el estándar de la siguiente manera:

- **Planificar**.- Clausulas 4, 5, 6 y 7 excepto la planificación de Gestión de continuidad
- **Hacer.-** Cláusula 8 excepto el establecimiento de la Gestión de continuidad
- **Verificar.-** Cláusula 9 excepto la evaluación de la Gestión de continuidad
- **Actuar**.- Cláusula 10 excepto la mejora de la Gestión de continuidad.

La Figura 1. Muestra esquemáticamente la estructura de vinculación de Deming con la Norma 22301.

Figura 1. Proceso de la Gestión de Continuidad de Negocios.
Fuente: (Dexconsultores NTC ISO 22301:2012, 2012)

ISO 22301 especifica los requisitos para planificar, establecer, implementar, operar, supervisar, revisar, mantener y mejorar continuamente un sistema de gestión de continuidad de negocio para prepararse, responder y recuperarse de los eventos perturbadores que puedan surgir.

Figura 2. Ciclo PDCA (Planificar, Hacer, Verificar y Actuar)
Fuente: (Dexconsultores NTC ISO 22301:2012, 2012)

2.1.2.3 Cláusulas Norma ISO 22301

Según (Stefan & Dave, 2012) La norma se divide en 10 cláusulas principales, comenzando con el alcance, referencias normativas, y los términos y definiciones. Le siguen a éstos los requisitos de la norma y las siguientes son las cláusulas claves: (Stefan & Dave, 2012)

Cláusula 4.- Contexto de la organización, según (Stefan & Dave, 2012), el primer paso consiste en conocer la organización, tanto las necesidades internas como externas, y establecer límites claros para el alcance del sistema de gestión. En particular, esto requiere que la organización entienda las necesidades de las partes interesadas pertinentes, tales como reguladores, clientes y personal. En especial, comprende los requisitos legales y reglamentarios aplicables. Esto permite determinar el alcance del sistema de gestión de la continuidad del negocio y alcanzar los resultados esperados, tales como: (Stefan & Dave, 2012)

- Las actividades de la organización, sus funciones, servicios, productos, sociedades, cadenas de suministros, relaciones con las partes interesadas y el impacto potencial relacionado con un incidente que genere una interrupción.
- vínculos entre la política de continuidad de negocio y los objetivos de la organización y otras políticas, incluyendo, la estrategia de gestión de riesgos globales
- El apetito por el riesgo de la organización.
- las necesidades y expectativas de las partes interesadas relevantes.
- leyes, regulaciones y otros requisitos aplicables, a los cuales la organización está suscrita.

Figura 3. Cláusula 4, Contexto de la organización
Fuente: **(Professional Evalution and Certification Board, 2012)**

Identificar el alcance del SGCN, tomando en cuenta los objetivos estratégicos de la organización, sus productos y servicios claves, su tolerancia al riesgo y cualquier obligación reglamentaria, contractual o de sus partes interesadas, también forma parte de esta cláusula.

Cláusula 5.- Liderazgo, según (Stefan & Dave, 2012), La ISO 22301 hace especial hincapié en la necesidad de un liderazgo adecuado en la gestión continuidad de negocio. Esto es para que la alta dirección asegure que se proporcionen los recursos necesarios, establece la política y nombra a las personas que implementan y mantienen la continuidad de negocio. (Stefan & Dave, 2012)

La alta dirección debe demostrar un compromiso continuo con el Sistema de Gestión de Continuidad de Negocio. A través de su liderazgo y acciones, la dirección puede crear un ambiente en el cual distintos miembros del personal estén completamente involucrados y el sistema de gestión pueda funcionar de manera eficaz en sinergia con los objetivos de la organización. La dirección es responsable de:

- Asegurar que el Sistema de Gestión de Continuidad de Negocio es compatible con la dirección estratégica de la organización;
- Integrar las obligaciones del Sistema de Gestión de Continuidad de Negocio en las técnicas de negocios de la organización (Alberto Alexander Servat, 2012);
- Proveer los recursos necesarios para el Sistema de Gestión de Continuidad de Negocio;
- Comunicar la importancia de la gestión de continuidad de negocio eficaz;
- Asegurar que el Sistema de Gestión de Continuidad de Negocio alcanza sus resultados esperados;
- Dirigir y apoyar la mejora continua;
- Establecer y comunicar la política de continuidad de negocio;
- Asegurar que los objetivos y planes del Sistema de Gestión de Continuidad de Negocio se establecen;

- Asegurar que las responsabilidades y autoridades, para las funciones relevantes, se asignen.

Cláusula 6.- Planificación, Según (Stefan & Dave, 2012) Requiere que la organización identifique sus riesgos para la implementación del sistema de gestión y establezca los objetivos y criterios claros que se pueden utilizar para medir su éxito. (Stefan & Dave, 2012)

Esta es una etapa crítica en la que se establecen objetivos estratégicos y principios para la orientación del Sistema de Gestión de Continuidad de Negocio en su totalidad. Los objetivos del Sistema de Gestión de Continuidad de Negocio son una expresión del propósito de la organización para el tratamiento de los riesgos identificados y/o para cumplir con los requisitos de las necesidades de la organización. Los objetivos de la continuidad de negocio deben:

- Ser consistentes con la política de continuidad de negocio;
- Tomar en cuenta el nivel mínimo de productos y servicios que es aceptable para que la organización alcance sus objetivos (Alberto Alexander Servat, 2012);
- Ser medibles;
- Tomar en cuenta requisitos aplicables;
- Ser controlados y actualizados, según sea apropiado.

Cláusula 7.- Soporte, (Stefan & Dave, 2012), dado que los recursos son necesarios para la implementación, introduce el importante concepto de competencia. Para tener éxito en la continuidad del negocio, se debe contar con las personas con los conocimientos, las habilidades y la experiencia adecuada, para que contribuyan al sistema gestión continuidad de negocio y respondan a los incidentes cuando éstos se producen. También es importante que todo el personal esté consciente de su propio papel en la respuesta a incidentes y esta cláusula se encarga de todas estas áreas. (Stefan & Dave, 2012)

La gestión diaria de un sistema de gestión de la continuidad de negocio, se basa en el uso de recursos apropiados para cada actividad. Estos recursos incluyen personal competente en base a formaciones y servicios de soporte, toma de conciencia y comunicación pertinentes (y demostrables), esto debe ser apoyado por información documentada adecuadamente gestionada.

Las comunicaciones, tanto internas como externas, deben ser consideradas en esta área, incluyendo su formato, contenido y el momento oportuno de estas comunicaciones.

Los requisitos para la creación, actualización y control de la información documentada, también se especifican en esta cláusula.

Cláusula 8.- Operaciones, Según (Stefan & Dave, 2012), esta sección contiene el cuerpo principal de conocimientos específicos de continuidad del negocio. La organización debe llevar a cabo el análisis de impacto en el negocio para entender cómo su negocio se ve afectado por una interrupción y cómo esto cambia con el tiempo. La evaluación de riesgos busca entender los riesgos para el negocio de una manera estructurada e informar de éstos en el desarrollo de la estrategia de continuidad del negocio, esta cláusula incluye: (Stefan & Dave, 2012)

- **Análisis de impacto en el negocio:** Según (Professional Evalution and Certification Board, 2012), Esta actividad permite que una organización identifique los procesos críticos que apoyan a sus productos y servicios claves, las interdependencias entre procesos y recursos requeridos para operar los procesos en un nivel mínimamente aceptable**.**

Figura 4. Cláusula 8, Análisis de Impacto al Negocio
Fuente: (Professional Evalution and Certification Board, 2012)

Evaluación de riesgos: La norma ISO 22301 propone referirse a la norma ISO 31000 para implantar el proceso. Según (Professional Evalution and Certification Board, 2012), la meta de este requisito es establecer, implantar y mantener un proceso formal documentado de valoración de riesgos que identifique, analice y evalúe sistemáticamente el riesgo de incidentes que generen interrupciones en la organización.

- **Estrategia de continuidad de negocio:** Una vez que los requisitos se han establecido a través del análisis de impacto en el negocio y la evaluación de riesgos, las estrategias pueden ser desarrolladas para identificar disposiciones que permitan que la organización proteja y recupere actividades críticas, basadas en la tolerancia de riesgo organizacional y dentro de objetivos de tiempo de recuperación definidos. (Professional Evalution and Certification Board, 2012)

  La experiencia y las buenas prácticas indican claramente, que las previsiones tempranas de una estrategia global de Gestión de Continuidad de Negocio, aseguran que las actividades de Gestión de Continuidad de Negocio estén alineadas y apoyen la estrategia global de negocios de la organización. La estrategia de continuidad de negocios debe ser un componente integral de la estrategia corporativa de la institución.

- **Procedimientos de continuidad de negocio:** La organización debe documentar los procedimientos para asegurar la continuidad de las actividades y la gestión de un incidente que genere una interrupción. Los procedimientos deben:

  - establecer un protocolo adecuado de comunicaciones internas y externas;
  - ser específicos en relación a los pasos inmediatos a ser tomados durante una interrupción;

- ser flexibles para responder a amenazas no anticipadas y a situaciones internas y externas versátiles;
- enfocarse en el impacto de eventos que puedan potencialmente interrumpir operaciones;
- ser desarrollados bajo hipótesis establecidas y análisis de interdependencias; y;
- ser efectivos en minimizar las consecuencias a través de la implantación de estrategias de mitigación adecuadas.

➲ **Ejercicios y pruebas:** Según (Jimenéz, 2007) para asegurar que los procedimientos de continuidad de negocio son consistentes con sus objetivos de continuidad de negocio, las organizaciones deben hacer pruebas regularmente. Los ejercicios y las pruebas son procesos de validación de planes y procedimientos de la continuidad de negocio para asegurar que las estrategias seleccionadas son capaces de proveer resultados de respuesta y recuperación dentro de plazos acordados con la gerencia. (Jimenéz, 2007)

Tipo de ejercicio	¿Qué es?	Beneficios	Desventajas
Lista de verificación	Distribuye planes para revisión	Asegura que el plan cubra todas las actividades	No está dirigido hacia la eficacia
Recorrido estructurado	Mirada detallada a cada paso del Plan de Continuidad de Negocio (PCN)	Asegura que las actividades planificadas estén descritas correctamente en el PCN	Valor bajo al probar las capacidades de respuesta
Simulación	Escenario para representar los procedimientos de recuperación	Sesión práctica	Cuando los subconjuntos son muy distintos
Paralelo	Prueba total, pero procesamiento principal no es interrumpido	Asegura un alto nivel de confiabilidad sin interrumpir las operaciones normales	Costoso ya que todo el personal se involucra
Interrupción total	El desastre es replicado al punto de interrumpir las operaciones normales	Prueba más confiable del PCN	Arriesgado

Figura 5. Cláusula 8, ejercicios y pruebas
Fuente: (Professional Evalution and Certification Board, 2012)

Cláusula 9.- Evaluación, Según (Stefan & Dave, 2012)para cualquier sistema de gestión, es esencial evaluar el desempeño contra el plan. La ISO 22301 por lo tanto requiere que la organización seleccione y se mida a sí misma contra las métricas de

rendimiento adecuadas. Se deben llevar a cabo auditorías internas y se exige que la dirección revise y actué sobre estas revisiones periódicas para mejorar su operación: (Stefan & Dave, 2012)

- seguimiento de la medida en la cual la política, objetivos y metas de continuidad de negocio son cumplidos;
- medición del desempeño de los procesos, procedimientos y funciones que protegen las actividades priorizadas;
- seguimiento de la conformidad con esta norma y con los objetivos de la continuidad de negocio;
- seguimiento histórico de evidencia de desempeño deficiente del SGCN;
- realización de auditorías internas a intervalos planificados; y
- evaluación de todo lo anterior en las revisiones por la dirección, a intervalos planificados.

Cláusula 10.- Mejora, Según (Stefan & Dave, 2012) no existe un sistema de gestión perfecto desde el principio, y las organizaciones y sus entornos están cambiando constantemente. La cláusula 10 define las acciones a tomar para mejorar las SGCN en el tiempo y asegurar que se aborden las acciones correctivas derivadas de las auditorías, revisiones, ejercicios y así sucesivamente. (Stefan & Dave, 2012)

La mejora continua puede ser definida como todas las acciones, realizadas a lo largo de la organización, para aumentar la eficacia, cumplir objetivos y la eficiencia de la proporción costo/beneficio, el cual optimiza los procesos y controles de seguridad para brindar más beneficios a la organización y a sus partes interesadas. Una organización puede mejorar continuamente la eficacia de su sistema de gestión a través del uso de la política de continuidad de negocio, los objetivos, los resultados de auditorías, el análisis de eventos controlados, los indicadores, las acciones correctivas y preventivas y la revisión por la dirección.

2.1.3 Las 10 prácticas profesionales para la planificación de continuidad de Negocios.

Según (DRI International, 2014), Las Prácticas Profesionales son un cuerpo común de conocimientos mundialmente aceptado en la profesión de continuidad de negocios que resaltan habilidades específicas, tareas, procedimientos o actividades que comúnmente se caracterizan.

Estas Prácticas han sido desarrolladas por el DRI International, a continuación lo podemos observar en la Figura 6.

Figura 6. Las 10 Prácticas Profesionales para Planificadores de Continuidad del Negocio
Fuente: (DRI International, 2014)

2.2 Evaluación y control de riesgos.

Es importante determinar los riesgos que pueden afectar en forma adversa a la organización y sus recursos (personas, instalaciones, tecnologías) debido a una interrupción del negocio, de igual manera determinar la pérdida potencial que pueden causar los riesgos y los controles necesarios para evitar o mitigar los efectos y completar un análisis de costo-beneficio para justificar la inversión en los controles necesarios para mitigar el efecto de los riesgos. (DRI Internacional, Enero 2014)

Según (Jimenéz, 2007) “El objetivo de un Análisis de Riesgos es poner de manifiesto aquellas debilidades actuales que por su situación o su importancia pueden poner en marcha, antes de lo deseable, el Plan de Recuperación de Negocio.

El Análisis de Riesgo debe centrarse en los procesos o actividades del negocio que se han considerado críticos, aunque también puede extenderse a aquellos que no lo son" (Jimenéz, 2007)

En la siguiente figura 9 se podrá visualizar el rol de los profesionales para una evaluación y por qué se debe realizar (ISACA, 2012):

- Proporcionar prioridad a la planificación y distribución de los recursos
- Identificar y mitigar exposiciones.
- Identificar las amenazas, riesgos y vulnerabilidades en la cadena de desastre.

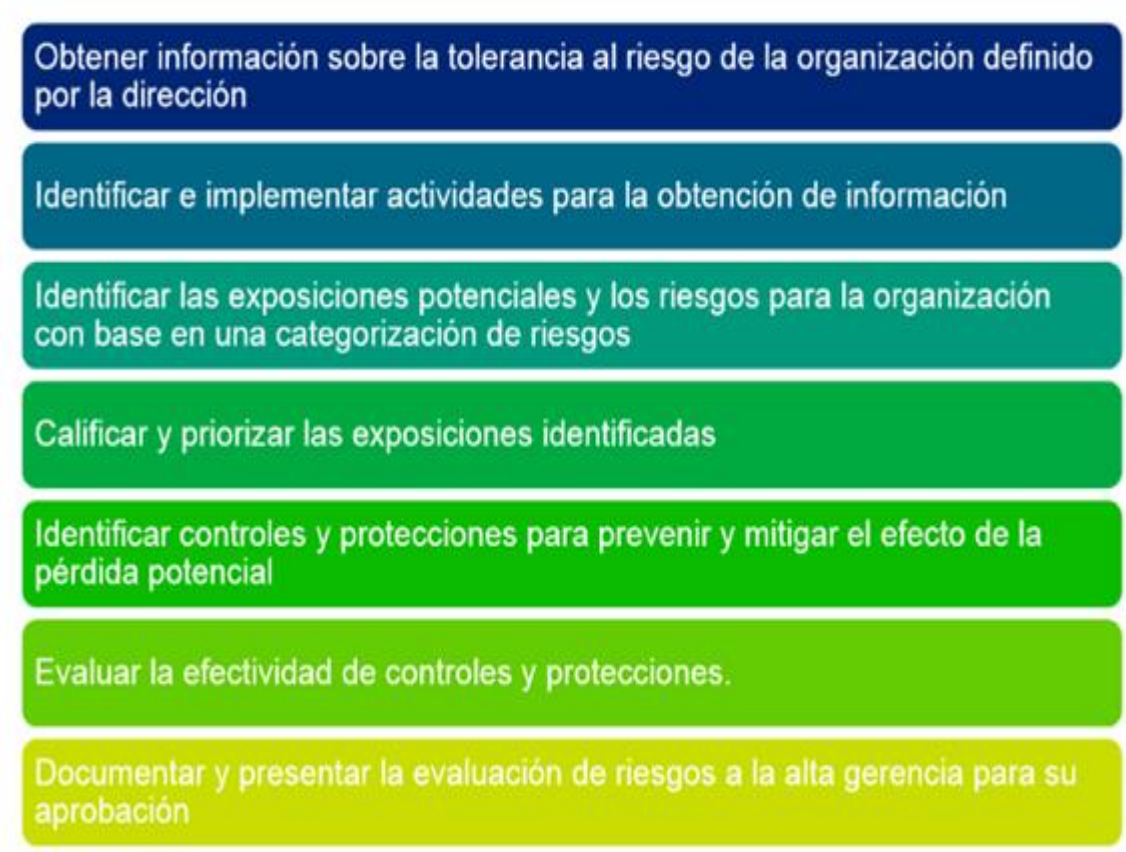


Figura 7. Rol del profesional en una evaluación
Fuente: (DRI International, 2014)

Para obtener información sobre la tolerancia al riesgo de la organización definido por la dirección se debe;

- Entrevistar al área legal y otras áreas pertinentes de la organización para

identificar los asuntos relevantes relacionados con riesgos. (ISACA, 2012)

- Trabajar con la dirección para seleccionar un modelo de análisis de costo-beneficio apropiado.
- Establecer los criterios de medición para cuantificar la tolerancia al riesgo.
- Determinar los métodos para obtener información, fuentes y la credibilidad. (ISACA, 2012)

Para Identificar e implementar actividades para la obtención de información se debe;

- Desarrollar una estrategia para obtener información.
- Crear métodos para recolección y distribución de información a lo largo de toda la organización.
- Establecer un proceso para revisión y análisis de documentación.

En la siguiente Figura.10 se puede conocer de una manera más detallada que podemos hacer con los riegos que se presenten.

Figura 8. Qué hacer con los riegos
Fuente: (DRI International, 2014)

Según (ISACA, 2012), hay razones para preocuparse de los riesgos la continuidad de negocios se preocupa de los riesgos porque;

- Es mucho más fácil prevenir un desastre que recuperarse de uno.

- Ayudarle a determinar dónde utilizar su presupuesto de mitigación.
- Instalar controles apropiados para resolver los problemas menores antes de que se conviertan en desastres. (ISACA, 2012)

De igual manera hay que Evaluar la efectividad de los controles y protecciones, el flujo de comunicaciones relacionadas con la seguridad con otras áreas internas y proveedores de servicio externos, los acuerdos de nivel de servicio de continuidad de negocios con proveedores y con organizaciones de clientes y grupos internos y externos de la organización. (ISACA, 2012)

Observar los escenarios de desastre basados en los riesgos severos en magnitud, ocurriendo en el peor momento y escenario posible y resultando en un deterioro grave de la habilidad de la organización para hacer negocios, y asesorar sobre medidas de seguridad viables y costo efectivas requeridas para prevenir o reducir riesgos y exposiciones relacionados con la seguridad, a continuación podremos visualizar el esquema del análisis de riesgos. (ISACA, 2012)

Figura 9. Esquema del análisis de riesgos
Fuente: (Jimenéz, 2007)

Las metas para este paso del proceso incluyen:

- Presentar las hallazgos de la evaluación de riesgos
- Determinar los próximos pasos para iniciar el desarrollo de las estrategias de continuidad de negocios. (ISACA, 2012)

2.3 Análisis de Impacto al negocio.

Según (ISACA, 2012), para este análisis es necesario identificar los impactos que resultan de las interrupciones del negocio que puedan afectar a la organización y las técnicas que pueden ser utilizadas para cuantificar y calificar dichos impactos, además hay que identificar funciones críticas con base en el tiempo, sus prioridades de recuperación e interdependencias, con el propósito de que los tiempos objetivos de recuperación puedan ser establecidos y aprobados. (ISACA, 2012)

"Los incidentes causan un impacto dentro de la organización, que también deberá tomarse en cuenta a la hora de calcular los riesgos. La valoración del impacto puede realizarse de forma cuantitativa, estimando las pérdidas económicas, o de forma cualitativa, asignando un valor dentro de una escala (p.e. alto, medio, bajo)". (Jimenéz, 2007)

Por ejemplo, el robo de información confidencial de la compañía puede causar un impacto alto si ésta cae en malas manos. En otro caso podemos estimar las pérdidas económicas de equipos tangibles valorando el coste de reposición y puesta en marcha.

Según (ISACA, 2012) para ello se debe:

- Establecer el proceso y metodología del Análisis de Impactos al Negocio.
- Planificar y coordinar la obtención de datos y su análisis
- Preparar y presentar el reporte a la gerencia

Según (ISACA, 2012), los objetivos del análisis de impacto al negocio son:

- Determinar la criticidad de las funciones y procesos de la empresa
- Determinar los períodos críticos de las funciones y procesos de la empresa
- Identificar interdependencias entre las funciones de negocio y los procesos
- Evaluar el impacto de las interrupciones potenciales,
- Identificar los recursos críticos necesarios para una recuperación,
- Determinar los Objetivos de Recuperación para cada función de negocio y

para los procesos,

- Determinar los requerimientos legales y regulatorios
- Identificar los registros vitales. (ISACA, 2012)

En la siguiente Figura 10, podremos visualizar como se debe planificar y coordinar la obtención de datos y su análisis.

Figura 10. Coordinar la obtención de datos y su análisis.
Fuente: (DRI International, 2014)

Para el análisis de los datos se requiere identificar las funciones de negocio, determinar el impacto potencial de un incidente, estimar la pérdida potencial de negocio, determinar los marcos de tiempos de recuperación, obtener los requerimientos para la recuperación.

2.3.1 Identificar las funciones de negocio

Se requiere obtener y revisar los organigramas, identifique todas las áreas principales de la organización, determine los criterios de criticidad y entrenar al personal gerencial del área funcional

2.3.2 Impactos de un incidente al negocio.

Financiero.- Los posibles impactos financieros de un desastre incluyen: Pérdidas financieras serias, aumentos en primas de seguro, una reducción en el flujo de efectivo debido a la afectación de funciones de facturación, cuentas por cobrar y cobranza, incapacidad administrativa para utilizar capital de trabajo, pérdida de clientes, reducción de calificación de solvencia, gastos importantes por la contratación de personal temporal.

Clientes y proveedores.- Los clientes podrían preguntarse qué tan rápidamente los clientes sabrían que usted tiene un problema, que tan preocupados van a estar sobre el problema?, ¿Qué tipo de impacto podría causar a sus clientes por no estar disponible?, ¿Cuál es la probabilidad de que se lleven su negocio con algún otro proveedor?, ¿Cuál es la posibilidad de que enfrente una demanda grupal?,¿Qué impacto tendrá esto en su reputación?

Relaciones públicas / credibilidad / reputación.- Cuando no existe una inestabilidad al negocio y se siente afectado por alguna crisis o incidente y no se puede afrontar y tratar de que se afecte lo menos posible a la negocio esto puede afectar directamente la imagen del negocio hacia los clientes externos.

Legal.- Los posibles impactos legales y regulatorios de un desastre incluyen: Repercusiones de contratos con proveedores externos, clientes y distribuidores que usted no pueda ser capaz cumplir, penalizaciones que pueda enfrentar como consecuencia por ser incapaz de cumplir los requerimientos de otros contratos, penalizaciones por incumplimiento de informes o presentaciones en fechas límite a organismos reguladores, el potencial de demandas.

Medio Ambiente.- se puede afectar de manera directa e indirecta según en el sector y la clase de negocio a la cual se dediquen.

Operacional.- Los posibles impactos operacionales de un desastre incluye: Que usted pudiese estar operando en modo manual por un período de tiempo significativo, que la información que está normalmente disponible con oprimir un botón requiera investigación y trabajo manual tedioso, que la eficiencia se vea afectada, que la dirección tenga que tomar decisiones vitales para llevar la operación a través de la crisis.

De Personal.- Los mayores impactos luego de incidente se pueden generar en el personal que labora en el negocio dependiendo de qué tipo de desastre haya suscitado los que corren más riesgo son los empleados, ya sea físico o intelectual o incluso la pérdida del puesto.

2.4 Desarrollo de estrategias de continuidad de negocio.

Según el (DRI International, 2014), gestión de continuidad de negocios; "El objetivo es aprovechar los resultados del análisis de impacto del negocio y de la Evaluación de Riesgos para desarrollar y recomendar estrategias efectivas de continuidad de negocios. La base para estas estrategias incluye la consideración tanto del tiempo objetivo de recuperación como del punto objetivo punto de recuperación. Esta lo ayudará a evaluar y planificar el soporte de las funciones críticas de la organización" (P. 104) para ello hay que:

- Identificar y revisar los requerimientos de las estrategias de continuidad de negocios de la empresa
- Identificar y desarrollar estrategias para las unidades.
- Consolidar las estrategias de las unidades y de la empresa

En esta fase se seleccionarán los métodos operativos alternativos que se van a utilizar en el caso de que ocurra un incidente que provoque una interrupción en la organización. El método seleccionado deberá garantizar la restauración de los procesos afectados en los tiempos determinados por el Análisis de Impacto. (Jimenéz, 2007)

Para el desarrollo de las estrategias se seguirá los siguientes pasos:

2.4.1 Evaluar las estrategias

Analice los criterios de las necesidades de la empresa, la continuidad de funciones sensibles al tiempo, la continuidad de funciones impulsadas por factores externos, mantener las ventajas estratégicas y competitivas, mantener la rentabilidad y la viabilidad para sobrevivir, mantener la lealtad del cliente y la imagen en la industria, cualesquier otros asuntos y preocupaciones que hayan sido identificados.

2.4.2 Desarrollo de la estrategia

Éste es un proceso de 4 pasos para desarrollar una estrategia efectiva de continuidad de negocios según lo indica la figura 12.

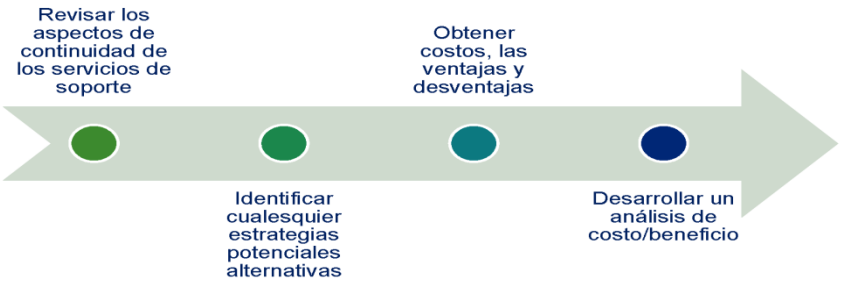


Figura 11. Pasos para desarrollar una estrategia
Fuente: (DRI International, 2014)

De todas las alternativas existentes hay que elegir la más adecuada en cada caso. Dependerá de las necesidades de cada empresa, en cuanto a tiempos de recuperación, costes económicos, recursos, etc.
Además deberá considerarse otros factores como:

- Ubicación y superficie requerida.
- Espacio suficiente.
- Zonas acondicionadas para acoger a personal
- Recursos técnicos necesarios: Hardware, Software, Comunicaciones y Datos de respaldo.
- Recursos humanos requeridos

2.5 Preparación y respuestas de emergencia.

DRI Internacional, 2014, Es importante identificar la preparación de la organización para responder a una emergencia de manera coordinada, oportuna y efectiva, desarrollar e implementar los procedimientos para la respuesta inicial y la estabilización de la situación hasta la llegada de las autoridades que tienen jurisdicción, para ello es necesario realizar lo siguiente;

- Identificar los tipos potenciales de emergencias y las respuestas requeridas
- Identificar y revisar los procedimientos existentes de respuesta de emergencia
- Recomendar el desarrollo de nuevos procedimientos de emergencia y la mejora de los procedimientos de emergencia existentes
- Recomendar el desarrollo de procedimientos de comando y control.

También se requiere preparación para la emergencia lo cual incluye

- Entrenar a los coordinadores de piso
- Programar simulacros de evacuación
- Programar simulacros de "refugio en el lugar"
- Programar simulacros de "Cierre"
- Designar los puntos de reunión
- Atender las preocupaciones de seguridad de vida de todos los empleados

En la siguiente Figura 12 se ilustra el equipo de respuesta de emergencia.

Figura 12. Equipo de respuesta de emergencia
Fuente: (DRI International, 2014)

2.5.1 Componentes del plan de evacuación.

En un plan de evacuación se debe contemplar los siguientes componentes, para tener una buena respuesta de tiempo objetivo de recuperación y punto objetivo de recuperación:

- Refugio en el Lugar: Requerido si las condiciones son más peligrosas fuera del edificio que dentro del edificio, Identifique el espacio de refugio o salón seguro
- Establezca los procedimientos para enviar personal al refugio
- Determine las necesidades de provisiones de emergencia –Agua, comida y material médico
- Designe administradores del refugio
- Evacue la instalación si las condiciones son más seguras fuera del edificio.
- Considere al menos 2 puntos de reunión
- Cuente a las personas ya evacuadas y aseguradas
- Identifique a las personas que no están presentes
- Todos los ocupantes del edificio están obligados a participar
- Los visitantes deben ser informados
- Los mapas de evacuación e instrucciones tienen que ser colocados en cada espacio común y área de trabajo
- Grupo de Evacuación de Emergencia
- Identifique al personal con la autoridad para ordenar una evacuación
- Determine las condiciones bajo las cuales sería necesaria una evacuación
- Identifique a las personas que contarán al personal

2.5.2 Manejo de crisis

(DRI International, 2014), "Las contingencias comienzan con el manejo de incidentes, si no se maneja apropiadamente los incidentes, todos los otros riesgos pueden ocurrir, el manejo de incidentes es acerca de la comunicación y la respuesta, necesita ser practicado y utilizar métodos de comunicación". Podemos observar en la siguiente Figura 14, el modelo de manejo de crisis.

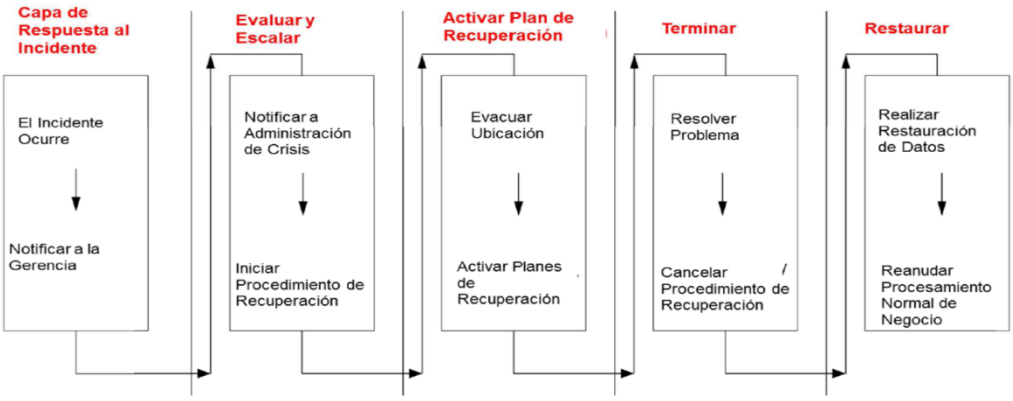


Figura 13. Modelo de Manejo de crisis
Fuente: (DRI International, 2014)

2.6 Desarrollo e implementación del Plan de Continuidad de Negocio

Se debe Diseñar, desarrollar e implementar Planes de Continuidad de Negocios que proporcionen continuidad y/o recuperación con base en los requerimientos de la organización, para ello definiremos:

- Los recursos necesarios para el progreso del Plan.
- Las responsabilidades y funciones de los activos.
- Las dependencias funcionales entre los distintos equipos.
- El desarrollo de procedimientos de alerta y acción contra sucesos que puedan activar el Plan de Continuidad de Negocio.
- Los procedimientos de acción contra sucesos.
- La estrategia de vuelta a la regularidad. (Jimenéz, 2007)

2.6.1 Organización de los equipos

"Los equipos de emergencia están formados por el personal clave necesario en la activación y desarrollo del Plan de Continuidad. Cada equipo tiene unas funciones y procedimientos que tendrán que desarrollar en las distintas fases del Plan" (Jimenéz, 2007) (P.25)

2.6.2 Director o comité de crisis

(Jimenéz, 2007) “El objetivo de este comité es reducir al máximo el riesgo y la incertidumbre en la dirección de la situación. Este Comité debe tomar las decisiones "clave" durante los incidentes, además de hacer de enlace con la dirección de la compañía, manteniéndolos informados de la situación regularmente, las principales tareas y responsabilidades de este comité son:

- Análisis de la situación.
- Decisión de activar o no el Plan de Continuidad.
- Iniciar el proceso de notificación a los empleados a través de los diferentes responsables.
- Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación.

2.6.3 Equipo de recuperación

El equipo de recuperación es responsable de establecer la infraestructura necesaria para la recuperación. Esto incluye todos los servidores, computadoras, comunicaciones de voz, datos, como otro elemento necesario para la restitución de un servicio.

2.6.4 Equipo logístico

Este grupo de trabajo debe estar pendiente del todo el personal, para atestiguar que cualquier necesidad logística sea cubierta, además es responsable de la relación con las necesidades logísticas en el ámbito de la recuperación, como son:

- Transporte de talento humano y activos al sitio alterno de recuperación.
- Relación con las empresas proveedoras.
- Provisiones de oficina.
- Alimentación.
- Reservaciones de hospedaje, de ser necesarias.

2.6.5 Equipo de relaciones públicas y atención a clientes.

El valor más significativo de una organización son sus clientes, por lo que es primordial mantenerles informados, la frecuencia de transmisión de información que se ejecuta al exterior es importante que se lo realice con un solo origen y un determinado punto, estableciendo canales de comunicación, sus funciones principales son:

- Comunicación con los interesados/clientes.
- Elaboración de comunicados a la prensa.

2.6.6 Equipo de las unidades de negocio

Cada equipo deberá conformar las diferentes pruebas en los sistemas. Estos equipos estarán formados por el personal que labora con los aplicativos críticos, y deben ser los delegados de ejecutar las ensayos de actividad para verificar la operatividad de los sistemas.

2.6.7 Desarrollo de Procedimientos

Luego de haber definido los equipos y establecido las funciones que debe desempeñar cada equipo, se tiene que desarrollar los procedimientos que van a seguir, y su actuación en cada una de las fases de activación del Plan de Continuidad.

Fase de Alerta

- Procedimiento de notificación del desastre.
- Procedimiento de lanzamiento del Plan.
- Procedimiento de notificación de la puesta en marcha del Plan a los equipos

Fase de transición.

- Procedimiento de traslado y puesta en marcha de la recuperación.
- Procedimiento de concentración de equipos.

Fase de recuperación

- Procedimientos de soporte y gestión.

- Procedimientos de restauración.

Fase de vuelta a la normalidad

- Análisis del impacto.
- Procedimientos de vuelta a la normalidad.

También es necesario solidificar lo siguiente datos antes de que el plan de continuidad de negocios sea requerido.

- Una referencia rápida para una emergencia.
- Los roles de los grupos de recuperación.
- La Lista de Notificación de Emergencia.
- El manejo de incidentes.
- Los procedimientos de declaración.
- Las listas de verificación y los planes de acción.
- Los procedimientos detallados de recuperación.
- El Soporte de Recursos Humanos / Finanzas / Administración.
- Las comunicaciones.

A continuación en la Figura 14. Podemos observar las fases y actividades del Plan de Continuidad de Negocio.

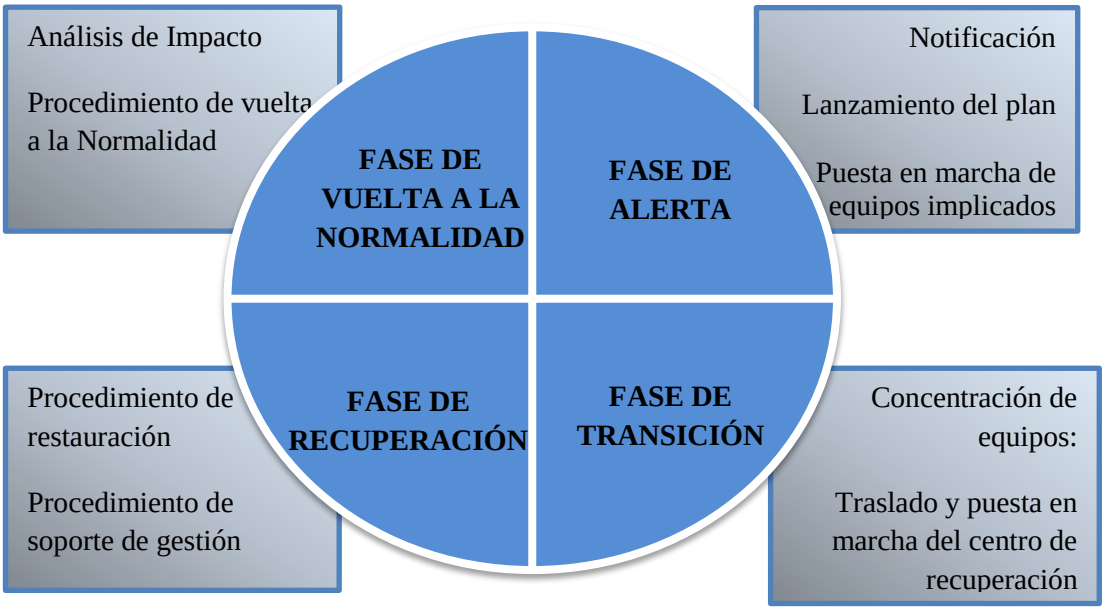


Figura 14. Fases y actividades de un plan de continuidad del negocio

2.7 Programas de concientización, entrenamiento y mantenimiento.

Preparar un programa para establecer y mantener la concientización corporativa de que la Administración de Continuidad de Negocios, es parte de la administración normal del negocio, así como desarrollar y mejorar las habilidades requeridas para crear e implementar la Administración de Continuidad de Negocios. (DRI International, 2014)

Para esto es muy Importante obtenga el apoyo de la alta gerencia, asegurar un presupuesto adecuado, definir el enfoque de la administración del programa y marcos de tiempo para su implementación, obtener el compromiso de los gerentes y del personal de operaciones que implementará el plan y alinear a las prioridades del negocio, así como también definir el nivel deseado del concientización con base en las responsabilidades.

2.7.1 Concientización

Es necesario dar a conocer los siguientes temas para la concientización de todos lo que son parte de la organización.

- Componentes del programa del plan.
- Importancia de los planes.
- Quiénes son los Planificadores / Coordinadores y los integrantes del grupo.
- Dónde puede ser localizada la información del plan.
- Cuándo es ejercitado o activado el plan.
- Cómo es ejercitado o activado el plan.

2.7.2 Entrenamiento

Se debe considerar los siguientes Temas para el programa de entrenamiento del plan de continuidad del negocio, todo el personal debe ser responsable de:

- Reconocer y reportar una emergencia.
- Advertir a los otros empleados en el área.
- Llevar a cabo la protección adecuada y las medidas de seguridad.
- Conocer la localización y el uso de equipo común de emergencia.
- Conocimiento de su rol específico en la ejecución.
- Entrenamiento específico de su función.
- Manejo de materiales peligrosos.
- Seguridad y protección.
- Conocer los procedimientos apropiados de respuesta de emergencia.
- Procedimientos de notificación.
- Procedimientos de escalamiento.
- Procedimientos de evacuación, refugio y control del personal.
- Entrenamiento previo al ejercicio.
- Entrenamiento en el software del plan.
- Roles y responsabilidades individuales.

2.7.3 Mantenimiento del plan de continuidad

"Por la propia dinámica de negocio, se van incorporando nuevas soluciones a los Sistemas de Información y los activos informáticos van evolucionando para dar respuesta a las necesidades planteadas. La correcta planificación del mantenimiento del Plan de Continuidad evitará que quede en poco tiempo obsoleto y que en caso de contingencia no pueda dar respuesta a las necesidades". Jiménez, L. d. (2007, P.36)

2.8 Requisitos legales, normativos y reglamentarios.

2.8.1 Requisitos reglamentarios

Se considera lo estipulado en el reglamento interno de la Asociación en los siguientes Artículos:

Art. 34 Obligaciones del trabajador numeral 17, Participar en las brigadas de primeros auxilios, contra incendios y demás implementadas por la Asociación.

Art. 56 Inducción, entrenamiento y cursos obligatorios: Es obligación de los trabajadores y empleados asistir y aprobar los cursos, conferencias de información y entrenamiento que se realicen como parte de las políticas de la Asociación.

Art. 57 Uso de bienes, equipos e instrumentos de la Asociación.- El uso adecuado de los bienes de la Asociación, los equipos e instrumentos entregados para efectúa o facilitar el trabajo está bajo responsabilidad del trabajador o empleado y deberá responder por el daño o deterioro que no comprenda el uso normal; de igual manera, es responsable de la pérdida o mal uso de los mismos en caso de no presentar justificación valida.

En cualquier caso el trabajador o empleado deberá notificar a su jefe directo el daño o perdida con el correspondiente informe que justifique el hecho de no hacerlo o si la información presentada no es aceptable, el valor de reposición o reparación del bien, equipo o instrumentos será de responsabilidad del trabajador o empleado y se reducirá de su remuneración o liquidación.

Art. 58 De los bienes instrumentos y equipos de trabajo. Los trabajadores e empleados están obligados a cuidar de todos los instrumentos de trabajo procurando su correcto uso y aplicación y velar por su conservación al igual que todos los bienes de la Asociación.

Está prohibido el uso de instrumentos y equipos de la Asociación para fines distintos a los destinados por naturaleza y la utilización de estos instrumentos en actividades personales o ajenas a las que realiza el empleado.

Art. 59 Responsabilidad.- Todos los trabajadores o empleados son personal y pecuniariamente responsables por los daños que ocasionen a los bienes , máquinas y equipos de la Asociación o por el retardo en la prestación del servicio a sus clientes

como consecuencia de descuido negligencia o desobediencia las disposiciones legales o reglamentarias correspondientes.

2.8.2 Requisitos legales.

(Constitución de la República del Ecuador, 2008), la constitución de la política el ecuador en sus artículos 389 y 390.

Art. 389.- El Estado protegerá a las personas, las colectividades y la naturaleza frente a los efectos negativos de los desastres de origen natural o antrópico mediante la prevención ante el riesgo, la mitigación de desastres, la recuperación y mejoramiento de las condiciones sociales, económicas y ambientales, con el objetivo de minimizar la condición de vulnerabilidad. (Constitución de la República del Ecuador, 2008)

(Constitución de la República del Ecuador, 2008). El sistema nacional descentralizado de gestión de riesgo está compuesto por las unidades de gestión de riesgo de todas las instituciones públicas y privadas en los ámbitos local, regional y nacional. El Estado ejercerá la rectoría a través del organismo técnico establecido en la ley. Tendrá como funciones principales, entre otras:

1. Identificar los riesgos existentes y potenciales, internos y externos que afecten al territorio ecuatoriano.
2. Generar, democratizar el acceso y difundir información suficiente y oportuna para gestionar adecuadamente el riesgo.
3. Asegurar que todas las instituciones públicas y privadas incorporen obligatoriamente, y en forma transversal, la gestión de riesgo en su planificación y gestión.
4. Fortalecer en la ciudadanía y en las entidades públicas y privadas capacidades para identificar los riesgos inherentes a sus respectivos

ámbitos de acción, informar sobre ellos, e incorporar acciones tendientes a reducirlos.

5. Articular las instituciones para que coordinen acciones a fin de prevenir y mitigar los riesgos, así como para enfrentarlos, recuperar y mejorar las condiciones anteriores a la ocurrencia de una emergencia o desastre.
6. Realizar y coordinar las acciones necesarias para reducir vulnerabilidades y prevenir, mitigar, atender y recuperar eventuales efectos negativos derivados de desastres o emergencias en el territorio nacional.
7. Garantizar financiamiento suficiente y oportuno para el funcionamiento del Sistema, y coordinar la cooperación internacional dirigida a la gestión de riesgo. (Constitución de la República del Ecuador, 2008)

Art. 390.- Los riesgos se gestionan bajo el principio de descentralización subsidiaria, que implica la responsabilidad directa de las instituciones dentro de su ámbito geográfico. Cuando sus capacidades para la gestión del riesgo sean insuficientes, las instancias de mayor ámbito territorial y mayor capacidad técnica. (Constitución de la República del Ecuador, 2008)

CAPITULO III

MARCO METODOLÓGICO

3.1 Metodología de Investigación.

Para efectos de este estudio, es decir la elaboración del plan de continuidad de negocio aplicado al centro de datos de la fiscalización del Proyecto Hidroeléctrico Coca Codo Sinclair, se describe los métodos técnicos y procedimientos que fueron empleados para el logro de los objetivos propuestos.

3.1.1 Tipo de investigación

Al realizar el diagnóstico del estado actual que opera la fiscalización en esta área de datos, frente a posibles interrupciones sean estas naturales o provocadas por el hombre, en concordancia con el objetivo general se inscribe dentro de la modalidad de investigación proyectiva , la cual permite solucionar necesidades de una empresa y proponer alternativas de cambio.

En este sentido (Hurtado, 2000) indica, "La investigación proyectiva consiste en la elaboración de una propuesta o un modelo como solución a un problema o una necesidad de tipo practico, ya sea de un grupo social o una institución de una área particular del conocimiento a partir de un diagnóstico preciso de una necesidad del momento, los procesos explicativos y generadores involucrados y las tendencias futuras" (p.325)

Se utilizó de igual manera la investigación, Descriptiva, de Campo y Bibliográfica, para la obtención de la información complementaria:

- **Descriptiva**.- La investigación se circunscribe a un estudio descriptivo, la recolección de datos sobre la base de una teoría, esto permitirá describir las

actividades que realiza la fiscalizadora detallando claramente cada uno de sus componentes.

- **De Campo.-** La investigación se desarrollará directamente en la organización encargada de la fiscalización. Se mantendrá una relación directa con las fuentes de información, tanto a nivel general como individual. Se observó las actividades y se aplicó encuestas.

- **Bibliográfica.-** Se sustenta la base teórica de la investigación, mediante consultas a: fuentes bibliográficas, textos, revistas, apuntes, documentos expertos varios, así como también fuentes informáticas e internet.

3.1.2 Métodos de investigación

Para la investigación y el desarrollo de la presente tesis se utilizó los siguientes métodos:

- **Método inductivo – deductivo**.- Se aplicó un proceso analítico sintético, estudiando aspectos particulares de las actividades realizadas dentro de la organización, estableciendo un sustento teórico general.

- **Método de Muestreo – no probabilístico.-** Este método no es un tipo de muestreo riguroso y científico, dado que no todos los elementos de la población pueden formar parte de la muestra, se trata de seleccionar a los sujetos siguiendo determinados criterios procurando que la muestra sea representativa. Es decir, los elementos de la muestra son seleccionados por procedimientos al azar o con probabilidades conocidas de selección.

  Se aplica al jefe del área del centro de datos de la Fiscalización del Proyecto Hidroeléctrico, quien nos proporciona la información básica necesaria para el diagnóstico respectivo.

3.1.3 Técnicas de Investigación

Las técnicas e instrumentos de recolección de datos de la Investigación se aplicaron de manera explicativa, de tal manera que se pudieron fundamentar los resultados de la investigación y así poder respaldar de la mejor manera las estrategias propuestas.
Se entiende que la recolección de datos está en función del tipo de investigación el contexto y la fuente, la temporalidad y el número de mediciones.
Por lo tanto la recolección de datos según el contexto y la fuente del cual proviene, se utilizó en el presente estudio fueron de fuentes múltiples, este comprende la consulta documental y la aplicación de instrumentos propios de recolección de información.
De igual manera este estudio implico la recolección de datos de fuentes vivas, como es el caso de los datos obtenidos directamente de los sujetos estudiados.
En relación a las técnicas de recolección de datos utilizadas para llegar al desarrollo de la propuesta son las siguientes:

- **La Encuesta.-** Es un instrumento que nos permite recaudar información mediante la aplicación de un cuestionario con preguntas claras y necesarias para conocer la realidad de la situación de la organización y en base a ello tomar las decisiones.

- **La Observación.-**"Uso sistemático de nuestros sentidos en la búsqueda de los datos que necesitamos para resolver un problema de investigación" (Sabino, 1985). Esta técnica fue de mucha utilidad para conocer las características del ente y la forma en que ejecuta sus actividades, sin que el investigador asumiere una actitud participante en los mismos.

- **Entrevista.-** Como una forma de interacción social, consiste en establecer un dialogo, donde una de las partes busca obtener información y la otra sirve de fuente (Sabino, 1985), la razón por la cual se utilizó esta técnica es porque son los actores de la realidad que se estudia, los que conocen de la manera más integra y confiable los procesos, las entrevistas no fueron estructuradas

debido a que las conversaciones se orientaron de un desarrollo flexible y espontaneo, lo que permitió detectar elementos no previstos y con ello poder efectuar el diagnóstico de los principales problemas que actualmente se puede evidenciar en la organización fiscalizadora.

3.1.4 Población y muestra.

La población puede estar referida a cualquier conjunto de elementos de los cuales pretendemos indagar y conocer sus características las cuales serán validadas con las conclusiones de la investigación.

Por otro lado la muestra, es un subconjunto fielmente representativo de la población. Hay diferentes tipos de muestreo, esto depende de la calidad y cuán representativo es el estudio de la población.

- **Aleatoria.-** cuando se selecciona al azar y cada miembro tiene igual oportunidad de ser incluido.

- **Estratificada.-** cuando se subdivide en estratos o subgrupos según las variables o características que se pretenden investigar. Cada estrato debe corresponder proporcionalmente a la población.

- **Sistemática**.- cuando se establece un patrón o criterio al seleccionar la muestra. Ejemplo: se entrevista una familia por cada diez que se detecten

- **El muestreo.-** es indispensable para el investigador ya que es imposible entrevistar a todos los miembros de una población debido a problemas de tiempo, recursos y esfuerzo. Al seleccionar una muestra lo que se hace es estudiar una parte o un subconjunto de la población, pero que la misma sea lo suficientemente representativa, para que luego pueda generalizarse con seguridad de ellas a la población.

El tamaño de la muestra depende de la precisión con que el investigador desea llevar a cabo su estudio, pero por regla general se debe usar una muestra tan grande como sea posible de acuerdo a los recursos que haya disponibles. Entre más grande la muestra mayor posibilidad de ser más representativa de la población.
Atendiendo las fases de proceso de muestreo se sugiere los siguientes pasos para determinar la muestra de investigación.

1. **Definición de unidades de estudio**.- se tomó como unidad de Estudio el Proyecto Coca Codo Sinclair, es decir el universo de la investigación.

2. **Delimitación de la población de estudio**.- La delimitación de la población de estudio estuvo delimitada a los funcionarios que laboran en la empresa fiscalizadora del proyecto Hidroeléctrico Coca Codo Sinclair, que laboran en la gerencia de Administración y el área directamente involucrada sistemas informáticos.
   La población es de tipo finita dado que sus elementos pudieron ser identificados y enlistados en su totalidad.

3. **Calculo del tamaño de la muestra.-** Para establecer el tamaño de la muestra existen diversas opiniones sin embargo, la mayoría apuntan a establecer de acuerdo a la homogeneidad de la población y los objetivos del estudio.

En virtud de aquello y, por ser la población finita y accesible se consideró una muestra de 9 funcionarios como actores sociales, a través de la aplicación de los instrumentos de recolección de datos suministraron elementos de criterios básicos vinculados con el sistema de datos que maneja la empresa fiscalizadora, por lo que no fue necesario aplicar la técnica de muestreo, y se considera que estudiados los miembros representativos de la población los resultados observados y obtenidos describen el verdadero comportamiento de la misma.

3.1.5 Técnicas de procesamiento y análisis de datos.

Una vez recopilada la información referente al objeto de estudio, se procede a tabular los datos recopilados para su posterior análisis e interpretación.

La tabulación implico el ordenamiento de esta información la cual fue procesada y ordenada y clasificada según los objetivos planteados, esto permitió el análisis, luego del registro de cálculos y la presentación de cuadros, gráficas y tablas, haciendo uso del software Microsoft Excel.

En lo que respecta a datos obtenidos mediante registro de observación documental, se revisaron documentos relacionados con planes de continuidad de negocios, específicamente se tomó de referencia la Norma ISO 22301, a si mismo se estudiaron diferentes fuentes de carácter legal y normativo.

3.2 Métodos para el desarrollo

3.2.1 Metodología para el plan de continuidad del negocio.

La metodología aplicada se basa en la (Norma ISO 22301, 2012) "Sistema de Gestión de Continuidad del Negocio" que inicia desde el entendimiento del negocio, la identificación de posibles riesgos, su impacto y valoración, definición de estrategias, elaboración del plan, desarrollo de una cultura, hasta la prueba, mantenimiento y auditoría del plan.

El propósito general de un Plan de recuperación es obtener un mapa de acciones que reduzcan "la toma de decisiones" durante las operaciones de recuperación, restaure los servicios críticos rápidamente y permita un normal funcionamiento de los sistemas y procesos lo antes posible, minimizando costes y aumento de la efectividad.

Las fases planteadas en la metodología son:

- **Comprensión de la Organización y su contexto:** Se determina los problemas externos e internos que son relevantes para su propósito y que afecta a su capacidad para lograr el resultado deseado, se conoce las funciones, servicios y actividades de la empresa, vincular los objetivos, las políticas, las estrategias para definir el propósito y el alcance de la gestión de continuidad de negocios.

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

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

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

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

CAPÍTULO IV

DIAGNÓSTICO SITUACIONAL

4.1 Introducción.

Es importante la elaboración de un diagnóstico situacional, para conocer el estado en que se encuentra la Asociación en el ámbito de seguridad de la información en el área de sistemas, además obtener una visión clara y comprensible sobre las fortalezas y debilidades que la organización adquirido en el transcurso de sus funciones.

En síntesis para la realización del diagnóstico se enfatizará en la aplicación de la utilización de técnicas de recolección de información, con los resultados que se obtengan identificaremos los riesgos que puedan ocasionar un alto grado de impacto en las actividades, ayudando a detectar áreas de mejora para poder diseñar un plan de continuidad de negocio que responda a las actuales necesidades prioritarias, así como las previstas necesidades futuras.

La realización de esta fase está enfocada en tomar en cuenta los siguientes aspectos de análisis;

1. Situación actual y análisis de resultados respecto a la seguridad de los datos del área de sistemas de la Asociación.
2. Análisis y evaluación de criterios; liderazgo, planificación, apoyo, funcionamiento, y planeación estratégica.
3. Identificación y análisis de riesgos existentes.

La Asociación cuenta con una estructura organizativa informal, quiere decir que las relaciones no han sido definidas explícitamente y responden básicamente a las necesidades que están en contacto con el trabajo, esto surge a través de la búsqueda de un objetivo mutuo y la satisfacción de las necesidades, en la tabla siguiente podemos ver el organigrama de la Asociación.

➲ **Estructura Organizacional de la Empresa**

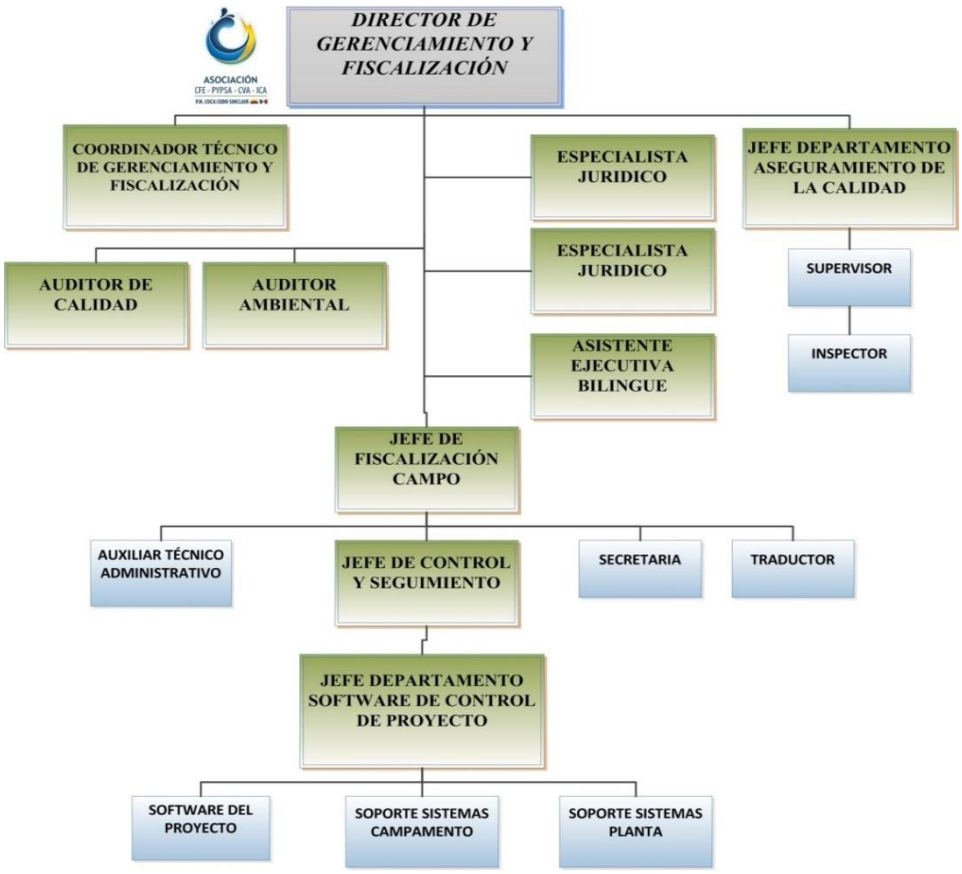


Figura 15. Organigrama de la fiscalización

4.1.1 Situación actual y análisis de resultados respecto a la seguridad de los datos del área de sistemas de la Asociación.

En la actualidad la Asociación centraliza sus trabajos en su campamento con nombre “La Loma” desde junio del 2014, su centro de datos cuenta con servidores que contienen software de control de proyectos, software de cronograma de proyecto, aplicaciones internas y unidades de red compartidas.

La información almacenada es recopilada diariamente de todos los frentes de obra para posterior ser transmitida al principal interesado que es la empresa pública Coca

Codo Sinclair y también sirve como información para las diferentes áreas de trabajo de la Asociación.

4.1.2 La Entrevista

Para conocer la situación actual de la Asociación respecto a la seguridad de la información, fue necesario realizar una entrevista, la misma que se le realizó al jefe de sistemas de información de la Asociación, para el desarrollo de la entrevista se consideraron varios puntos a tratar entre ellos el conocimiento y utilización de la Norma ISO 22301 y Plan de Continuidad de Negocio.

Con esta entrevista se pudo conocer el compromiso que tiene como líder dentro de la Asociación, si se ejecutan procesos de operación y control de información, si existe una planificación estratégica con objetivos, políticas y estrategias establecidas para la continuidad de negocios, lo que piensa acerca de los riegos existentes y cuán importante pueden ser sus impactos.

La entrevista se la realizó en la oficina del jefe del área de sistemas y tuvo una duración de 45 minutos, la plática con el líder permitió escuchar su versión y además despejar ciertas dudas respecto al tema planteado ya que a su criterio no es algo muy conocido. Para identificar los resultados se hizo un análisis cualitativo de los datos obtenidos, además se enlisto los criterios importantes a continuación.

- Conoce algo sobre el plan de continuidad de negocios, lo escucho en las anteriores empresas donde laboró, pero no adquirió experiencia porque él no estaba en cargos directivos de donde se manejaba estos temas.
- Desconoce sobre la existencia de la norma ISO 22301 que regula la continuidad de negocios.
- Noto que era necesario resguardar la información, por la zona geográfica que está ubicada la Asociación y por las erupciones volcánicas de menor impacto que se puede visualizar constantemente.
- La información estaba en peligro de poder ser eliminada y no había un resguardo, por lo que solicitó la adquisición de discos externos para respaldar la información y mantenerla fuera de las instalaciones.

- En el nuevo campamento donde funciona el centro de datos de la Asociación está rodeado de varios riesgos naturales, como las montañas, la creciente del Río Coca, el oleoducto y poliducto y los asentamientos humanos, los mismo que no los identificó anteriormente, sólo se percató en la Erupción del Volcán Reventador, sismos y la variación de voltaje de la energía eléctrica que es constante lo cual puede causar daños a los activos de la Asociación.
- Está consciente de que la Asociación no cuenta con procesos adecuados para minimizar el impacto de los riesgos ante un posible incidente.
- La Asociación no cuenta con una planificación estratégica definida específicamente para la seguridad de la información y los datos existentes esta desactualizada.
- Falta comunicación y preparación del personal para actuar ante un incidente.
- El comité de activación de alarmas no ha sido reestructurado.
- En las nuevas Instalaciones de la Asociación los altos directivos no han hablado de seguridad y no han dado a conocer los procedimientos para actuar ante las emergencias además no se ha conocido sobre una alarma como anuncio de un incidente, además no se han realizado simulacros.
- La Asociación carece de personal competente para ejecutar un plan de continuidad.
- Ahora conociendo sobre el impacto que puedan ocasionar los riesgos, mira a un plan de continuidad de negocios como un bien necesario, ya que los incidentes ocasionados por desastres naturales son imprevistos y pueden causar grandes daños e incluso paralizar las actividades de su lugar de trabajo, puesto que estas catástrofes ya han sucedido en ocasiones anteriores en este lugar.

4.1.2.1 Análisis Particular de la entrevista respecto a la seguridad de los datos.

De acuerdo a los resultados obtenidos de la entrevista se puede concluir que se comprobó en la presente investigación, que el entrevistado esta al tanto y también

manifiesta la preocupación que existe por parte de los lideres conociendo los riesgos a los cuales está expuesta la Asociación por la zona geográfica en la cual está ubicada, se puede evidenciar que la Asociación no está preparada para enfrentar un incidente y minimizar el impacto del mismo.

Debido a que no tiene una planificación estratégica y procedimientos administrativos adecuados y actualizados, el control establecido para la seguridad de la información que es respaldar en un disco duro externo la misma no es muy seguro, porque tratándose de desastres naturales estos ocurren de imprevisto y de manera inesperada, y al no haber una preparación del personal de cómo actuar ante las emergencias el riesgo.

La pérdida de información también puede afectar a la integridad física de los funcionarios y por ende una paralización de las actividades normales de la Asociación, basado en el diagnóstico actual de la Asociación de acuerdo a los resultados, esta no cumple con los estándares establecidos en la norma ISO 22301 de la gestión de continuidad de negocios.

4.1.3 La Encuesta

Esta fue aplicada a nueve personas que conforman el área de sistemas y administrativos encargado de la toma de decisiones respecto a seguridad de la información, (ver anexo A: encuestas para analizar la gestión de continuidad de negocios que tiene la Asociación ante los riesgos de la seguridad de la información.)
Se aplicó preguntas abiertas y cerradas, basadas en los lineamientos que estipula la norma ISO 23100 respecto a la gestión de continuidad de negocios, para efecto de conocer si se cumple o no con esta norma y su análisis respectivo para la propuesta, el cual comprende el siguiente cuestionario:

1.- Primera pregunta; Si se produce un desastre o una interrupción significativa, ¿La Asociación tiene un plan documentado para la continuidad de negocio y recuperación de desastres. Se solicita que respondan SI o NO, dando estos resultados:

Tabla 1. Resultados de la encuesta referente a la primera pregunta

RESPUESTAS	CANTIDAD	PORCENTAJE
SI	1	11.11%
NO	8	88.89%
TOTAL	9	100%

Como indica la tabla de las nueve personas encuestadas las 8 respondieron que la empresa no cuenta con un plan de continuidad de negocios, y una respondió que si al parecer no está claro lo que es una gestión de continuidad de negocios por lo cual esto no ha sido socializado dentro de la Asociación, el gráfico siguiente muestra con claridad los porcentajes de los resultados y evidencia la confirmación de lo planteado.

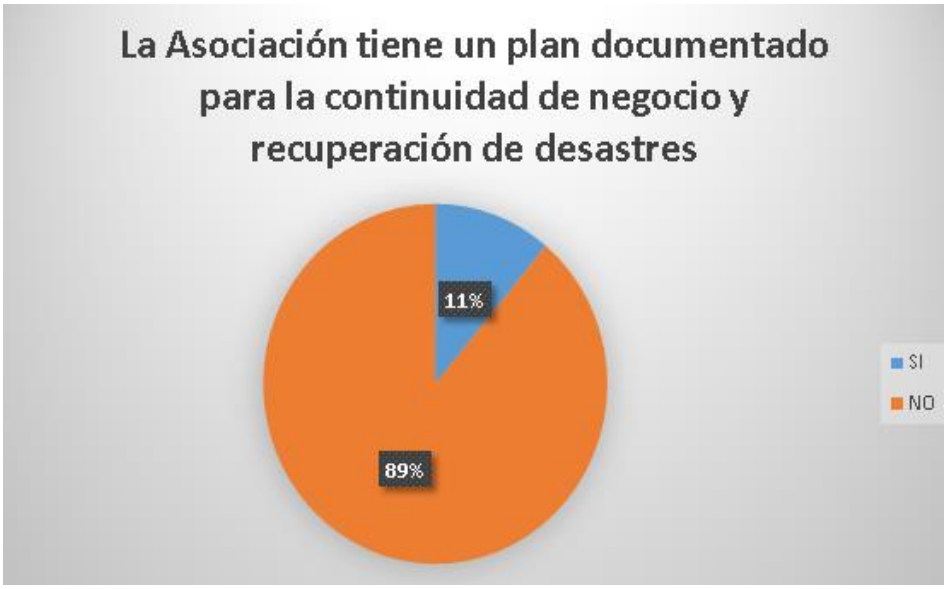


Figura 16. Gráfico de respuestas con respecto a la primera pregunta

2.- Segunda Pregunta; Se cuenta con un proceso documentado de comunicación de crisis la Asociación? Se solicita que respondan SI o NO, obteniendo los siguientes resultados:

Tabla 2. Resultados de la encuesta referente a la segunda pregunta

RESPUESTAS	CANTIDAD	PORCENTAJE
SI	2	22.22%
NO	7	77.78%
TOTAL	9	100%

Como se puede observar los resultados en la tabla 6, la cual indica que de las 9 respuestas, 7 dicen que NO existe una comunicación en crisis, y las 2 restantes optan por la respuesta SI pero su criterio no es el adecuado con la pregunta realizada, debido que no se tiene conocimientos sobre comunicación en crisis.

Figura 17. Gráfico de respuestas si cuentan con un proceso de comunicación de crisis

3.- Tercera Pregunta; La Asociación tiene una ubicación alternativa para la recuperación del centro de datos. Se solicita que respondan SI o NO, obteniendo los siguientes resultados:

Tabla 3. Resultados de la encuesta referente a la tercera pregunta

RESPUESTAS	CANTIDAD	PORCENTAJE
SI	0	0%
NO	9	100%
TOTAL	9	100%

En cuanto a la tercera pregunta se obtiene como resultado un total de 9 respuestas que coinciden en que NO existe una ubicación alternativa para la recuperación de información.

Figura 18. Gráfico de resultados referente a la tercera pregunta de la encuesta

4.- Cuarta Pregunta; Los líderes de la Asociación han demostrado su compromiso y han garantizado la seguridad de la información. Se solicita que respondan SI o NO, obteniendo los siguientes resultados:

Tabla 4. Resultados de la encuesta referente a la cuarta pregunta

RESPUESTAS	CANTIDAD	PORCENTAJE
SI	3	33.33%
NO	6	66.66%
TOTAL	9	100%

En la cuarta pregunta el intervalo se reduce entre las respuestas SI y NO, tenemos un resultado de 3 encuestados que dicen, que SI existe un compromiso de los líderes en garantizar la seguridad de información, basándose en un proceso de resguardo de información, el mismo que no está debidamente documentado, formalizado y comunicado al resto de personal de la Asociación.

Además existe la falta de compromiso y actualización en hacer cumplir este proceso los 6 encuestados restantes dijeron que NO existe liderazgo y compromiso que garantice la seguridad de su información, ya que no tuvieron ningún conocimiento o argumento sobre el proceso de resguardo de información.

Como se puede visualizar de acuerdo a los resultados indicados en la tabla anterior 8 de los nueve encuestados manifiestan que no hay mayor compromiso de los líderes respecto a garantizar la seguridad de la información, por lo contrario 3 de los encuestados han respondido que SI, con ello podemos concluir que existe una responsabilidad de compromiso ante el liderazgo solo en un 33.33% , como lo expresa el siguiente gráfico estadístico.

Figura 19. Gráfico de los resultados correspondientes a la cuarta pregunta de la encuesta

5.- Quinta Pregunta; Considera usted que la Asociación está preparada para enfrentar un incidente o posible interrupción a causa de un desastre natural.

Tabla 5. Resultados de la encuesta referente a la quinta pregunta

RESPUESTAS	CANTIDAD	PORCENTAJE
SI	0	0%
NO	9	100%
TOTAL	9	100%

Como respuesta en la quinta pregunta todos los encuestados dicen que la Asociación NO cuenta con los recursos suficientes y personal calificado necesario, para enfrentar un incidente o una posible interrupción a causa de un desastre natural.

Figura 20. Gráfico de resultados y porcentajes de las respuestas de la quinta pregunta de la encuesta

6.- Sexta Pregunta; Conoce usted los riesgos naturales que rodean a la Asociación.

Tabla 6. Resultados de la encuesta referente a la sexta pregunta

RESPUESTAS	CANTIDAD	PORCENTAJE
SI	9	100%
NO	0	0%
TOTAL	9	100%

Todos los encuestados están al tanto de los riesgos naturales que los rodean, ya que los perciben día a día, dándole muy poca importancia hasta acostumbrarse a vivir con ellos y aceptar el apetito de riesgo, sus respuestas en total mayoría son la erupción del Volcán El Reventador, sismos o temblores, deslaves, terremotos e inundación. Además algunos se fijan en algo más detallado como es la variación de voltaje de electricidad, lo cual es continuo.

Figura 21. Gráfico de resultados y porcentajes de acuerdo a la sexta pregunta de la encuesta

4.1.3.1 Análisis Particular de las encuestas respecto a la seguridad de los datos.

Tabla 7. Resultados con los porcentajes generales de las preguntas aplicadas en la encuesta

Nro.	PREGUNTAS	SI	NO
1	Si se produce un desastre o una interrupción significativa, ¿La Asociación tiene un plan documentado para la continuidad de negocio y recuperación de desastres	11%	89%
2	Se cuenta con un proceso documentado de comunicación de crisis la Asociación?	22%	78%
3	La Asociación tiene una ubicación alternativa para la recuperación del centro de datos.	0%	100%
4	Los líderes de la Asociación han demostrado su compromiso y han garantizado la seguridad de la información.	33%	67%
5	Considera usted que la Asociación está preparada para enfrentar un incidente o posible interrupción a causa de un desastre natural.	0%	100%
6	Conoce usted los riesgos naturales que rodean a la Asociación.	100%	0%

Los resultados obtenidos en las encuestas demuestran un amplio intervalo de coincidencia, los encuestados conocen de los riesgos que los rodean, pero desconocen de control alguno que exista para mitigar estos riesgos, En la pregunta 1, el 89% de los encuestados responde que la Asociación no está preparada para enfrentar una posible interrupción a causa de un desastre natural, pese a que todo el personal conoce los riesgos que existen en la zona.

En la pregunta 2, el 78% de los encuestados responde que desconocen de un proceso documentado de comunicación en crisis y que al suscitarse no se podría responder de manera adecuada.

En la pregunta 3, el 100% de los encuestados tienen noción de que la Asociación no tiene una ubicación alternativa de recuperación de centro de datos, esto implica que de suscitar algún desastre natural, paralizaría las actividades normales y no habría una pronta recuperación y reactivación de la misma.

En la pregunta 4, el 67% de los encuestados han manifestado que los líderes no han demostrado su compromiso, mucho menos han garantizado la seguridad de la información, su respuesta se fundamenta en que no han recibido comunicación alguna sobre compromisos realizados con el personal y el líder.

En la pregunta 5, el 100% de los encuestados están conscientes de que la Asociación no está preparada para enfrentar un incidente o un posible desastre natural, debido a que no cuenta con los recursos y personal necesarios.

En la pregunta 6, el 100% de los encuestados conocen de los riesgos naturales que los rodean, entre sus respuestas podemos encontrar: erupción del Volcán El Reventador, deslaves, temblores, inundaciones, terremotos, y sismos.

4.2 Análisis y evaluación de criterios; liderazgo, planificación y apoyo, funcionamiento y planeación estratégica.

Para el análisis de criterios se utilizó los parámetros de la norma ISO 22301, que enmarca una gestión de continuidad de negocios, con ello confrontar la realidad de la Asociación.

La determinación de los criterios y la calificación se lo realizo en base a los resultados obtenidos de la entrevista y encuestas, tomando en cuenta las variables, indicadores y fuentes de información que muestra la siguiente matriz:

Tabla 8. Matriz de Evaluación de Criterios

OBJETIVO	**VARIABLES**	**INDICADORES**	**TECNICAS**	**FUENTE DE INFORMACION**
Evaluar criterios de continuidad de negocios, para determinar el impacto y el período de recuperación que puedan ocasionar los siniestros.	Liderazgo y compromiso	Gestión Compromiso Política impartidas Roles de la organización, las responsabilidades y autoridades	Encuesta	EMPLEADOS:
	Planificación y apoyo	Acciones para abordar los riesgos y oportunidades. Recursos conciencia y comunicación Control de información documentada		Jefe de Fiscalización de Campo. Departamento de control y seguimiento. Departamento de software del proyecto.
	Funcionamiento Planeación estratégica	Planificación y control operacional. Desarrollo de Objetivos, Políticas y Estrategias. Procedimientos de continuidad de negocios.	Entrevista	Expertos

La valoración respectiva se realizó otorgando una puntuación sobre el 100%, y distribuida para cada criterio de acuerdo a los datos indicados en la siguiente tabla de valoración.

Tabla 9. Escala de valoración de puntuación

CRITERIO	INDICADORES	PONDERACIONES	
Liderazgo y compromiso (25%)	Gestión Compromiso (10%)	No	0
		Bajo	1
		Medio	3
		Alto	6
	Política impartida. (7%)	No	0
		Bajo	1
		Medio	2
		Alto	4
	Roles de la organización, las responsabilidades y autoridades (8%)	No	0
		Bajo	1
		Medio	2
		Alto	5
Planificación y apoyo (35%)	Acciones para abordar los riesgos y oportunidades (15%)	No	0
		Bajo	1
		Medio	5
		Alto	9
	Recursos conciencia y comunicación. (12%)	No	0
		Bajo	1
		Medio	4
		Alto	7
	Control de información documentada. (8%)	No	0
		Bajo	1
		Medio	2
		Alto	5
Funcionamiento Planeación estratégica (40%)	Planificación y control operacional. (9%)	No	0
		Bajo	1
		Medio	3
		Alto	5
	Desarrollo de Objetivos, Políticas y Estrategias. (15%)	No	0
		Bajo	1
		Medio	6
		Alto	8
	Procedimientos de continuidad de negocios. (16%)	No	0
		Bajo	1
		Medio	5
		Alto	10
TOTAL			100%

4.2.1 Evaluación de criterios; Liderazgo.

Tabla 10. Evaluación de Liderazgo

LIDERAZGO Y COMPROMISO	PUNTUACIÓN MÁXIMA	PUNTUACIÓN	PORCENTAJE TOTAL
Gestión de compromiso Garantizar que las políticas y objetivos se establecen para el sistema de gestión de la continuidad del negocio son compatibles con la dirección estratégica de la organización, Garantizar que los recursos necesarios para el sistema de gestión de la continuidad del negocio están disponibles. Dirigir y apoyar a las personas que contribuyen a la eficacia de la BCMS, la promoción de la mejora continua, y El apoyo a otras funciones de gestión pertinentes para demostrar su liderazgo y compromiso que se aplica a sus áreas de responsabilidad.	10	3	3%
Política Impartida La alta dirección deberá establecer una política de continuidad de negocio y: Proporciona un marco para el establecimiento de objetivos de continuidad de negocio. Incluye un compromiso de cumplir con los requisitos aplicables. Incluye un compromiso de mejora continua del BCMS.	7	4	4%
Responsabilidades de las autoridades La alta dirección deberá asegurarse asignar la responsabilidad y autoridad para asegurar que el sistema de gestión se ajusta a los requisitos de esta norma internacional, e informar sobre el desempeño de la BCMS a la alta dirección	8	2	2%
TOTAL	**25**	**9**	**9%**

De acuerdo al análisis realizado, se obtuvo como resultado un 9% de liderazgo, en referencia al 25% establecido para este criterio, lo cual indica que la participación de los líderes en cuanto a compromiso con la gestión de continuidad de negocios de la Asociación es media en cuanto a la escala de ponderación, debido a otras responsabilidades no se ha priorizado ni considerado los riesgos que podrían afectar la seguridad de la información y cuán importante es tomar medidas de prevención esto manifiestas las fuentes de información consideradas en esta evaluación.

4.2.2 Evaluación de criterios; Planificación y apoyo.

Tabla 11. Evaluación de Procesos Administrativos

PLANIFICACIÓN Y APOYO	PUNTUACIÓN MÁXIMA	PUNTUACIÓN	PORCENTAJE TOTAL
Acciones para abordar los riesgos y oportunidades Asegurar que el sistema de gestión puede alcanzar el resultado pretendido (s), Prevenir, o reducir, los efectos no deseados, lograr la mejora continua Acciones para hacer frente a estos riesgos y oportunidades.	15	1	1%
Recursos conciencia y comunicación. Proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua. Las personas que hacen el trabajo bajo el control de la organización deberán conocer la política de continuidad de negocio, su propio papel durante incidentes perturbadores. La organización deberá determinar la necesidad para comunicaciones internas y externas pertinentes y saber cuándo comunicar y a quien comunicar.	12	1	1%
Proceso de control de información Mantiene la información documentada en la			

CONTINÚA

medida necesaria para tener confianza en que los procesos se han llevado a cabo. Garantiza que la información esté disponible y adecuada para su uso, donde y cuando sea necesario. La información está protegida en forma adecuada y controla de una manera organizada, para su distribución, acceso, recuperación y uso.	8	5	5%
TOTAL	**35**	**7**	**7%**

Según la evaluación realizada la planificación y apoyo dentro de la Asociación alcanza apenas un 7% del 35% distribuido para este criterio, con una ponderación baja en cuanto a lo que comprende estos aspectos, de ello se puede deducir que no existen acciones para para abortar riesgos, prevenir y reducir impactos no deseados, de igual manera no se han asignado recursos para la implementación de planes de continuidad.

Para efecto de resguardo de información según lo expresado en la entrevista realizada al líder del área de sistemas el proceso que realiza la asociación se basa en sacar un respaldo diariamente y otro quincenal mediante un software COBIAN, se indica el horario de respaldo de la información en un disco duro externo, normalmente se lo hace al finalizar la jornada de trabajo, y el respaldo quincenal se lo realiza de igual manera en un disco duro externo este es transportado por el jefe de sistemas cuando el sale a sus días de descanso que normalmente es los sábados, y en su ingreso el primer día de la siguiente semana los dos discos, es decir el interno y el externo pasan dentro del centro de datos, lo que se convierte en una debilidad para la seguridad de la información, de producirse algunos de los riesgos indicados anteriormente se perdería la información y por ende la paralización de las actividades normales de la empresa hasta su recuperación.

4.2.3 Evaluación de criterios; Funcionamiento, Planeación estratégica.

Tabla 12. Evaluación de Planificación estratégica

FUNCIONAMIENTO PLANIFICACIÓN ESTRATÉGICA	PUNTUACIÓN MÁXIMA	PUNTUACIÓN	PORCENTAJE TOTAL
Planificación y control operacional. Planifica, ejecuta y controla los procesos necesarios, para mitigar e implementar acciones determinadas para efectos adversos según sea necesario.	**9**	**3**	**3%**
Desarrollo de Objetivos, Políticas y Estrategias. Se han establecido requerimientos de recurso, protección y mitigación. Apropiado protocolo de comunicación interna y externa por políticas establecidas. Implementa estrategias apropiadas de control y mitigación.	15	6	6%
Procedimientos de continuidad de negocios Documenta e implementa procedimientos y cuenta con una estructura para responder al incidente perjudicial, utilizando personal con la responsabilidad necesaria, autoridad y competencia para gestionar un incidente. Tiene procesos, procedimientos finales para la activación, operación, coordinación, y respuesta de comunicación y minimizar un impacto	16	5	5%
TOTAL	**40**	**14**	**14 %**

Según el análisis realizado el resultado obtenido es de un 14% referente al 40% determinado para este criterio, lo cual refleja un valor bajo en cuanto a ponderación, por lo que se puede evidenciar que no se maneja una planificación estrategia de continuidad de negocios dentro de la Asociación.

Las políticas y procedimientos están desactualizadas, se conoce que en la actualidad se está elaborando el plan estratégico de la Asociación en general, puesto que por estar conformada por varias organizaciones, las mismas tienen su dirección estratégica individual.

4.2.4 Conclusiones de la fase de evaluación

- **De la evaluación de Liderazgo.-** Se concluye que en la actualidad la alta dirección de la Asociación no ha contemplado dentro de sus objetivos y organización interna el Sistema de Gestión de Continuidad de Negocio por lo que no han proporcionado los recursos necesarios, tampoco se ha establecido la política y las personas que implementen y mantengan la continuidad de negocio.
- **De la evaluación de Planificación y apoyo.-** Luego de efectuado la evaluación se concluye que existe debilidad en las seguridad de la información, de producirse algún incidente a causa de un riesgo latente se puede paralizar el funcionamiento de las actividades normales de la Asociación, debido a la falta de planificación para abordar los riesgos, prevenir y reducir el impactos.
- **De la evaluación de Funcionamiento, Planeación estratégica.-** La Asociación cuenta con una planeación estratégica desactualizada y la misma no contempla objetivos, políticas ni estrategias de continuidad, además en su estructura orgánica funcional no se incluye personal responsable de gestionar un incidente y comunicar los diferentes procesos para etapas de prevención y control.

4.3 Identificación riesgos existentes.

Se pudo identificar que los principales riesgos que podrían afectar al centro de datos de la Asociación son los desastres naturales, este resultado se obtiene de las encuestas realizadas en la pregunta 6, la misma que indica en un 100%, que los riesgos naturales existen y lo detallan en sus respuestas.

4.3.1 Desastres Naturales

4.3.1.1 Erupción del Volcán el Reventador

Este volcán ha pasado activo durante varias décadas, la última y de gran magnitud transcurrió en el año 2002 cuando se produjo una erupción volcánica acompañada de lava y movimientos sísmicos, la Asociación está expuesta a este riesgo por la ubicación geográfica de su campamento, la cual se encuentra a escasos kilómetros del conocido Volcán El Reventador, no se encuentra registro sobre la perdida información o activos a causa de este riesgo.

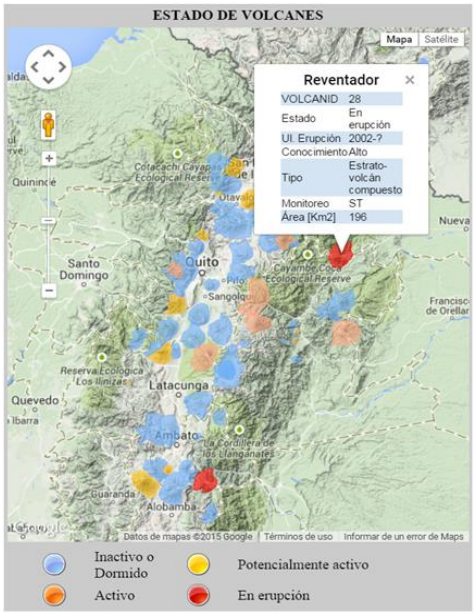


Figura 22. Estado Volcán El Reventador
Fuente: (Instituto Geofísico de la Escuela Politécnica Nacional, 2015)

Figura 23. Distancia del Volcán El Reventador hacia el Campamento la Loma
Fuente: (Google Inc., 2013)

4.3.1.2 Inundación por crecida del río Coca

El río Coca drena un porcentaje muy alto de la precipitación, debido al clima variado y muy lluvioso que existe en este sector, las instalaciones de la Asociación están ubicadas en un valle a 250 metros aprox, del rio Coca.

Las constantes lluvias producen grandes crecientes que podrían desbordar el caudal del río, se tiene registros de paralización de actividades laborales en dos puntos de trabajo del proyecto Coca Codo Sinclair, debido a la crecida del caudal del rio, llevando consigo dos puentes que servían como comunicación y envió de información.

Figura 24. Río Coca

4.3.1.3 Deslizamientos en masa

El campamento de la fiscalización está rodeado de grandes sistemas montañosos inestables que por las continuas lluvias suelen generar deslizamientos de tierra, las constante lluvia y el clima inestable ha producido una serie de deslizamientos de tierra en el último año en diferentes sectores de esta zona, algunos de gran magnitud que ha paralizado el tráfico vehicular durante varias horas.

Existen registros de perdida de información o activos ocasionados por el terremoto en el año 1987, el cual destruyo gran parte del campamento de la compañía Rodio, que se encontraba ubicado en el mismo lugar que actualmente labora la Asociación, los registros indican que además existieron pérdidas humanas.

4.3.1.4 Derrames de petróleo

Por el sector donde está ubicado el campamento de la asociación atraviesa el oleoducto y poliducto, siendo uno de los linderos del campamento, lo cual por su naturaleza genera algún grado de riesgos en caso de un accidente y el subsiguiente escape de gas las fugas o roturas de los oleoductos, que pueden causar explosiones e incendios, además el derrame de gasolinas limpias.

No existen registro alguno sobre accidentes anteriores que representan un riesgo importante para la salud humana y la infraestructura alojada en este campamento, en la siguiente figura podemos observar el lindero del campamento y el oleoducto.

Figura 25. Terreno se encuentra enterrado el oleoducto y poliducto

4.3.1.5 Asentamientos y Deforestación

El proyecto hidroeléctrico Coca Sinclair, es el proyecto de mayor magnitud en nuestro país, y se encuentra en plena construcción, a sus alrededores existen asentamientos de personas nacionales y extranjeras, generando la construcción de todo tipo de viviendas, hoteles y negocios, existiendo una total pérdida de planificación en estos asentamientos, con ello y en algún momento pueden ocasionar una disconformidad, teniendo como consecuencias la paralización de las actividades de las empresas que los rodean, incluyendo a la asociación.

La deforestación es otro factor alarmante, el campamento la loma está rodeado de montañas que contienen una biodiversidad en flora y fauna, para los asentamientos

aledaños esto lo ven como una fuente de ingresos, destruye el sostén de estas montañas y a su paso las dejan vulnerables para sufrir deslizamientos, no se encuentra registro alguno que haya ocasionado perdida de información a causa de este riesgo.

En la figura a continuación podemos observar la deforestación de una montaña que se encuentra muy cerca del campamento, esta fue destruida para la construcción y el paso de tuberías que serviría como traslado de agua entubada hacia el asentamiento o recinto de San Luis ubicado a 1,2 km del campamento.

Figura 26. Asentamientos y deforestación

CAPÍTULO V

PLAN DE CONTINUIDAD DE NEGOCIO

5.1 Introducción

En base al diagnóstico situacional realizado en el capítulo anterior se pudo conocer que la Asociación no está preparada para enfrentar una posible interrupción, pese a que el personal conoce de los riesgos que existen en la zona, desconocen también de la existencia de un proceso documentado de comunicación de crisis, de igual manera no se cuenta con una ubicación alternativa del centro de datos.

Lo que implicaría una paralización de las actividades normales de suscitarse un desastre natural, esto deja en evidencia el nivel medio de compromiso de los líderes respecto a garantizar la seguridad de la información debido a que no se han tomado la acciones necesarias para implementar un plan de continuidad de negocios, añadir también que la Asociación tampoco cuenta con la certificación de la norma ISO 22301.

5.2 Desarrollo del modelo

Los estándares, normas y buenas prácticas implementadas en diversas organizaciones a nivel mundial, surgen ante la necesidad de gestionar los riesgos y estandarizar las políticas de seguridad en las organizaciones.

El planteamiento adecuado, preparación y la comunicación son los requisitos necesarios para una exitoso plan de continuidad de negocio en caso de contingencia o desastre, ante esta situación se plantea el desarrollo de este plan el cual ayuda a establecer lo que se debe hacer para asegurar en todo momento la funcionalidad de los sistemas y disposición de la información dentro del centro de datos de la Asociación y con esto garantizar la continuidad de los procesos.

Por abarcar todos los componentes referentes a continuidad se utilizó el estándar ISO 22301 Sistemas de gestión de la continuidad del negocio, Seguridad de la sociedad, es la primera norma internacional para la Gestión de la Continuidad del Negocio y ha

sido desarrollada para ayudar a las organizaciones a minimizar el riesgo de interrupciones.

Un BCMS, como cualquier otro sistema de gestión, tiene los siguientes componentes principales: Una política, personas con responsabilidades definidas, procesos de gestión relativa a; política, planificación, implementación y operación, también se considera la evaluación del desempeño, revisión por la dirección, y mejora; Documentación que evidencia auditable; y Cualquier gestión de la continuidad de procesos de negocio relevantes para la organización.

La continuidad del negocio contribuye a una sociedad más resistente. Por lo tanto, pueden necesitar otras organizaciones la comunidad en general y el impacto del entorno de la organización y participar en el proceso de recuperación.

Esta norma contiene las siguientes clausulas para la gestión de continuidad de negocios:

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Requerimientos generales
5. Liderazgo
6. Planeación
7. Soporte
8. Funcionamiento
9. Evaluación del desempeño
10. Mejora

5.3 Alcance

Este plan de continuidad de negocio se desarrolló para salvaguardar la información que contiene el centro de datos de la Asociación Fiscalizadora del Proyecto Coca Codo Sinclair, el cual tiene alcance adaptable a su estructura y necesidad, que básicamente comprende establecer, implementar, mantener y mejorar continuamente un sistema de gestión documentado que garantice la continuidad.

Con el propósito de proteger, reducir la probabilidad de ocurrencia, prepararse, responder y además permitir la pronta recuperación de los sistemas tecnológicos, información, funciones, procesos que requieran mayor atención y proteger la información, recursos y resultados contra daños, siniestros y además que pongan en riesgo las actividades de esta área.

5.4 Contexto

5.4.1 Descripción del centro de datos de la Asociación.

El centro de datos de la Asociación, se encuentra albergada junto a las oficinas del departamento de software de control de proyecto, la misma que es parte del área de control y seguimiento de la Asociación, en esta se almacena toda la información que genera la ejecución del proyecto Hidroeléctrico Coca Codo Sinclair día a día, además se brinda soporte y administración de los sistemas informáticos al resto de áreas administrativas de la Asociación.

5.4.2 Misión.

Tener al día toda la información generada en la construcción del proyecto Hidroeléctrico Coca Sinclair y almacenarla en su sistema de información supervisión de obras civiles (SISOC), para luego comunicar a las partes interesadas que son los trabajadores de la empresa pública Coca Codo Sinclair. E.P.

5.4.3 Servicios.

Los servicios que se desarrollan y se brinda en el centro de datos de la Asociación se los detalla a continuación:

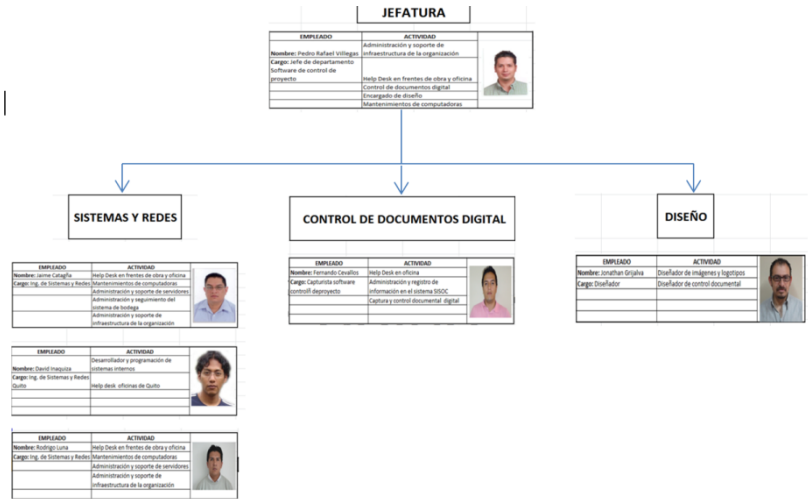
- Registro de control documental digital de información de avance del proyecto Hidroeléctrico Coca Sinclair.
- Envío de información por medio del protocolo FTP a la empresa mexicana PYPSA, para posterior subirlas a su página web.
- Registro Administración de compras activos del departamento de software de control de proyecto.

- Registro Inventario de resguardos del departamento de software de control de proyecto.
- Se realiza revisión de control de redes en todos los departamentos de la Asociación.
- Atención y mantenimiento de servidores e instalaciones.
- Se brinda soporte en todos los departamentos de la Asociación, incluyendo al personal de campo.
- Control documental de procura.
- Registro de credenciales de correo.

5.4.4 Estructura orgánica funcional del centro de datos de la Asociación

El centro de datos que funciona actualmente la Asociación está conformado por seis funcionarios que se encargan de las distintas actividades de acuerdo a los servicios que presta esta área, y se lo puede observar en la siguiente figura.

Tabla 13. Organigrama del Departamento de Sistemas y Software de Control de Proyectos



5.4.5 Sistemas Informáticos.

La Asociación dentro de su área cuenta con sistemas informáticos, los cuales brindan servicios de información. A continuación se definieron las funciones y principales características de los sistemas utilizados:

- **Sistema de Información para la Supervisión de Obras Civiles (SISOC)**.- es una herramienta para el procesamiento de la información de proyectos de construcción, cuenta con herramientas para el manejo completo de bitácoras, oficios, minutas, planos, documentos de trabajo y procedimientos, fotografías, entre otros.

  Este sistema está basado en una arquitectura cliente-servidor de 3 capas, utiliza el gestor de base de datos SQL Server y sus interfaces se encuentran desarrolladas en Java Script, la plataforma de trabajo está diseñado en un entorno preferentemente Windows XP Profesional.

- **ORACLE Primavera P6 Control de Cronograma de Proyectos**.- es la solución más poderosa, sólida y fácil de usar para priorizar, planificar, gestionar y evaluar proyectos, programas y carteras. Brinda una solución al 100% basada en tecnología web para gestionar proyectos de cualquier tamaño, se adapta a diferentes niveles de complejidad en todos los proyectos y de manera inteligente para satisfacer las necesidades de todos los roles, funciones y niveles de habilidad de su organización y equipo del proyecto.

5.4.6 Diagrama de red.

En la Figura 27. Se puede apreciar el diagrama de red organizacional con el que cuenta la Asociación, la cual consta de dos nodos principales: las oficinas matriz (en la cual se basará nuestro trabajo) y las oficinas centro ubicados en la Ciudad de Quito, el mismo que se conecta por medio de un servidor de Túnel de Datos. Adicionalmente cuenta con 3 nodos secundarios, Enlace de datos, San Carlos, Lumbaquí y Captación.

Además se posee 3 enlaces de internet por medio fibra óptica que es brindada por la empresa constructora del proyecto en los frentes de obra; Embalse Compensador y Casa de Máquinas, también existe un enlace que se recepta por radio frecuencia en la vía de acceso al Embalse Compensador kilómetro 7.

Figura 27. Diagrama de Red

5.5 Liderazgo

5.5.1 Compromiso de la dirección

El Compromiso de la Dirección se refiere a las obligaciones y responsabilidades que adquiere la alta dirección en el desarrollo y la implementación del Plan de Continuidad de Negocio.

A continuación se detallan las obligaciones o compromisos que adoptará la Dirección:

- Asegurarse que las políticas y objetivos son establecidos.
- Asegurar la integración del Plan con los procesos de negocio.
- Asegurar que los recursos necesarios para el plan estén disponibles.
- Comunicar la importancia del plan.
- Asegurar que se logre el resultado esperado.
- Nombrar las personas competentes para ser responsables de la implementación del Plan y dotarlas de la autoridad apropiada.
- Direccionar y dar soporte a las personas que contribuyen a la efectividad del plan.
- Promover la mejora continua.
- Definir los criterios de aceptación del riesgo y los niveles aceptables de riesgo.
- Participar activamente en los ejercicios y pruebas.
- Asegurar que las auditorías internas del BCP son realizadas.

- Conducir las revisiones administrativas del BCP.

5.5.2 Designar un Coordinador de Continuidad de Negocio

El coordinador o el equipo deben trabajar con la dirección para identificar el alcance y los objetivos que persigue el plan, así como las actividades de negocio que son críticas en la organización.

Adicionalmente, el perfil o perfiles de las figuras encargadas de la gestión de la continuidad de negocio no tiene que estar forzosamente localizado en las áreas de tecnología y sistemas, lo más importante es que posea una visión integral de la organización.

El coordinador de Continuidad de Negocio debe poseer:

- Habilidades de Liderazgo, para desarrollar un ambiente participativo y cooperativo.
- Buenas relaciones interpersonales.
- Capacidad analítica.
- Buena comunicación verbal y escrita.
- Orientación al logro.
- Trabajo en equipo.
- Capacidad de delegar autoridad y toma de decisiones.
- Capacidad de autogestión.

Además se recomienda evaluar el comportamiento del liderazgo en las organizaciones y así identificar al miembro del equipo que posea más capacidades de liderazgo frente al grupo para ser designado luego como Coordinador del Plan de Continuidad de Negocio.
El análisis del liderazgo se lleva a cabo por medio de la evaluación de cinco comportamientos:

- **Desafiar los procesos**: El líder se hace responsable de los riesgos que conllevan los procesos administrativos y operativos, además de la dinámica interna y externa que juegan los procesos.

- **Inspirar una visión compartida**: Se refiere a la imaginación apasionante del líder sobre escenarios futuros.

- **Habilitar a los demás a que actúen**: Esta característica se refiere a la facultad del líder para desarrollar un ambiente participativo y cooperativo, haciendo del equipo de trabajo, compañeros pro-activos.

- **Modelar el camino:** Se refiere a una alta jerarquía de valores y de igual forma una alta moralidad. Coloquialmente podría decirse: "El líder predica con el ejemplo".

- **Dar aliento con el corazón:** Es un comportamiento transaccional integrado en el Inventario de las prácticas de liderazgo. Este comportamiento se refiere a la retroalimentación positiva que el líder da a los seguidores, reconociendo públicamente las contribuciones individuales y celebrando los logros del equipo.

Sumado a lo anterior, se propone que la Asociación conforme un equipo de continuidad de negocio, principalmente por personal que pertenezca o conozca las diferentes actividades que se desarrollan dentro del área ya que los riesgos y amenazas varían en función de dicha actividad y deben ser absolutamente identificados y priorizados.

Para conformar este equipo se propone que esté integrado por un coordinador y tres miembros que sean parte de este comité.

5.6 Política de Continuidad de Negocio

5.6.1 Introducción

El objetivo global de la Continuidad de Negocio de La Asociación es realizar los preparativos necesarios y planificar un conjunto suficiente de procedimientos para responder de forma adecuada ante un incidente, desde el momento en que se declare el desastre hasta la vuelta a la normalidad, de forma que se reduzca al mínimo su impacto.

5.6.2 Alcance.

Esta política aplicará para todo el personal que labore dentro del área de software y control del proyecto para la Asociación con el fin de poder garantizar la continuidad del negocio, en caso de un evento que afecte la operación normal.

5.6.3 Objetivo.

Evitar interrupciones a los procesos críticos del negocio como consecuencia de fallas o desastres.

5.6.4 Enunciado de la Política General

Debido a que cualquier interrupción en los procesos de negocio afecta la operación, es responsabilidad de las directivas de la organización aprobar un plan de continuidad de negocio (BCP), que cubra las actividades esenciales y críticas de la Asociación.

5.6.5 Elementos de la Política

La Política de Continuidad establece un marco apropiado a las características de La Asociación (naturaleza, complejidad, criticidad de las actividades, etc.) que repercute directamente en el entorno operativo, centros de trabajo y cultura de empresa con el que identificar, desarrollar, implantar, operar, mantener, revisar y probar las medidas necesarias para garantizar el correcto funcionamiento del plan, ante la materialización de un incidente.

La Política de Continuidad se sustenta en un conjunto de principios que han sido formulados basándose en las necesidades de la Asociación y el entendimiento de los riesgos asociados como son:

- La primera premisa y el objetivo prioritario es la protección y seguridad del personal, tanto en situación normal como en situación de contingencia.

- La Dirección de Asociación se responsabilizará de la gestión de los riesgos clave para la continuidad operativa de los procesos considerados críticos para la Organización.
- La Asociación garantizará que el Plan de Continuidad de Negocio se desarrolle e implante de forma adecuada.

- La Asociación garantizará que el Plan de Continuidad de Negocio se mantenga actualizado, se revisa, se prueba y, en su caso, se mejoran de forma periódica o ante cambios significativos en premisas, personas, procesos, tecnología o estructura organizativa; para lo cual participarán activamente el área destinada.

- Se nombrará representante con la debida experiencia para que formen parte del Comités y Equipos de Continuidad de Negocio y participen en el Plan de Continuidad de Negocio.

- La Asociación garantizará que todo el personal del área esté informado de las responsabilidades que le competen en el marco de la Continuidad de Negocio, mediante labores periódicas de formación, divulgación y prueba del Plan de Continuidad de Negocio.

- La Asociación garantizará que los procesos críticos son recuperados dentro de los márgenes de tiempo requeridos en el plan.

- La Dirección garantizará la promoción y divulgación de la capacidad de Continuidad de Negocio dentro de la cultura de empresa.

5.6.6 Roles y responsabilidades.

Esta política es responsabilidad de ser aprobada por los directivos de la Asociación, luego de un estudio previo y detallado de sus posibles consecuencias, con el fin de garantizar la continuidad del negocio en caso de un evento que afecte la operación normal de los procesos críticos.

5.6.7 Violaciones a la política.

La dirección de la Asociación se compromete a desarrollar este plan, será responsabilidad de ellos, no faltar a este compromiso y tener en cuenta que al no realizar dicho plan, la Asociación pudiera estar expuesta a procesos contractuales, que pudieran poner en riesgo el futuro de la operación.

5.6.8 Revisión de la política.

Esta política debe ser modificada si existieran cambios en los procesos de negocio de la Asociación o en su infraestructura tecnológica, de no haber cambios, se debe realizar su revisión anualmente.

Para la revisión anual o de ser el caso realizar un cambio el coordinador deberá notificar a los integrantes del comité y analizar la situación de acuerdo a los resultados obtenidos en experiencias pasadas de ano haberlas se observara los cambios internos o de personal dentro de la Asociación para incrementar o disminuir lo que se considere necesario, luego de realizado los cambios, este comité planteara a los máximos directivos para su socialización y aprobación.

5.7 Planificación del Plan de continuidad

El coordinador o equipo de continuidad, debe aplicar sus habilidades en gestión de proyectos, para programar y desarrollar los componentes del plan de trabajo: tareas a llevar a cabo para satisfacer los objetivos descritos en la política de continuidad,

responsables de ejecutar tales tareas, tiempos de ejecución, hitos, presupuestos, plazos e indicadores de éxito.

Se iniciara con la ejecución de un cronograma de actividades para detallar las tareas, los tiempos de ejecución, presupuestos e indicadores, esto se detallara específicamente más adelante en el desarrollo de los planes. Para la planificación del plan se deberá tomar en cuenta las acciones consideradas en el siguiente punto.

5.7.1 Acciones para abordar los riesgos y oportunidades.

El propósito de abordar acciones de riesgos es aplicar medidas de seguridad que eviten en lo posible que se produzcan incidentes, que al no ser gestionados adecuadamente hagan necesaria la activación del Plan de Continuidad de Negocio.

Por lo tanto, en vez de esperar a que un desastre afecte a la organización para ver cómo esta se recupera, las medidas preventivas (en ocasiones denominadas contramedidas) deben ser aplicadas con el objetivo de incrementar la fortaleza de sus actividades frente a posibles impactos y para ello se considerará las siguientes medidas:

- Adquisición de seguros con diferentes grados de cobertura.
- Copias de seguridad de información que soporta una actividad crítica de la organización.
- Sistemas de detección y extinción de incendios.
- Sistemas de prevención de intrusiones, control de accesos, alarma y vigilancia.

En la siguiente tabla 14. Se puede apreciar las acciones preventivas, que proporcionan una protección ante los riesgos que pueden afectar la productividad y reputación de la organización, y que cuya ocurrencia se puede atenuar implementando controles adecuados.

Tabla 14. Acciones de prevención de riesgos

RIESGO	ACCIONES
Interrupción eléctrica.	Fuentes alternas de generación eléctrica: UPS y plantas eléctricas. Mantenimiento de las fuentes alternas de generación eléctrica. Estado de la instalación eléctrica y capacidad eléctrica instalada. Lámparas de emergencia
Fallos en el Hardware	Equipo de cómputo utilizado y obsolescencia. Capacidad de redundancia entre servidores. Monitoreo de problemas en los servidores. Contratos de mantenimiento preventivo y correctivo. Condiciones físicas y ambientales (limpieza, humedad, temperatura).
Fallos en el Software	Desarrollo local de aplicaciones (metodologías/ estándares). Cambios y configuración en aplicaciones. Trascendencia de los sistemas incluidos en el estudio.
Fallas en comunicaciones	Soporte técnico de los equipos utilizados. Mantenimiento preventivo y correctivo de los equipos de comunicación
Desastres naturales	Pólizas de seguro vigentes. Brigadas de atención ante situaciones de emergencia. Capacitación al personal. Rutas de evacuación. Iluminación de pasillos, puertas y salidas de emergencia.
Incendios	Pólizas vigentes de seguro. Sistemas automáticos y manuales contra incendio (gabinetes, extintores, aspersores). Uso de materiales retardantes del fuego. Almacenamiento de material combustible. Detectores de humo revisados regularmente
Fallas de respaldo	Procedimientos para respaldo y recuperación de información, fuentes, objetos, documentación, y configuración de los sistemas. Periodicidad de los respaldos. Facilidades y protección para el almacenamiento dentro y fuera de sitio. Configuración de los discos duros de los servidores. Documentación actualizada sobre procedimientos de respaldo y recuperación.
Violación a la seguridad física	Procedimientos para respaldo y recuperación de información, fuentes, objetos, documentación, y configuración de los sistemas. Periodicidad de los respaldos. Facilidades y protección para el almacenamiento dentro y fuera de sitio. Configuración de los discos duros de los servidores. Documentación actualizada sobre procedimientos de respaldo y recuperación.
Virus	Seguridad física para el ingreso al edificio, oficinas y cuartos de servidores y equipos de comunicación. Capacitación al personal para detectar situaciones que puedan representar riesgo o cuestionar la presencia de personas desconocidas o sin identificación. Sistemas de seguridad: circuitos cerrados de televisión, sensores de movimiento, alarmas. Revisión y control de salida e ingreso de equipo de cómputo. Utilización de bitácoras para el registro de ingresos
Hackeo	Procedimientos establecidos para otorgamiento de acceso a las aplicaciones y políticas de acceso lógico. Procedimientos establecidos para el acceso a los recursos tecnológicos (redes y aplicaciones). Administración y configuración de "firewalls". Monitoreo de los accesos tanto legítimos como ilegítimos. Disponibilidad de herramientas para el monitoreo de la seguridad.
Recursos Humanos	Dependencia en el personal. Capacitación. Documentación de las funciones del personal.

5.8 Apoyo

Es fundamental no perder de vista la relación costo beneficio de las posibles medidas a adoptar, para lograr una solución frente a este tema hay que considerar dos factores importantes; por un lado la participación y el compromiso de los involucrados en los procesos del plan y por otro disponer de la infraestructura adecuada para sustentar los procedimientos establecidos en el plan.

El apoyo fundamentalmente se enmarca desde la alta dirección quienes adquieren su compromiso con la realización del plan y se comprometen en los aspectos más importantes como son el personal, la infraestructura y los recursos.

5.8.1 Personal.

Son factores claves, contar con personal no solo capacitado sino también comprometido con las tareas que tiene que ver responder ante una contingencia y con las acciones a seguir en caso de ser necesario. Por otra parte hay que buscar no depender de las personas para la ejecución de las medidas, para ello se definirá el comité de crisis, para los cuales es necesario determinar funciones y responsabilidades, así como el nivel de autoridad requerida para llevar adelante sus tareas.

Conformar el comité es responsabilidad de la Asociación para la cual deberá tomar en cuenta:

- Habilidades, conocimientos y experiencias.
- Existencia de líneas de reporte y mando.
- No colisionar la estructura organizativa de la Asociación, sin descuidar la flexibilidad que otorga el concepto de equipos de trabajo.
- Restricciones de acceso y confidencialidad respecto a la información que se maneja.
- Compromiso personal

5.8.2 Infraestructura.

Se refiere tanto a la infraestructura edilicia, así como a los elementos tecnológicos y no tecnológicos, y demás recursos necesarios para llevar a cabo los procesos del plan, el

listado de la infraestructura básica se la define más adelante en el desarrollo de la estrategia.

5.9 Documentación del Plan de Continuidad de negocios.

Documentos que se tendrá como evidencia el plan según lo establecido por el estándar ISO 22301:

- Política de Continuidad de Negocio.
- Material que contenga los términos de referencia para que el personal identifique los términos claves.
- Análisis de riesgos de la Asociación.
- Análisis de Impacto al Negocio (BIA
- Programa de Capacitación para que cada persona tenga perfectamente definidas las tareas que debe realizar una vez declarada la contingencia.
- Plan de Evacuación. El Plan debe tener los detalles sobre la forma en que los equipos deben trasladarse al sitio alterno. Los números de contacto de las instituciones que se necesite contactar en un escenario de contingencia.
- Plan de Recuperación de Tecnología en caso de Desastre (DRP por sus siglas en inglés). Para la Continuidad de Negocio es importante contar con un Plan para la recuperación de tecnología actualizado al día, pues es el soporte principal del BCP.
- Plan de vuelta a la normalidad.

Esta documentación está desarrollada más adelante en el desarrollo de los planes.

5.10 Funcionamiento

5.10.1 Análisis de Impacto al negocio

El objetivo de un análisis de impacto es determinar de manera cuantitativa y/o cualitativa impactos, efectos, y pérdidas que podrían resultar si la organización sufre un

evento serio y establecer las funciones críticas, sus prioridades de recuperación e interdependencias a fin de determinar Tiempos del Negocio. Para ello se procederá con:

5.10.1.1 Identificación de actividades críticas.

Posterior a un análisis de investigación realizada a los diferentes procesos, se puede determinar las actividades críticas, para con ello definir el impacto que tendría la no ejecución de cierta actividad, se puede asignar una escala de valores a los siguientes factores:

- Impacto en el bienestar de los empleados.
- Daño o pérdida de la información.
- Incumplimiento de las normas legales.
- Daño de la reputación.
- Daños a la viabilidad financiera.
- Deterioro de la calidad del servicio o producto.
- Daño ambiental.

De tal forma que se ha otorgado un valor más alto a los factores que la Asociación considera más importantes de salvaguardar y viceversa. Para luego sumar los valores y poder así obtener información cuantitativa.

5.10.1.2 Procesos Soportados.

Los procesos soportados son la infraestructura tecnológica que cubre Sistemas relevantes, y los servicios que brinda el centro de datos para conocer los procesos y poder valorarlos e identificar su criticidad para emitir el informe final del Análisis de Impacto, se va a realizar la descripción de cada uno de ellos en base a la información emitida por el jefe del departamento de software de control de proyecto.

Tabla 15. Procesos relevantes infraestructura tecnológica

Procesos	Breve descripción	Frecuencia
registro de control documental de información	se encarga, de ingresar información generada por todos los frentes del Proyecto Hidroeléctrico.	diario
atención y mantenimiento de servidores e instalaciones	revisar su funcionamiento, control de su funcionalidad	diario
envío de información por medio del protocolo FTP	reportes diarios de avance se deben subir a host en México	diario
registro Inventario	registro de resguardo de equipos de computo	semanal
revisión y control de redes en todos los departamentos de la Asociación.	inspección de las redes de los departamentos, junto con sus dispositivos	diario
soporte en todos los departamentos de la Asociación	solución a Inconvenientes en dispositivos y las redes	diario
control documental de procura	registro en el sistema de control de proyectos información de procura	diario
registro de credenciales de correo	registro de identidad y contactos del personal que ingresa a laborar en la organización	semanal

- **Componentes de los procesos:**

Para calificar la criticidad a criterio del jefe del Sistemas de la Asociación, se considera una numeración ascendente 1, 2, 3, 4, 5, 6 de acuerdo a la prioridad he importancia de los procesos definidos, según los servicios que brinda el centro de datos con cada uno de los componentes Hardware, Software y comunicación. Para conocer su alcance y su prioridad.

Tabla 16. Registro del control documental de información

Nombre del Sistema	Descripción	Criticidad	Tipo de sistema (PC,Servidor)	Números de equipos con la aplicación	Localización
SISOC	Sistema para el ingreso de información	1	servidor	52	Oficinas campamento La loma

Tabla 17. Atención y mantenimiento de servidores e instalaciones

Nombre del Sistema	Descripción	Criticidad	Tipo de sistema (PC,Servidor)	Números de equipos con la aplicación	Localización
Antivirus, herramientas de limpieza lógica/física	Limpieza de virus y acumulación de polvo	2	servidor	4	Centro de Datos

Tabla 18. Envío de información por medio del protocolo FTP.

Nombre del Sistema	Descripción	Criticidad	Tipo de sistema (PC,Servidor)	Números de equipos con la aplicación	Localización
Filezilla	Conexión servidor pypsa México, para envió información	3	servidor	1	Centro de Datos

Tabla 19. Registro Inventario

Nombre del Sistema	Descripción	Criticidad	Tipo de sistema (PC,Servidor)	Números de equipos con la aplicación	Localización
ofimática	Control y actualización de resguardos de equipos de computo	4	PC	1	Oficinas campamento La loma

Tabla 20. Revisión y control de redes en todos los departamentos de la Asociación.

Nombre del Sistema	Descripción	Criticidad	Tipo de sistema (PC,Servidor)	Números de equipos con la aplicación	Localización
Aplicativos de seguridad	Revisión de puertos abiertos, computadoras, en la red y consumo	5	PC y Servidor	3	Oficinas campamento La loma

Tabla 21. Registro de credenciales de correo.

Nombre del Sistema	Descripción	Criticidad	Tipo de sistema (PC,Servidor)	Números de equipos con la aplicación	Localización
Exchange	Registro del Personal nuevo en sistemas	6	Servidor	1	Oficinas campamento La loma

Luego de conocido e identificado los procesos claves en el orden de criticidad, con la ayuda del jefe del departamento de control del software de proyectos de la Asociación, quien bajo su criterio considera la estimación de los tiempos máximos de recuperación, información de impacto que se describen en la siguiente tabla de resultados del Análisis de Impacto.

Tabla 22. Análisis de Impacto

ANALISIS DE IMPACTO						
Nombre del Departamento: Sistemas y software de control de proyecto						
Número de Personal: 7						
Procesos	**Prioridad**	**RTO**	**RPO**	**Dependencias**	**Costo Impacto**	**Consecuencia**
Registro de control documental de información	1	3 horas	5 horas	Coca codo Sinclair	9500.00	Perdida de información Daño a la reputación
Atención y mantenimiento de servidores e instalaciones	2	1 hora	3 horas	Coca codo Sinclair Asociación	3000.00	Daño o pérdida de información. Daño a deterioro de los equipos
Envío de información por medio del protocolo FTP	3	1 meses	2 Meses	PYPSA	800.00	Falta de información toma de decisiones
Registro Inventario	4	3 horas	1 día	Asociación	500.00	Pérdida de control de bienes
Revisión y control de redes en todos los departamentos de la Asociación.	5	1 hora	1 día	Asociación	300.00	Deterioro de la calidad del servicio.
soporte en todos los departamentos de la Asociación	6	1 hora	1 día	Asociación	200.00	Malestar en el personal Retrasos en los trabajos.
Control documental de procura	7	1 hora	1 semana	Departamento de control del proyecto.	100.00	Perdida de información
Registro de credenciales de correo	8	1 día	1 mes	Recursos Humanos	100.00	Malestar en el personal. Afecta al control del personal

5.10.1.3 Listado de Amenazas

Seguidamente se enlista las amenazas que se puede considerar que afecten a la Asociación debido a desastres naturales según la información recopilada.

- Erupción del Volcán El Reventador
- Deslizamiento en masa
- Derrame de petróleo
- Inundaciones por crecida del Río Coca

A continuación se enlista los daños accidentales que se puede considerar que afecten a la Asociación según la información recopilada.

- Fuego fortuito
- Fallo de suministro eléctrico
- Fallo del banco de baterías
- Accidentes del personal
- Degradación / fallo del hardware
- Fallo en las copias de seguridad de información
- Fallos en los sistemas de autenticación
- Pérdida de confidencialidad
- Incumplimiento legales

La Asociación, líder entre las organizaciones fiscalizadoras en proyectos de obras civiles nacionales, no cuenta con un Plan Estratégico Organizacional, debido a que es la fusión de 4 empresas: dos nacionales y 2 extranjeras (México), no tiene una visión definida, debido a la búsqueda de un objetivo mutuo y la satisfacción de necesidades, esto responde a no tener una relación explícitamente definida.

Con base Plan Estratégico Organizacional no definido, tampoco existe un Comité de Informática Corporativo, mucho menos un Plan Informático formulado, la única aprobación en decisiones del Departamento sería la del Jefe de Software de Control de Proyectos. Por otra parte cabe señalar que la Asociación es una organización de aproximadamente 600 empleados de los cuales 7 son dependientes directamente del jefe de Software de Control de Proyectos, único representante dentro del área de tecnología con autoridad.

Existe un reglamento interno de la Asociación que contiene cláusulas del uso apropiado de equipos de cómputo e internet que fue entregado por el departamento administrativo al personal de la Asociación. Además un reglamento de uso de las

Herramientas informáticas y equipos de cómputo, los mismos fueron comunicados vía correo electrónico, pero ninguno de los dos fueron socializados y explicados.

Actualmente el centro de datos de la Asociación, cuenta con 4 servidores: sistema de información de obras civiles, el mismo que es utilizado además para compartir información por medio de unidades de red, ocasionando que los discos duros se saturen teniendo que liberar espacio periódicamente, el servidor de primavera; está funcionando en una Workstation y una licencia de Windows 7, se realizó la adquisición de un servidor pero no se ha podido migrar por la falta de capacitación al personal a cargo.

Las instalaciones del centro de datos tienen una puerta de vidrio y aluminio, no tiene cerradura electromagnética, brazo cierra puerta y barra antipático. No consta de productos de detección y extinción de incendios, que protejan a personas y equipos críticos contra fuego, no existe una vigilancia constante mediante cámaras y sistemas de identificación de control de acceso.

Por otro lado la Asociación posee dos configuraciones computacionales idénticas de grandes magnitudes de procesamiento, que se comunican entre sí mediante un túnel de datos para compartir información una en La Loma y la otra en Quito. En ambas instalaciones se efectúan labores de soporte de sistemas para optimizar el uso de los equipamientos.

El desarrollo de proyectos informáticos es reportado al Jefe de control de Software con revisiones periódicas, El equipo que actualmente labora en el departamento de software de Control de Proyectos, está compuesto por un egresado en auditoria en sistemas, ingenieros en sistemas, ingenieros en informática, con conocimientos en hardware, redes, comunicación, operadores de consola de antivirus, ejecución en computación o programador y digitadores, este equipo ha desarrollado varias aplicaciones que están actualmente funcionando se realizó la capacitación del Uso de aplicaciones usuario por usuario y las ventajas de los mismos se comunicaron mediante Memorando.

Todos ellos son administrados por el Jefe de Software de Control de Proyectos y están bajo la dependencia del Jefe de Control y Seguimiento, El ingeniero jefe quien está a cargo del desarrollo simultáneo de varios proyectos, se turna esporádicamente con su subalterno de soporte de sistemas las cuales disponen de tiempo para ejercer labores operativas específicamente de producción.

Existe un proveedor encargado de mantenimiento de comunicaciones, estas son efectuadas mediante microondas, las mismas que se utilizan para comunicar con los diferentes frentes del proyecto Hidroeléctrico Coca Codo Sinclair, existe una revisión mensual de este proveedor, y la cual es fiscalizada por un ingeniero en informática, habido varios percances en el último año por falta de recursos y falta de gestión en adquisiciones.

Se conoce que existe un problema de licenciamiento de software, hace falta la adquisición de licencias de software para ingenieros civiles, por esta razón se ha procedido a instalar software a prueba por días, hasta que sean adquiridas.

5.10.1.4 Matriz de Riesgos

Una matriz de riesgo constituye una herramienta de control y de gestión utilizada para identificar las actividades (procesos y productos) más importantes de una empresa, el tipo y nivel de riesgos inherentes a estas actividades. Se ha utilizado la matriz de riesgos para la identificación, monitoreo, control, medición y divulgación de los riesgos.

También se ha realizado una valoración que consiste en asignar a los riesgos calificaciones dentro de un rango, para este caso se ha escogido los siguientes niveles para la probabilidad y el impacto de que ocurra un evento, en la siguiente tabla se detalla la matriz de calificación de la evaluación de riesgos:

Para la elaboración de la matriz de gestión de riesgos, la calificación y evaluación se realiza mediante valores en base a su probabilidad e impacto tomando los siguientes

índices para los riesgos con o sin control, estos valores fueron acordados con el Jefe de Sistemas de la organización evaluada.

Tabla 23. Matriz de Calificación de Evaluación de Riesgos

Probabilidad	Impacto
5 = Alta 3 = Media 1 = Baja	5 = Alta 3 = Media 1 = Baja

Tabla 24. Matriz de Calificación de Evaluación de Riesgos

MATRIZ DE CALIFICACIÓN Y EVALUACIÓN DEL RIESGO					
VULNERABILIDAD	Alta	5	5 Moderado Evitar el riesgo	15 Importante Reducir el riesgo (plan de contingencia), evitar el riesgo, compartir o transferir	25 Inaceptable Evitar el riesgo, reducir el riesgo (plan de contingencia), compartir o transferir (pólizas de seguros)
	Media	3	3 Tolerable Asumir el riesgo, reducir el riesgo (revisar el método de control)	9 Moderado Reducir el riesgo, evitar el riesgo, compartir o transferir	15 Importante Reducir el riesgo (plan de contingencia), evitar el riesgo, compartir o transferir
	Baja	1	1 Aceptable Asumir "aceptar" el riesgo (revisar el método de control)	3 Tolerable Reducir el riesgo, compartir o transferir (revisar el método de control)	5 Moderado Reducir el riesgo (plan de contingencia), compartir o transferir (compañías de seguros)
			1 Leve	3 Moderado	5 Catastrófico

En la siguiente tabla 9. Encontramos los índices de vulnerabilidad e impacto con su descripción correspondiente.

Tabla 25. Niveles Impactos

VULNERABILIDAD	Posibilidad de que ocurra un evento o resultado específico.
ALTA	Se espera que ocurra en la mayoría de las circunstancias. Es muy factible que el hecho se presente.
MEDIA	Es posible que ocurra en algunas veces. Es factible que el hecho se presente.
BAJA	Puede ocurrir solamente en circunstancias excepcionales. Es muy poco factible que el hecho se presente.
IMPACTO	(Consecuencia) Resultado de un evento expresado cualitativa o cuantitativamente, como por ejemplo una pérdida, lesión, desventaja o ganancia. Puede haber una serie de resultados posibles asociados con un evento.
CATASTRÓFICO	Afecta la operación segura del proceso y/o involucra el incumplimiento de regulaciones gubernamentales. Si el hecho llegará a presentarse tendría alto impacto o efecto sobre los objetivos de la entidad. Pérdidas financieras altas. Pérdidas humanas.
MODERADO	Permite la operación del proceso, pero bajo condiciones de desempeño reducido. Si el hecho llegará a presentarse tendría medio impacto o efecto sobre los objetivos de la entidad. Medianas pérdidas financieras. Personas lesionadas o heridas.
LEVE	No afecta la operación del proceso ni su desempeño. Si el hecho llegará a presentarse tendría bajo impacto o efecto sobre los objetivos de la entidad. Pérdidas financieras pequeñas. Bajo impacto en la salud de las personas.

A continuación se observa la matriz que contempla los riesgos detectados con su respectiva valoración, que se la realizo conjuntamente con el jefe de la área de control de software del proyecto de la Asociación, quien bajo su criterio y de acuerdo a lo analizado se considera la importancia de cada uno de los riesgos.

Tabla 26. Matriz de Riesgos

VALORACIÓN Y MAPEO DE RIESGOS

Mapa de Riesgo

NOTA: Diligencie solo las celdas que se encuentran sombreadas en color verde, las celdas restantes se encuentran bloqueadas para protección de las formulas que graficarán los riesgos.

	PROCESO	LIDER PROCESO	TIPIFICACIÓN RIESGO	RIESGO EVALUADO	OBSERVACIÓN	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS	Calificación Funcionario Nro. 1 (Director de Gerenciamiento)	Calificación Funcionario Nro. 2 (Jefe Control y Sequimiento)	Calificación Funcionario Nro. 3 (Jefe Control Software)
R1	Estructura organizacional	Gerencia General	R1	La arquitectura no esta alineada con la	No cuenta con un Plan estrategico	Alto	3.7	4.3	VOTO IMPACTO	5.0	5.0	3.0
									VOTO VULNERABILIDAD	5.0	3.0	3.0
R2	Estructura organizacional	Talento Humano	R2	Distribución inapropiada de	Único representante	Alto	3.7	4.3	VOTO IMPACTO	3.0	5.0	5.0
									VOTO VULNERABILIDAD	3.0	3.0	5.0
R3	Administracion de cambio	Jefe de Software de	R3	Incapacidad para recuperar el	No existe Plan Informática	Medio	2.3	3.7	VOTO IMPACTO	3.0	3.0	5.0
									VOTO VULNERABILIDAD	1.0	1.0	5.0
R4	Nomina inexacta de	Talento Humano	R4	Falta de personal necesario para	Personal insuficiente en las	Medio	2.3	3.0	VOTO IMPACTO	1.0	3.0	5.0
									VOTO VULNERABILIDAD	1.0	1.0	5.0
R5	Administración del proyecto	Jefe de Software de	R5	Incapacidad para identificar, priorizar,	Reglamentos de uso de	Alto	3.7	5.0	VOTO IMPACTO	5.0	5.0	5.0
									VOTO VULNERABILIDAD	3.0	3.0	5.0
R6	Administracion de activos	Jefe de Software de	R6	Uso de software y hardware no	Discos duros de servidor saturado	Alto	3.7	4.3	VOTO IMPACTO	3.0	5.0	5.0
									VOTO VULNERABILIDAD	3.0	3.0	5.0
R7	Adquisición de software	Jefe de Software de	R7	Metodología ineficaz para la	Falta de licencias de Autocad y	Alto	3.7	4.3	VOTO IMPACTO	3.0	5.0	5.0
									VOTO VULNERABILIDAD	3.0	3.0	5.0
R8	Seguridad de la Información	Ingeniero de desarrollo	R8	Falta e integridad en la información	intermitencias en el túnel de datos	Medio	3.0	3.0	VOTO IMPACTO	5.0	1.0	3.0
									VOTO VULNERABILIDAD	5.0	1.0	3.0
R9	Administración de problemas	Jefe de Software de	R9	Acciones inadecuadas e	Falta de comunicación	Medio	3.0	2.3	VOTO IMPACTO	1.0	1.0	5.0
									VOTO VULNERABILIDAD	1.0	3.0	5.0
R1	Seguridad de la Información	Ingeniero de producción	R10	Vulnerabilidad en ataques maliciosos	Compartir información por	Medio	3.0	3.7	VOTO IMPACTO	3.0	5.0	3.0
									VOTO VULNERABILIDAD	1.0	5.0	3.0
R1	Administración del proyecto	Jefe de Software de	R11	Incapacidad para manipular e	No se comunica el avance en el	Alto	3.7	4.3	VOTO IMPACTO	3.0	5.0	5.0
									VOTO VULNERABILIDAD	3.0	5.0	3.0
R1	Administración de proyectos	Jefe de Software de	R12	Incapacidad para asegurar la	Desarrollo simultaneo de	Medio	3.0	3.7	VOTO IMPACTO	1.0	5.0	5.0
									VOTO VULNERABILIDAD	1.0	3.0	5.0
R1	Administración de cambio	Jefe de Software de	R13	Pruebas insuficientes antes	Falta de pruebas globales antes de	Alto	3.7	4.3	VOTO IMPACTO	3.0	5.0	5.0
									VOTO VULNERABILIDAD	3.0	5.0	3.0
R1	Estrategias en sistemas	Ingeniero de desarrollo	R14	Desarrollo, prueba y despliegue	Software sin migrar a servidor	Medio	3.0	3.7	VOTO IMPACTO	5.0	3.0	3.0
									VOTO VULNERABILIDAD	1.0	5.0	3.0
R1	Administración de problemas	Talento Humano	R15	Incapacidad para resolver problemas	Personal no capacitado	Alto	3.7	4.3	VOTO IMPACTO	3.0	5.0	5.0
									VOTO VULNERABILIDAD	3.0	3.0	5.0
16	Seguridad de la Información	Jefe de Software de	R16	Falta de seguridad física / lógica	Puerta de acceso a Centro de	Medio	3.0	3.7	VOTO IMPACTO	1.0	5.0	5.0
									VOTO VULNERABILIDAD	1.0	3.0	5.0
17	Seguridad de la Información	Jefe de Software de	R17	Falta de seguridad física / lógica	Centro de datos con instalaciones	Alto	3.7	4.3	VOTO IMPACTO	3.0	5.0	5.0
									VOTO VULNERABILIDAD	1.0	5.0	5.0
18	Adquisición de hardware	Ingeniero de producción	R18	Equipos utilizados insuficientes	Información no integra	Medio	4.3	3.0	VOTO IMPACTO	1.0	3.0	5.0
									VOTO VULNERABILIDAD	3.0	5.0	5.0
19	Adquisición de software	Jefe de Software de	R19	Metodología ineficaz de	Metodología ineficaz de	Medio	3.7	3.7	VOTO IMPACTO	5.0	3.0	3.0
									VOTO VULNERABILIDAD	3.0	5.0	3.0
20	Admistración de activos	Gerencia Comercial	R20	Uso de software no soportado	No existe licencias de	Alto	4.3	3.7	VOTO IMPACTO	3.0	5.0	3.0
									VOTO VULNERABILIDAD	3.0	5.0	5.0
21	Delegación de responsabilidad	Jefe de Software de	R21	Falta desegregación de	Delegación de resposabilidades	Medio	3.0	3.0	VOTO IMPACTO	1.0	5.0	3.0
									VOTO VULNERABILIDAD	1.0	3.0	5.0
22	Arquitectura	Gerencia Comercial	R22	Metodología Ineficaz de	Falta de recursos y gestión de	Medio	4.3	3.0	VOTO IMPACTO	1.0	5.0	3.0
									VOTO VULNERABILIDAD	3.0	5.0	5.0
23	Administración de la	Jefe de Software de	R23	Inacapacidad para recuperarse de	Banco de baterias sin	Medio	3.7	3.7	VOTO IMPACTO	1.0	5.0	5.0
									VOTO VULNERABILIDAD	1.0	5.0	5.0
24	Operaciones	Jefe de Software de	R24	Incapacidad para archivar	Discos duros de respaldo se	Alto	4.3	3.7	VOTO IMPACTO	1.0	5.0	5.0
									VOTO VULNERABILIDAD	3.0	5.0	5.0
25	Operaciones	Ingeniero a cargo de	R25	Incapacidad para asegurar los	Discos duros transportados a	Medio	3.0	4.3	VOTO IMPACTO	3.0	5.0	5.0
									VOTO VULNERABILIDAD	1.0	3.0	5.0
26	Administración del proyecto	Jefe de Software de	R26	Incapacidad para monitorear,	Aplicaciones desarrolladas se	Medio	3.7	3.7	VOTO IMPACTO	3.0	5.0	3.0
									VOTO VULNERABILIDAD	3.0	3.0	5.0
27	Fisica y Ambiental	Gerencia General	R27	Incapacidad para administrar los	Ubicación del centro de datos	Alto	5.0	5.0	VOTO IMPACTO	5.0	5.0	5.0
									VOTO VULNERABILIDAD	5.0	5.0	5.0
28	Administración de la	Ingeniero a cargo de	R28	Incapacidad para recuperar la	Información despojada o	Alto	3.7	4.3	VOTO IMPACTO	3.0	5.0	5.0
									VOTO VULNERABILIDAD	3.0	5.0	3.0
29	Administración de la	Jefe de Software de	R29	Incapacidad para recuperarse de	No existe procedimiento en	Alto	4.3	3.7	VOTO IMPACTO	1.0	5.0	5.0
									VOTO VULNERABILIDAD	3.0	5.0	5.0

Seguidamente se puede observar en la Figura 28. El gráfico de la matriz de riesgos, en donde se muestra el grado de impacto de acuerdo a los riesgos antes enunciados.

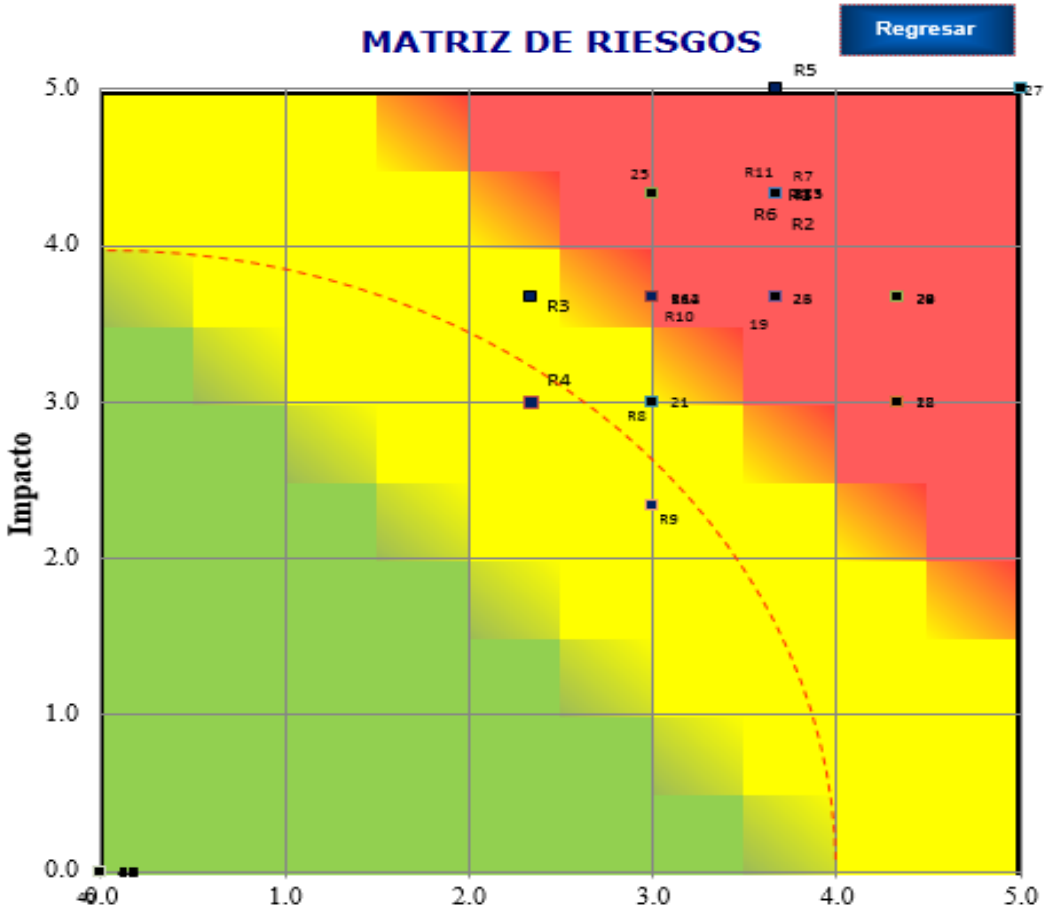


Figura 28. Gráfico de la Matriz de Riesgos

5.10.1.5 Control de Riesgos inherentes.

Una vez detectado los riesgos y su grado de afectación se define los controles para cada uno de ellos con el fin de prevenirlos o mitigarlos, con la descripción realizada en la matriz de riesgos de describirá cada control.

R1: Implementación de Organigrama de estructuración Organizacional acorde a las necesidades de la Asociación, es necesario que los directivos desarrollen el organigrama estructural contemplando los requerimientos propios de la misma,

en la actualidad existe uno el cual se tomó como referencia, a este se puede incrementar el personal que se considere para la implementación de la estrategia de continuidad.

R2: Establecer políticas para la gestión de funciones del Departamento de Control de Software de acuerdo al número de personal de la organización.

R3: Implementar un Plan Informático en base al manual de funciones y portafolio de proyectos según el organigrama vigente en la organización con respecto al departamento de Software de Control de Proyecto.

R4: Establecer políticas de contratación de personal y segregación de funciones.

R5: Implementar políticas de utilización para los sistemas de información.

R6: Realizar partición en discos duros de almacenamiento específicamente para Sistema de Información de Obras Civiles.

R7: Revisar que el inventario de software y hardware se encuentre actualizado cada mes.

R8: Monitoreo del cifrado de la información antes de ser enviada.

R9: Manual de procedimientos y capacitar al personal con nuevas herramientas eficaces para la tomo de decisiones.

R10: Ejecución de ethical hacking.

R11: Establecer parámetros de tiempos de trabajo desde el Inicio.

R12: Contar con un profesional capacitado y con experiencia probada en el área. Probabilidad de cubrir plazos de entrega.

R13: Verificar que el software utilizado cumpla con las normas y estándares de interconexión para la entidad.

R14: Implementar políticas de documentación y manuales de funcionamiento de los sistemas.

R15: Establecer planes de capacitación para los ingenieros de soporte.

R16: Implementación de puerta de acceso a centro de datos adecuada para seguridad de información con los estándares necesarios.

R17: Implementación de medidas de seguridad física en el Centro de datos.

R18: Monitoreo del cifrado de la información antes de ser enviada.

R19: Disponer de las normas y políticas para la adquisición de software necesario para la aplicación.

R20: Revisar los planes de renovación de equipos y los planes de actualización de software acorde al crecimiento de la organización.

R21: Analizar las áreas críticas y contratar nuevo personal.

R22: Evaluar la factibilidad económica para la realización de nuevos proyectos.

R23: Realizar solicitud para instalación de energía trifásica al proveedor.

R24: Establecer un adecuado almacenamiento de los respaldos.

R25: Contratar empresa de seguridad para el traslado de información crítica hacia el lugar de almacenamiento.

R26: Planes de capacitación anual de tecnología.

R27: Implementación del plan de continuidad para recuperación ante una interrupción causada por un desastre.

R28: Implementar políticas de seguridad técnica y contratación de personal para movilización de información.

R29: Implementar un procedimiento para comunicación en crisis, el mismo que funcione dentro del Campamento la Loma, se propone un modelo en el desarrollo de la estrategia.

5.11 Estrategia de continuidad de negocio.

Luego de haber evaluado los riesgos detectados, se seleccionara una estrategia de recuperación de negocio que asegure la continuidad de los procesos que se ha considerado críticos en el Análisis de Impacto.

De las alternativas existentes y dado que la opción de subcontratar espacios y soporte a terceros resultaría muy cara para la Asociación, la estrategia para la continuidad del negocio sería adecuar un centro de datos en la oficinas centrales de la Asociación Quito como alternativa en caso de incidencia grave, de esta forma la Asociación podría seguir dando servicio, sin que el impacto de un incidente tuviera consecuencias catastróficas. Para ello, se requiere:

- Espacio físico para 3 servidores, los mismos se ubicaran dentro de un rack, adicional a esto instalaciones de energía, puntos de red, detector de humo y demás señales de seguridad.
- Se requerían licencias de sistemas operativos de acorde a la necesidad de cada servidor.

Adicional es necesario que:

- Los respaldos que se generen sean más periódicos.
- Que los discos duros sean transportados a las oficinas de la ciudad de Quito en el departamento de TI, para su alojamiento y resguardo físico.

- El transporte de los respaldos de información deberán ser transportados por una persona ajena a la Asociación, puede ser una empresa de servicios de seguridad.
- Se deberá realizar Acuerdos de Nivel de Servicios con la empresa que transporta los respaldos, además asegurarse que reciban un salario digno.

Se considera también los siguientes recursos para la continuidad:

- El Personal.- con el fin de mantener el conocimiento y las capacidades del personal con funciones y responsabilidades en actividades críticas, se ejecutara un plan de capacitación y formación, se determinara las tareas claves a realizarse y se debe realizar simulacros con el personal a cargo de poner en funcionamiento el sitio alterno, y pruebas de los servicios.
- Información: Se verificara que se posea la información necesaria para dar continuidad a las operaciones del negocio, deben estar integras, disponibles y confidencialidad aunque se esté en las instalaciones alternas. Como parte de las estrategias de información, y siendo este tema muy sensible, es necesario elaborar respaldos de la información. También como medida se seguridad adicional, los respaldos pueden resguardarse en una bóveda especial.

5.11.1 Recursos económicos para la implementación de la estrategia.

Para poner en marcha esta estrategia es necesario determinar los recursos económicos que se requiere para adaptar los aspectos que describe la misma, si bien es cierto que la inversión podría ser considerable pero hay que tener en cuenta que en comparación con las pérdidas que podría ocasionar un desastre inesperado si es recomendable.

A continuación se detalla los recursos necesarios para la implementación del sitio alterno para el centro de datos en la siguiente tabla 29.

Tabla 27. Presupuesto para implementación de estrategia.

CANTIDAD	EQUIPOS	DETALLE	VALOR UNITARIO	VALOR TOTAL
3	Servidores Proliant HP	Un servidor para el SISOC. Un servidor para la primavera. Un servidor para unidades de red.	$ 3.500.00	$ 10.500.00
1	varios	Instalaciones (Rack, patch panel, switch capa 3 de 24 puertos y cableado.)	$ 7.000.00	$ 7.000.00
TOTAL				$ 17.500.00

5.12 Procedimientos de continuidad de negocios.

De suscitarse algún desastre o imprevisto para la continuidad del negocios se proseguirá de acuerdo a los siguientes procedimientos.

- **Procedimiento de notificación del desastre:** Personal de la Asociación que sea consciente de un incidente grave que puede afectar a la empresa, debe comunicar a su jefe inmediato y este a su vez al comité de crisis para su respectiva evaluación.

- **Procedimiento de ejecución del plan:** Una vez notificado del incidente el Comité de crisis se reunirá en el punto de encuentro definido, se evaluará el grado del incidente y decidirá si el Plan de Continuidad del Negocio es puesto en marcha la alarma de recuperación a desastre estará a cargo del Director de Gerenciamiento.

- **Procedimientos para incidentes:** Los incidentes relacionados con tecnología de la información y de la comunicación son informados telefónicamente al coordinador de continuidad de negocios que será parte del comité para funcionamiento de sitio alterno, los mismos serán del personal de Software de Control de Proyectos. El Jefe de control de Software será el encargado de dar declaraciones sobre los sucesos, basándose en hechos reales.

5.13 Planes de continuidad de Negocios.

5.13.1 Plan de Evacuación.

Esta se podría considerar como la fase de Alerta define los procedimientos de actuación ante las primeras etapas de un suceso que implique la pérdida parcial o total de uno o varios servicios críticos.
Se dividirá en tres partes:

- **Notificación:** Cualquiera del personal de la Asociación que descubra un incidente puede dar aviso inmediatamente a su jefe inmediato y este a su vez al comité de crisis, cabe indicar que como parte del plan es importante establecer un programan de concientización, en el que se informe debidamente al personal de cómo actuar ante estos casos y a quién comunicar lo ocurrido.

Tabla 28. Cuadro Fase de Notificación

Nro.	EVENTO	ACCIÓN
1	Situación de contingencia/incidente detectado por algún empleado de la compañía	Aviso inmediato con el máximo detalle posible a su jefe inmediato
2	El jefe conoce que ha sucedido una contingencia.	Aviso a la persona de contacto del Comité de Crisis

- **Evaluación:** Una vez que un miembro del Comité de Crisis es contactado e informado del incidente, procederá a evaluar la situación con la recopilación de la mayor información posible. El Comité informará de la situación y tomara la decisión de disparar el Plan o iniciar otro tipo de estrategia.

- **Ejecución del Plan:** Una vez que el Comité de Crisis ha decidido poner en marcha el Plan, debe de iniciarse el árbol de llamadas (En el Anexo B se incluye un ejemplo de un árbol de llamadas) para comunicar a los Responsables para dar inicio de las actividades del Plan para comenzar los procedimientos de actuación de cada uno de ellos. Deberá informarse también a la alta Dirección.

Para poner en marcha el plan de evacuación es necesario definir responsabilidades y crear el comité de crisis.

El objetivo de este comité es reducir al máximo el riesgo y la incertidumbre en la dirección de la situación. Este Comité debe tomar las decisiones "clave" durante los incidentes, además de hacer de enlace con la dirección de la compañía, manteniéndoles informados de la situación regularmente.
Las principales tareas y responsabilidades de este comité son:

- Análisis de la situación.
- Decisión de activar o no el Plan de Continuidad.
- Iniciar el proceso de notificación a los empleados a través de los diferentes responsables.
- Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación.

Tabla 29. Listado de Integrantes del Comité.

Responsable del Comité	Jefe de departamento de software de control de proyectos que actúa como coordinador
Miembros del comité.	La Asociación seleccionara los integrantes del comité de acuerdo a sus requerimientos, considerando las observaciones descritas en numeral 5.5.2 y serán tres personas como mínimo.

Lugar de Reunión: Área de Recursos Humanos

Una vez que se comunica un incidente, el Comité de Crisis debe reunirse y tomar decisiones para afrontar la situación y proceder de acuerdo a lo siguiente:

- **Procedimiento de concentración y traslado de material y personas**: Notificados todos los equipos involucrados y activados el Plan, deberán acudir al centro de reunión indicado, además del traslado del personal al centro de recuperación hay que trasladar todo el material necesario para poner en marcha las actividades.

- **Procedimiento de puesta en marcha del centro de recuperación**: Una vez que el equipo de recuperación llegue al Centro de recuperación y que los materiales empiecen a llegar, pueden comenzar a instalar las aplicaciones en los equipos que se encuentran en esta oficina.

5.13.2 Plan de Recuperación

Una vez que hemos establecido las bases para comenzar la recuperación, se procederá a la carga de datos y a la restauración de los servicios críticos.

Lo dividiremos en dos fases:

- **Procedimientos de Restauración**: Estos procedimientos se refieren a las acciones que se llevan a cabo para restaurar los sistemas críticos.
  El orden de recuperación de las funciones se realizará según la criticidad los sistemas: SISOC, primavera, los dos primeros sistemas deben recuperarse lo antes posible, en las 48 horas siguientes. Los demás sistemas pueden esperar a recuperarse después Filezilla, ofimática, Exchange y aplicativos de seguridad.

- **Procedimientos de soporte y gestión:** Una vez restaurados los sistemas hay que comprobar su funcionamiento, realizar un mantenimiento sobre los mismos y protegerlos, de manera que se reanude el servicio con las máximas garantías de éxito.
  Los integrantes del área de control de software del proyecto serán los encargados de comprobar y verificar el correcto funcionamiento de los procesos.

5.13.3 Plan de vuelta a la normalidad.

Luego de solventada la contingencia y con los procesos críticos en marcha se planteara las diferentes estrategias y acciones para recuperar la normalidad total de funcionamiento. Para ello se divide esta fase en diferentes procedimientos:

- **Análisis del impacto:** Es el momento de realizar una valoración detallada de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad. Para ello, el comité de coordinación, realizará un listado de los elementos que han sido dañados gravemente y son irrecuperables, así como

de todo el material que se puede volver a utilizar para que determinar las acciones necesarias que lleven a la operación habitual lo antes posible.

- **Procedimientos de vuelta a la normalidad:** Una vez determinado el impacto deben establecerse los mecanismos que en la medida de lo posible lleven a recuperar la normalidad total de funcionamiento. Estas acciones incluyen las necesidades de compra de nuevos equipos, mobiliario, material, según los resultados del impacto causado.

  El Comité de Crisis contactará con el seguro de la compañía para conocer qué parte cubre el seguro (dependiendo del tipo de póliza contratada por la Asociación y qué inversión tendrá que hacer la compañía en el material que no se pueda recuperar. Contactar con los proveedores para que en el menor tiempo posible reponga todos los elementos dañados.

5.14 Evaluación de Rendimiento

Luego de solventar el incidente y vuelto a la normalidad, el equipo encargado deberá realizar un informe de las acciones llevadas a cabo y sobre el cumplimiento de los objetivos del Plan de Continuidad, los tiempos empleados, dificultades con las que se encontraron, toda esta información servirá para valorar si el Plan ha funcionado según lo planeado, así como conocer los posibles fallos, y en su caso, tenerlos en cuenta para la adecuación del mismo, para ello la Asociación:

- Evaluará la conducta de los procedimientos de continuidad de negocio y capacidades con el fin de garantizar su idoneidad continua, adecuación y efectividad;

- La Asociación periódicamente evaluara el cumplimiento de los requisitos legales y reglamentos aplicables, mejores prácticas, conformidad final con sus propios

objetivos finales política de continuidad del negocio.

- Evaluará la conducta en intervalos planificados y cuando se produzcan cambios significativos

5.15 Mejora Continua

La Asociación seguirá adoptando acciones de mejora para corregir las situaciones presentadas y realizar cambios en el plan de continuidad si es necesario, para ellos se recomienda:

- Actualización y mantenimiento de las políticas y procedimientos que contiene el plan.
- Establecer un programa de capacitación periódica del personal.
- Capacitar al personal de las nuevas tecnologías en cuanto a seguridad de la información.
- Utilización de nuevas herramientas para el monitoreo de la redes y equipos de cómputo de la Asociación adquiridas por sugerencia de las capacitaciones.
- Actualización del personal que conforma el comité de crisis cada, para evitar que quede inactivo por salida de alguno de los integrantes o de su líder.
- Revisión y pruebas continúas del funcionamiento los implementos de seguridad física en el centro de datos como; extintor, detector de humo, puertas de emergencia y cámaras de seguridad.
- Hacer conocer al personal nuevo sobre la existencia y funcionamiento del plan de continuidad.
- Revisar periódicamente la integridad de los respaldo de información.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones.

Una vez finalizado el presente trabajo se concluye lo siguiente:

- El estándar utilizado ISO 22301 – 2012, se ajusta a las necesidades de la Asociación, por su flexibilidad de adaptación a cualquier organización, sin importar su tipo, tamaño y naturaleza, lo cual permitió realizar con éxito el plan de continuidad.
- Después del análisis realizado se conoce los riesgos y las debilidades existentes dentro del centro de datos de la Asociación y considerando los beneficios motiva a implementar el plan de continuidad dentro de esta área.

- El diseño del plan de continuidad realizado, comprende todos los aspectos que considera la norma ISO 22301, abarcando los resultados de los análisis de la Asociación, por lo que se considera una modelo adaptable y que puede ser implementado en cualquier momento.

- Con la aplicación del plan de continuidad de negocios propuesto la Asociación estará preparada para enfrentar los riesgos y minimizar los impactos, garantizando su pronta recuperación de las actividades normales y fundamentalmente preservando la seguridad de la información.

- Para la implementación del BCP se requiere del apoyo y compromiso de la Alta dirección y el personal encargado de ejecutarlo, para aprobarse, actualizarse y documentarse en forma completa en los procesos críticos y operativos.

- La metodología propuesta en el presente trabajo, puede servir para implementar un programa de continuidad de negocios para grandes empresas hidroeléctricas a nivel nacional e internacional.

6.2 Recomendaciones

Luego de haber analizado la aplicación de la norma ISO 22301, en el desarrollo del plan de continuidad de negocio aplicado al centro de datos se recomienda:

- Sugerir a la Asociación tome en consideración la propuesta del plan de continuidad desarrollado para el centro de datos, a fin de proteger la información y garantizar la continuidad de los procesos de servicios que presta este departamento que son la base sustentable para llevar acabo su principales actividades.

- Socializar el presente plan de continuidad a todo el personal de la Asociación, para concientizar las acciones y medidas correctivas, que se puedan tomar sin haberse implementado el plan, además de brindar una idea clara y de prevención ante desastres o incidentes que se puedan presentar.

- Capacitar al personal para que ayude adquirir habilidades básicas para la integración dentro del plan.

- Adoptar la norma ISO 22301, para las demás áreas de la Asociación, para asegurar la continuidad mediante un completo sistema de gestión de continuidad de negocios.

- Contar con la certificación ISO 22301.

BIBLIOGRAFÍA

Alberto Alexander Servat, P. (2012). *Nuevo Estándar Internacional* . Obtenido de Gestión Continuidad de Negocio: https://gestion.com.do/~gestioo9/pdf/018/018-nuevo-estandar-internacional.pdf

Bureau Veritas. (Septiembre de 2012). (P. S. Cruz, Editor) Obtenido de https://www.interempresas.net/FeriaVirtual/Catalogos_y_documentos/87942/Continuidad_Negocio-ISO-22301.pdf

Constitución de la República del Ecuador. (2008). *Sección Novena*. Obtenido de Gestión del Riesgo: http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

Dexconsultores NTC ISO 22301:2012. (2012). *Gestión de la Continuidad del Negocio.*

DRI International. (2014). *Gestión Continuidad de Negocio-BCM*. Obtenido de www.drii.org

Google Inc. (10 de 07 de 2013). *Google Earth*. Obtenido de kh.google.com: https://www.google.es/intl/es/earth/index.html

Hurtado, d. B. (2000). *La Investigación proyectiva*. Obtenido de http://pcc.faces.ula.ve/Tesis/Especialidad/Lic.%20Rosa%20M.%20Paredes%20M/CAPITULO%20III.pdf

Instituto Geofísico de la Escuela Politécnica Nacional. (10 de 01 de 2015). *Instituto Geofísico de la Escuela Politécnica Nacional* . Obtenido de Escuela Politécnica Nacional-EPN: http://www.igepn.edu.ec/red-de-observatorios-vulcanologicos-rovig

ISACA. (2012). *Administración y Fundamentos de Continuidad de Negocio*, 5. (K. C. Barrientos, Editor) Obtenido de http://www.isacacr.org/archivos/Presentacion%20BCM%20Karol%20Cordero.pdf

Jimenéz, L. (2007). Guía de Desarrollo de un Plan de Continuidad de Negocio. Madrid.

Norma ISO 22301. (2012). *Sistemas de Gestión de la Continuidad de Negocio.* Seguridad de la Sociedad.

Professional Evalution and Certification Board. (2012). *ISO 22301 PORTAL*. Obtenido de http://pecb.org/iso22301es/

Sabino. (1985). *Uso sistemático de nuestros sentidos en la búsqueda de los datos que necesitamos para resolver un problema de investigación".*

Stefan, T., & Dave, A. (2012). *Continuidad de Negocio*. Obtenido de ISO 22301 Cuando las cosas realmente van mal: http://es.scribd.com/doc/261212484/Continuidad-del-Negocio-ISO-22301-Cuando-las-cosas-van-realmente-mal-by-Stefan-Tangen-and-Dave-Austin-pdf#scribd

GLOSARIO DE TÉRMINOS Y ABREVIATURAS:

Actividad.- Proceso o conjunto de procesos emprendidos por una organización (o en su nombre) que produce o apoya una o más productos y servicios. Ejemplo Dichos procesos incluyen cuentas, Informática, fabricación, distribución. (Norma ISO 22301, 2012)

Auditoría.- Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría. (Norma ISO 22301, 2012)

Plan de Continuidad de Negocio.- Procedimientos documentados que guían a las organizaciones responder, se recuperan, reanudar, y restaurar a un nivel predefinido de operación seguida a interrupción. (Norma ISO 22301, 2012)

Acción correctiva.- Acción para eliminar la causa de una no conformidad y para prevenir la recurrencia, reduciendo impactos e impidiendo que se repita. (Norma ISO 22301, 2012)

Eficacia.- Grado en que las actividades planificadas se realizan y alcanzan los resultados planificados. (Norma ISO 22301, 2012)

Evento.- Aparición o cambio de un conjunto particular de circunstancias que pueden tener causas severas. (Norma ISO 22301, 2012)

Incidente.- Situación que podría ser o podría dar lugar a una alteración, pérdida, de emergencia o crisis. (Norma ISO 22301, 2012)

Sistema de Gestión.- Conjunto de elementos interrelacionados o que interactúan de una organización para establecer políticas y objetivos, y procesos para alcanzar dichos objetivos. (Norma ISO 22301, 2012)

Monitoreo.- Determinar el estado de un sistema, un proceso o una actividad. (Norma ISO 22301, 2012)

Evaluación de Desempeño.- Proceso de determinación de resultados medibles. (Norma ISO 22301, 2012)

Política.- Intenciones y dirección de una organización como expresan formalmente por la alta dirección. (Norma ISO 22301, 2012)

Procedimiento.- Especificada manera de llevar a cabo una actividad o un proceso. (Norma ISO 22301, 2012)

Proceso.- Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados. (Norma ISO 22301, 2012)

Registro.- Declaración de los resultados logrados o evidencia de las acciones realizadas. (Norma ISO 22301, 2012)

Requisito.- Necesidad o expectativa establecida, generalmente implícita u obligatoria, de una práctica habitual para la organización y partes interesadas. (Norma ISO 22301, 2012)

Recursos.- Todos los activos, las personas, las habilidades, información, tecnología (incluyendo planta y equipo), locales, y suministros y la información (electrónico o no) que la organización tiene que tener disponible para su uso, cuando sea necesario, en orden para operar y cumplir su objetivo. (Norma ISO 22301, 2012)

Riesgo.- Efecto de la incertidumbre en los objetivos, Es el efecto de una desviación de la esperada - positiva o negativa, que conlleva a diferentes aspectos y pueden aplicarse a distintos niveles. (Norma ISO 22301, 2012)

Alta dirección.-Persona o grupo de personas que dirige y controla en la organización al más alto nivel, tiene la facultad de delegar autoridad y proporcionar los recursos dentro de la organización. (Norma ISO 22301, 2012)

Cobian.- Software que tiene la función de la creación de copias de seguridad o respaldo de información, puede ser en un equipo de cómputo o una red local, con la utilización de pocos recursos, además posee un fácil acceso a la programación de respaldos.

Filezilla.- Software que tiene la función de transferir archivos mediante la conexión de FTP (Protocolo de Transferencia de Archivos), debidamente conectados a una red basada en arquitectura cliente-servidor.

Ofimática.- Es el conjunto de herramientas o aplicaciones informáticas, que permiten la creación, transmisión o visualización de información necesaria en un lugar de trabajo.

Microsoft Exchange.- Software propietario de Microsoft, es un aplicativo que ofrece soluciones de Mail y directorios, predestinadas para la utilización en servidores con una sola base de datos de almacenamiento.

Ethical hacking.- Utilizar tecnologías de ataque para localizar fallas de seguridad, con la autorización del dueño de la organización, con el objetivo de optimizar la seguridad de su información.