FACULTAD DE POSGRADOS

DISEÑO DEL SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO BASADO EN LA NORMA ISO 22301 PARA EL CENTRO DE OPERACIÓN DE TRANSMISIÓN DE CELEC EP TRANSELECTRIC

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

Profesora Guía

Mgt. Katalina Coronel Hoyos

Autor

Manuel Eduardo Romero Torres

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

Declaro haber dirigido el trabajo, Diseño del Sistema de Gestión de Continuidad de Negocio Basado en la Norma ISO 22301 Para el Centro de Operación de Transmisión de CELEC EP TRANSELECTRIC, a través de reuniones periódicas con el estudiante Manuel Eduardo Romero Torres, en el semestre Octubre – Marzo 2017, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

_____

Mgt. Katalina del Rocío Coronel Hoyos

CC. 1711000016

DECLARACIÓN DEL PROFESOR CORRECTOR

Declaro haber revisado este trabajo, Diseño del Sistema de Gestión de Continuidad de Negocio Basado en la Norma ISO 22301 Para el Centro de Operación de Transmisión de CELEC EP TRANSELECTRIC, del estudiante Manuel Eduardo Romero Torres, en el semestre Octubre – Marzo 2017 dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

_____

Ing. Carlos Andrés Regalado Moncayo

CC. 1716459373

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

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

_____

Ing. Manuel Eduardo Romero Torres

CC. 1713204525

AGRADECIMIENTOS

Quiero agradecer a Dios y a la Virgen María por brindarme la fuerza para concluir mi sueño y por iluminar mi sendero.

A mi madre por ser mi ejemplo de constancia y valentía quien con mucha ternura y cariño camina a mi lado desde siempre.

A mi esposa por su amor, su alegría y ser mi fuerza en todo momento, quien con pasión forja cada día un sueño hermoso llamado hogar.

A mi estimada guía y maestra, Ing. Katalina Coronel, quien con sus conocimientos y consejos colaboró para concluir este objetivo.

Manuel Eduardo Romero Torres

DEDICATORIA

Este trabajo se lo dedico a una persona especial en mi vida.

Al amigo que me encargó la mejor Tarea desde que me dio su mano, teniendo segundos de vida.

A mi seguidor de pasos y caminos, que cada día me exige ser mejor y lograr todos mis sueños.

Al compañero que tuvo que esperar hasta que esta obra terminara y en muchos momentos le hice falta en nuestros juegos y travesuras.

Gracias por entender y esperarme, seguro debió ser tarea compleja, lo fue para mí, estar sin mi compañero de aventuras.

A mi hijo Juan Diego.

Manuel Eduardo Romero Torres

RESUMEN

Ecuador ha planificado cumplir sus objetivos nacionales en base a su Plan del Buen Vivir; dentro de estos objetivos se han definido políticas y lineamientos estratégicos como es el de reestructurar la matriz energética. El Centro de Operación de TRANSELECTRIC es el encargado de supervisar y controlar la transmisión de la energía eléctrica en el Ecuador, contribuye de gran manera a la consecución de estas metas. TRANSELECTRIC ha definido indicadores operativos para el sistema S.N.T. muy elevados y para cumplir con sus responsabilidades debe contar con todas sus herramientas y recursos necesarios.

El presente trabajo propone un esquema de implementación un Sistema de Gestión de la Continuidad del Negocio para el Centro de Operación de Transmisión, haciendo una descripción de los requisitos definidos en estándares mundiales como la ISO 22301, se realiza un análisis de la situación actual del COT, una descripción de procesos y sistemas existentes, se establece las actividades y los requerimientos mínimos necesarios para continuar con la Operación en casos de un evento de falla total, se realiza el análisis de riesgos sobre sus activos de información y se definen controles para administrar los riesgos, lo cual, conjuntamente con el análisis de impacto de negocio, permitió establecer estrategias y requisitos detallados de continuidad que permita soportar las exigencias que implica entregar la energía al país, se determinaron los recursos para implementar un Sitio Alterno y los escenarios y disparadores para iniciar el trabajo desde esta instalación, y se estructuraron mecanismos de auditoría y mejora continua para este sistema.

ABSTRACT

Ecuador has planned to meet its national objectives based on its Plan for Good Living. Within these objectives, strategic policies and guidelines have been defined, such as restructuring the energy matrix. The TRANSELECTRIC Operations Center is responsible for supervising and controlling the transmission of electric energy in Ecuador, and contributes greatly to the achievement of these goals. TRANSELECTRIC has defined very high operational indicators for the S.N.T., and to fulfill its responsibilities must have all its necessary tools and resources.

This paper proposes an implementation scheme for a Business Continuity Management System for the Transmission Operation Center, describing the requirements defined in global standards such as ISO 22301, an analysis of the current situation of the TOC, a description of existing processes and systems, the activities and the minimum requirements necessary to continue the Operation in cases of a total failure event, performed the risk analysis on its information assets and defined controls to manage the Risks, which along with the business impact analysis, allowed the establishment of detailed strategies and requirements to support the continuity requirements involved in delivering energy to the country, the resources to implement an alternate site and the scenarios and triggers to start working from this installation as well as structured audit and continuous improvement mechanisms for this system.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

1. CAPÍTULO I. INTRODUCCIÓN

1.1 Antecedentes

La Corporación Eléctrica Ecuatoriana CELEC EP está constituida por varias Unidades de Negocios, entre las cuales se destaca TRANSELECTRIC, empresa encargada de la transmisión de energía en Ecuador, cuyas funciones principales son la operación, el mantenimiento y la expansión del Sistema Nacional de Transmisión. S.N.T. (CELEC EP – TRANSELECTRIC, 2012).

TRANSELECTRIC cuenta con su Centro de Operación de Transmisión, COT, conformado por un grupo multidisciplinario de profesionales que administran una compleja plataforma tecnológica, con sistemas informáticos, de comunicaciones y auxiliares específicos, cuya razón fundamental es operar ininterrumpidamente el S.N.T, las 24 horas los 365 días del año. La disponibilidad de funcionamiento de este Centro debe ser la máxima posible. (Adaptado de Amores, 2014, p.3-4).

El manejo de la continuidad de funcionamiento del COT y de sus diversos elementos tecnológicos se lo han venido trabajando y desarrollando, en base a un cúmulo de conocimientos y buenas prácticas, que han mantenido su operación en un nivel elevado de disponibilidad. Los riesgos que se pueden presentar en el desempeño de sus operaciones han sido manejados con una arquitectura tecnológica robusta y redundante en sus componentes constitutivos.

Su servicio ininterrumpido se ha basado en actividades de control y asistencias técnicas no formales y los procedimientos de restauración y continuidad de sus equipos y sistemas, se los ha llevado de una manera informal, dependiendo en su gran mayoría de la experiencia de sus responsables.

Por su alto nivel crítico y su funcionalidad requerida se ha concebido el manejo de una contingencia extrema, habilitando un Centro de Operación alterno

ubicado en otra empresa del Sector Eléctrico Ecuatoriano. Durante varios años este nivel de respaldo parcial ha funcionado, cuando ha sido requerido; en contadas ocasiones ambos Centros han trabajado como sitios alternos respectivamente. Pero este procedimiento es informal, lo que no garantiza el nivel de respaldo con la celeridad requerida. En la actualidad bajo un inminente problema con el volcán Cotopaxi se está implementando un nuevo Centro de Contingencia en otra ciudad del país.

Por la sensibilidad e importancia de sus funciones es indispensable que todos los componentes estén regidos por un sistema que gestione su continuidad operacional en base a marcos referenciales y estándares al más alto nivel, como son las normas ISO 22301 e ISO 31000 entre otros; de igual manera se deberían formalizar los procedimientos relacionados con la continuidad de negocio, realizando un control de los riesgos a éstos asociados y el impacto que puede sufrir la continuidad del negocio en condiciones de emergencia, de tal manera que se brinde un servicio adecuado, eficiente y efectivo a sus clientes internos y externos.

1.2 Objetivos

1.2.1 Objetivo General

Diseñar el Sistema de Gestión de Continuidad de Negocio (SGCN) basado en la norma ISO 22301 para el Centro de Operación de Transmisión de CELEC EP.

1.2.2 Objetivos Específicos

1. Determinar una metodología propia para implementar un SGCN para el COT a partir de los procesos relacionados de COBIT 5 y la norma ISO 22301.
2. Definir el estado actual del Centro de Operación de TRANSELECTRIC con relación a los requisitos de la norma.
3. Analizar los riesgos y el impacto de los mismos en la continuidad del servicio del COT en base a la norma ISO 22301.

4. Diseñar la estrategia documental y el plan de implementación del Sistema de Continuidad de Negocio para el COT.

1.3 Justificación de la Investigación

Las organizaciones modernas deben satisfacer los intereses de sus varios involucrados en su normal desenvolvimiento, alineándose a los requerimientos de sus clientes internos y externos; cumpliendo diversos tipos de expectativas: económicas, legales, así como ambientales de una manera ética y responsable. (ISACA b. 2012, p.18-19). Para lograr este objetivo es importante que la razón de ser de la empresa, su visión y misión, sean viabilizadas a través de una operatividad continua en sus actividades, evitando interrupciones o que los eventos que puedan detener su operación sean manejados o controlados de una manera eficiente y en el caso de que ocurrieran, la empresa pueda responder de manera apropiada con lo que reducirá drásticamente el daño ante cualquier incidente. (Adaptado de Coronel, K. (s.f.) p.8)

La implementación de un Sistema de Gestión de Continuidad de Negocio (SGCN) asegura que la operación se mantenga, lo que permitirá mejorar el resultado operacional de la empresa reflejado en una reducción de riesgos que a su vez se traducen en una minimización de tiempos de inactividad y mejora la competitividad empresarial; lo que permitirá una mayor eficacia operativa, (ISO 22301, 2014) brindará protección de los bienes materiales y del conocimiento o “Know how” del negocio, se mejorará en el cumplimiento de las legislaciones de Seguridad y Salud y en general se incrementará la Seguridad Global de la empresa. (ISO 22301, 2013).

La figura 1 esquematiza el SGCN, en la que se muestran como entradas los requisitos de la continuidad de las partes interesadas del negocio, los mismas que a través de procesos y acciones estructuradas, producen los resultados esperados sobre los aspectos de continuidad, todo esto regido y supervisado por actividades de mejora continua.

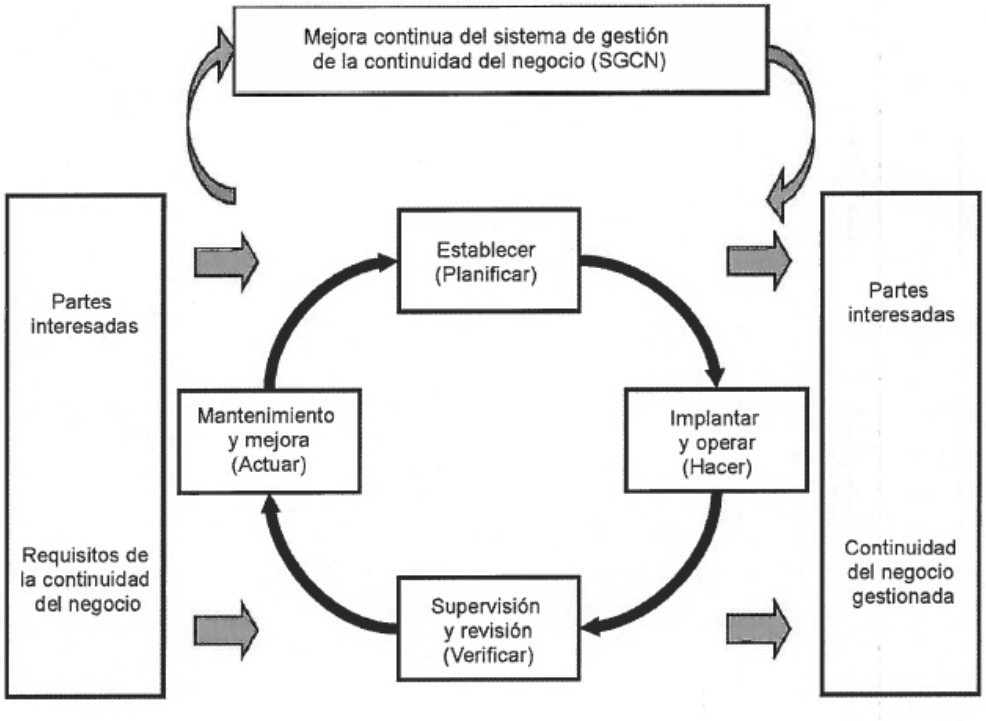


Figura 1 Modelo PDCA aplicado a procesos de SGCN.

Tomado de Asociación Española de Normalización, 2015a, p.8.

A continuación, se detalla en la Tabla 1 las etapas y actividades que conllevan la implementación del modelo Planificar, Hacer, Verificar y Actuar o PDCA, por sus siglas en inglés (Plan, Do, Check, Act), dentro de un Sistema de Gestión de la Continuidad del Negocio.

Tabla 1
Componentes del Modelo PDCA.

Fase	Detalle
Planificar (Plan)	Etapa en la cual se establecen: la Política de Continuidad del Negocio, sus objetivos, metas, controles, procesos y procedimientos necesarios para mejorar la Continuidad del Negocio.
Hacer (Do)	Fase en la cual se debe implantar y operar: la Política de Continuidad, controles, procesos y procedimientos de la Continuidad del Negocio.
Verificar (Check)	Etapa que permite supervisar y revisar el rendimiento según los objetivos y Política de Continuidad, informar los resultados a la dirección para su revisión y determinar correctivos y mejoras.
Actuar (Act)	Período para mantener y mejorar el SGCN aplicando las medidas correctoras y reevaluando su alcance, así como la Política y los objetivos de la continuidad del negocio.

Adaptado de AENOR, 2015a, p.8.

La implementación del SGCN se debe basar en un correcto manejo de los riesgos mediante su identificación, análisis y luego de evaluarlo se debería dar tratamiento del mismo. A través de este proceso las organizaciones se comunican y consultan con sus partes involucradas, monitorean y revisan el riesgo y los controles que lo están modificando, con el fin de garantizar que no se requiere de tratamiento adicional del riesgo. (Adaptado de Instituto Ecuatoriano de Normalización, 2014, P. iv)

En la figura 2 se muestra el proceso de la gestión de riesgos.

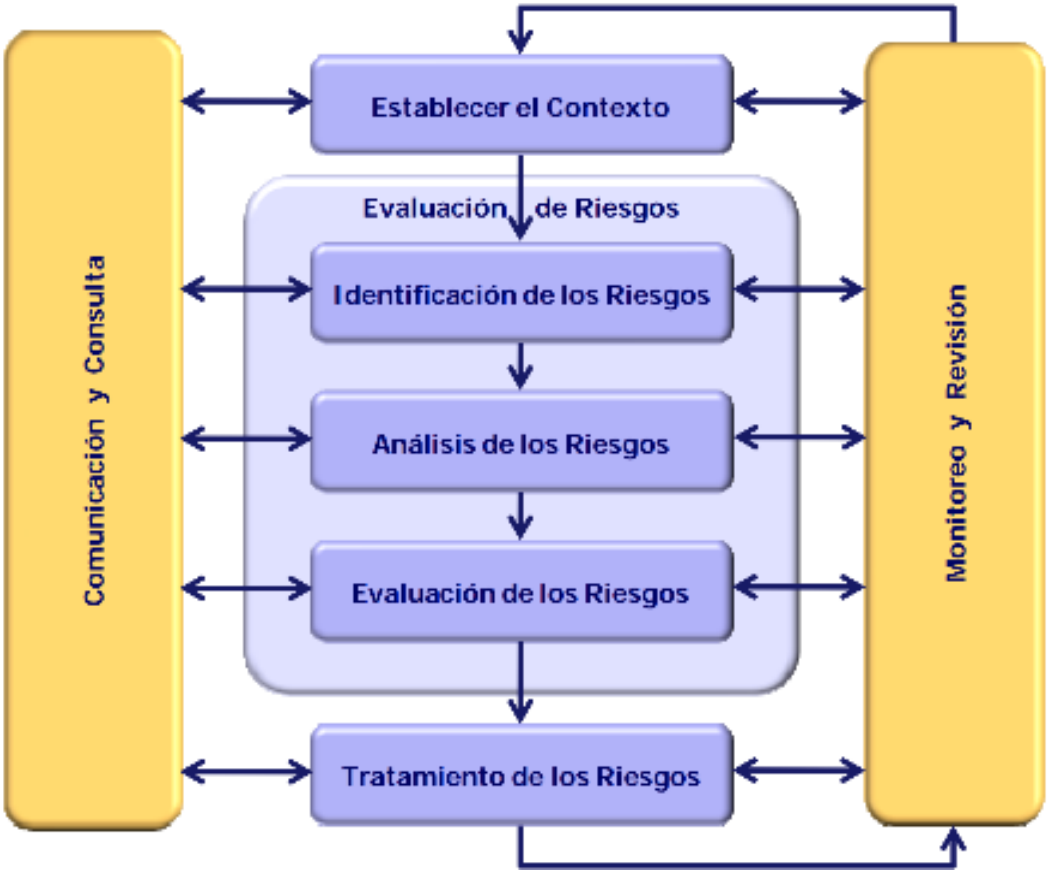


Figura 2 Proceso para la gestión de riesgos.
Tomado de Instituto Ecuatoriano de Normalización, 2014, p.14.

1.4 Aspectos Metodológicos

El presente trabajo de titulación se realizará a través de las siguientes fases y metodologías:

1. Consolidación de un marco teórico que sustente el trabajo y que permita la accesibilidad a quien analice la investigación.

2. Colección de información del Centro de Operación de Transmisión de CELEC EP TRANSELECTRIC; arquitectura de su sistema SCADA, así como sus comunicaciones específicas e infraestructura existentes.

3. Análisis de todas las entradas de información, validación de documentos existentes, análisis y creación de matrices con el fin de identificar los riesgos, impactos y frecuencias. (Adaptado de Técnicas de Estudio, (s/f*.). Metodología de la Investigación*.)

4. Entrevistas y talleres de trabajo con autoridades y el personal responsable del Centro de Operación de Transmisión y sus diferentes secciones de apoyo, durante las diferentes fases del trabajo, con la finalidad de definir actividades procesos o las actividades mínimas requeridas definidas de cada una de las unidades que conforman la organización. (Adaptado de Kosutic, D. ,2013).

5. Estructuración de servicios, productos y recursos mínimos requeridos y de todos estos analizar sus riesgos y el impacto en el desarrollo de sus actividades, maniobras y estrategias de recuperación con sus respectivos responsables.

6. Se investigará la estructura de la norma ISO 22301, y se determinará su aplicabilidad a la infraestructura del COT, como un proceso que mantendrá un ciclo de mejora continua para brindar la sostenibilidad requerida por la Institución.

7. Definición y documentación de objetivos y el alcance mínimo acordados de la política de continuidad del negocio e imbricar la planificación de continuidad en la cultura empresarial. (Adaptado de ISACA B, 2012, p.186)

8. Definición de elementos que aporten a la determinación de prioridades para la implementación del Sistema de Continuidad de Negocio.

2. CAPÍTULO II. MARCO TEÓRICO

2.1 Conceptos y requisitos de la norma ISO 22301

Continuidad de Negocio (CN)

Es la capacidad de la organización para continuar suministrando sus productos o servicios a niveles predefinidos aceptables después de un incidente disruptivo.

- Nota: Incidente es una situación que podría provocar o conducir a una interrupción, una pérdida, una emergencia o una crisis. (AENOR, 2015a, p. 12).

Gestión de la Continuidad de Negocio (GCN)

Proceso de gestión holístico que identifica las amenazas potenciales para la organización, así como los impactos en las operaciones del negocio, que tales amenazas pueden causar en caso de materializarse. Adicionalmente proporciona el contexto para aumentar la capacidad de resiliencia de la organización, con la finalidad de responder eficazmente y salvaguardar los intereses de sus principales partes interesadas, la reputación, la marca, y las actividades de creación de valor de la misma.

- Nota: Resiliencia es la habilidad de una organización y de sus recursos de absorber el impacto de un incidente y continuar entregando un nivel mínimo aceptable de servicio. (Flores, S., Araujo, V. & Flores, V. 2015, p.131)

Sistema de Gestión de la Continuidad del Negocio (SGCN)

Es parte del sistema de gestión global empresarial que establece, implanta, opera, supervisa, revisa, mantiene y mejora la continuidad del negocio. (Adaptado de AENOR, 2015a, p.10).

Requisitos de la Norma ISO 22301

La norma de Sistema de Gestión de Continuidad de Negocio está conformada por 7 secciones o requisitos, las cuales se detallan a continuación en la siguiente tabla:

Tabla 2
Requisitos de la Norma 22301.

NORMA ISO 22301				
Sección	**#**	**Título de sección**	**#**	**Requisitos de la norma**
	4	*Contexto de la organización*	4,1	Entendimiento de la organización y de su contexto.
			4,2	Entedimiento de las necesidades y expectativas de las partes interesadas.
			4,3	Determinación del campo de aplicación del sistema de gestión.
			4,4	Sistema de Gestión de la Continuidad del Negocio
	5	*Liderazgo*	5,1	Liderazgo y compromiso
			5,2	Compromiso de la dirección
			5,3	Política
			5,4	Funciones, responsabilidades y autoridades de las organizaciones
	6	*Planificación*	6,1	Acciones para cubrir los riesgos
			6,2	Objetivos de la continuidad del negocio y planes para conseguirlos.
	7	*Apoyo*	7,1	Recursos.
			7,2	Competencia.
			7,3	Concienciación.
			7,4	Comunicación.
			7,5	Información documentada.
	8	*Operación*	8,1	Planificación y control operacional.
			8,2	Análisis de Impacto en el Negocio BIA y Valoración del Riesgo VA.
			8,3	Estrategia de continuidad de negocio.
			8,4	Establecimiento e implementación de procedimientos de continuidad de negocios.
			8,5	Pruebas y ensayos.
	9	Evaluación del desempeño	9,1	Supervisión, medición, análisis y evaluación.
			9,2	Auditoría interna.
			9,3	Revisión de la gestión.
	10	Mejoras	10,1	No conformidad y acción correctora.
			10,2	Mejora continua.

Adaptado de AENOR, 2015a, p.17-33.

2.2 Objetivos, propósito y beneficios del Sistema de Gestión Continuidad de Negocio

2.2.1 Objetivos de SGCN

1. **Preservar la seguridad de las personas.**
2. Maximizar la defensa de la imagen y la reputación de la organización.
3. Minimizar el impacto causado por los eventos (incluyendo crisis) a los clientes.
4. Limitar o prevenir impactos más allá de los dominios internos y externos de la organización.
5. Proteger los activos de la organización.
6. Atender a las exigencias legales y reglamentarias. (Flores, S., et al. 2015, P.17)

2.2.2 Propósito y beneficios del SGCN

En una organización el implantar la norma de SGCN, permite demostrar la capacidad de la empresa para seguir funcionando con normalidad en caso de producirse una interrupción, minimizando sus debilidades y acentuando así sus fortalezas. La norma permite a las organizaciones:

- Proporcionar a las partes interesadas confianza en su conformidad y compromiso con las buenas prácticas reconocidas internacionalmente.
- Ser coherentes con la Política de continuidad del Negocio.
- Determinar el nivel mínimo aceptable de productos y servicios para que la organización consiga su objetivo.
- Ser medible.
- Proporcionar un lenguaje común en la organización y a nivel global.
- Determinar los requisitos aplicables.
- Definir procedimientos de seguimiento, control y actualización.

- Conservar la información documentada sobre los objetivos de continuidad. (Adaptado de Lloyd's Register Quality Assurance España, 2016.)

2.3 Procesos de COBIT orientados a la Continuidad de Negocio

COBIT 5 es un marco de trabajo integral que ayuda a las Organizaciones a crear un valor óptimo a partir de las Tecnologías de Información, es decir permite mantener información de calidad para apoyar las decisiones de negocio, generar un valor comercial de las inversiones habilitadas por estas tecnologías, proporciona las directrices para lograr las metas estratégicas y mejoras al negocio mediante un uso eficaz e innovador de las Tecnologías de Información, manteniendo un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos. (Adaptado de ISACA. 2012c. P.4-6)

COBIT 5 se basa en 5 principios fundamentales que se muestran a continuación:

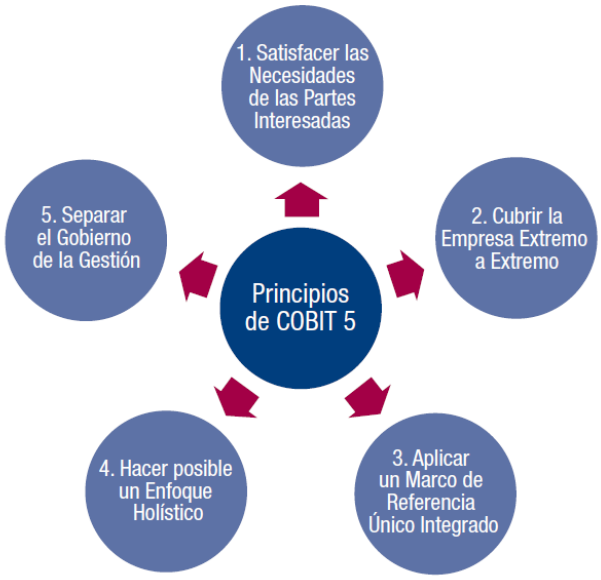


Figura 3 Principios de COBIT 5.

Tomado de ISACA, 2012b, p.13.

Para lograr un enfoque holístico, COBIT 5 hace uso de siete catalizadores, los cuales son factores que, individual o colectivamente, influyen sobre el funcionamiento y la gestión empresarial, los mismos que son:

1. Principios, políticas y marcos de referencia.
2. Procesos.
3. Estructuras organizativas.
4. Cultura, ética y comportamiento.
5. Información.
6. Servicios, infraestructura y aplicaciones.
7. Personas, habilidades y competencias.

De los siete catalizadores de COBIT 5 se analizará el segundo, los **Procesos**, que describen un conjunto organizado de prácticas y actividades para alcanzar los objetivos y producir resultados esperados. (ISACA, 2012b, p.27).

COBIT 5 recomienda que las empresas implementen procesos de gobierno y de gestión, procesos relacionados con las actividades de tecnologías de la información (TI), éste es un modelo complejo e integral, que brinda la posibilidad de acoplarse completamente a las necesidades de cada organización. (Adaptado de ISACA, 2015b, p.32).

Los procesos de COBIT 5 han sido clasificados en cinco dominios, entre los cuales un dominio es del área de gobierno y los cuatro restantes son del área de gestión:

Tabla 3
Clasificación de los dominios de COBIT 5.

Procesos de Gobierno de TI Empresarial			
Evaluar, Orientar y Supervisar			
Procesos de la Gestión de TI Empresarial			
Alinear, Planificar y Organizar	Construir, Adquirir e Implementar	Entregar, Dar servicio y Soporte	Supervisar, Evaluar y Valorar

Adaptado de ISACA, 2015b, p.33.

Dentro de la clasificación anterior existe un total de 37 procesos en COBIT 5, los cuales se detallan en el anexo 1. Modelo de Referencia de Procesos.

De todos los procesos de COBIT 5 se analizarán los enfocados en la Continuidad de Negocio y la Gestión de riesgos:

Tabla 4
Procesos de COBIT 5 enfocados a la Continuidad.

Proceso	Dominio	Sigla	Área
Asegurar la Optimización del Riesgo	Evaluar, orientar y Supervisar	EDM03	Gobierno de TI.
Gestionar el Riesgo	Alinear, Planificar y Organizar	APO12	Gestión de TI
Gestionar la Continuidad	Entregar, Dar Servicio y Soporte	DSS04	Gestión de TI

Adaptado de ISACA, 2015b, p.33.

2.3.1 Evaluación de Capacidad de Procesos

COBIT 5 incluye un modelo de capacidad de procesos, basado en la norma ISO/IEC 15504 de Ingeniería de Software-Evaluación de Procesos, este modelo permitirá la evaluación de procesos y apoyo a la mejora de los mismos. Proporcionará las herramientas para medir el desempeño de cualquier proceso sea este de gobierno o de gestión, identificando áreas de mejoras. (Adaptado de ISACA, 2015b, p.41).

La capacidad de los procesos para COBIT 5 se lo resume a continuación:

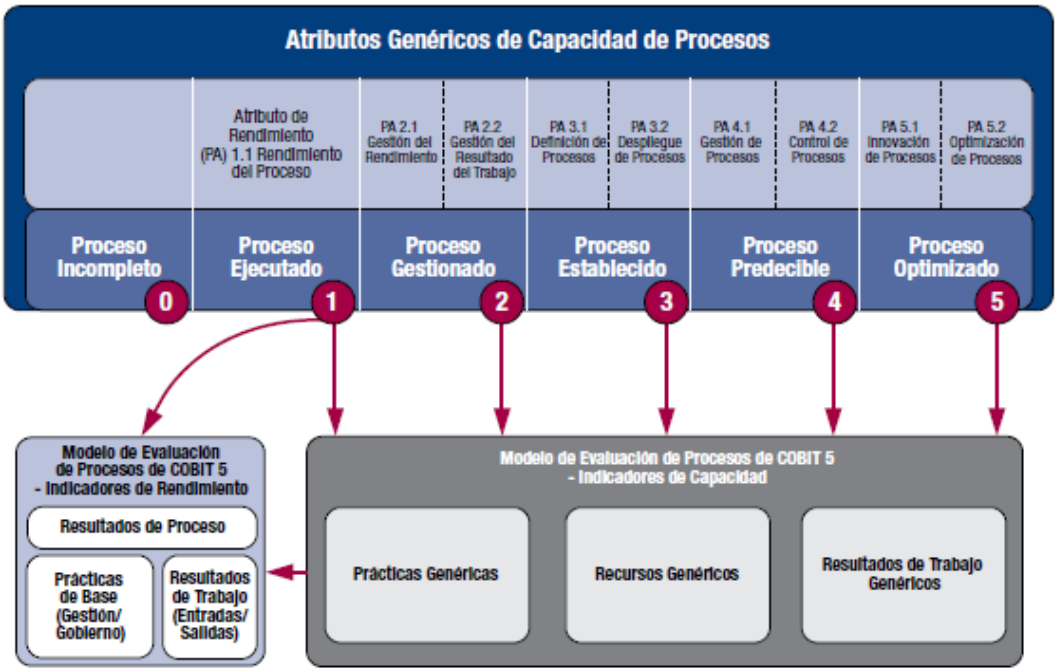


Figura 4 Resumen de Modelo de Capacidad COBIT 5.

Tomado de ISACA, 2012b, p.42.

Existen seis niveles de capacidad que se pueden alcanzar por un proceso, incluida la designación de “proceso incompleto”.

Tabla 5
Nivel de Capacidad de COBIT 5.

Nivel de Proceso	Descripción del nivel alcanzado
0 Incompleto	Proceso no implementado no alcanza su propósito. No hay evidencia de logro sistemático.
1 Ejecutado	El proceso implementado alcanza su propósito.
2 Gestionado	El proceso ya está implementado de forma gestionado (planificado, supervisado y ajustado) y los resultados son establecidos, controlados y mantenidos apropiados.
3 Establecido	El proceso gestionado está implementado usando un proceso definido capaz de alcanzar sus resultados.
4 Predecible	El proceso establecido se ejecuta dentro de límites definidos para alcanzar sus resultados.
5 Optimizado	El proceso predecible es mejorado de forma continua para cumplir con las metas empresariales presentes y futuras.

Adaptado de ISACA, 2015b, p.42.

La evaluación distingue entre evaluar el nivel 1 de capacidad y los niveles superiores, el nivel 1 de capacidad describe si un proceso alcanza su objetivo establecido, es decir se ejecuta con éxito y la organización obtiene los resultados esperados y es por tanto un nivel fundamental de conseguir. Si del resultado no se alcanzara el nivel se puede definir un plan de mejora.

La evaluación se la puede realizar mediante la revisión de los resultados del proceso, tal y como se describen para cada proceso en la descripción de sus detalles, para este efecto se usan las escalas y ratios definidos en el estándar ISO/IEC 15504. (Adaptado de ISACA, 2015b, p.45)
La escala definida se detalla a continuación:

Tabla 6
Escalas y ratios de evaluación de capacidad de procesos.

Escala	Descripción	Logro
N No alcanzado	Hay poca o ninguna evidencia de los logros del atributo en la evaluación del proceso.	0% al 15%
P Parcialmente alcanzado	Hay alguna evidencia de aproximación y un logro del atributo en la evaluación del proceso. Algunos aspectos de la realización del atributo pueden ser impredecibles	>15% al 50%
L Ampliamente alcanzado	Hay evidencia de un enfoque sistemático y de un logro significativo del atributo evaluado. Alguna debilidad relacionada con el atributo puede existir en el proceso.	>50% al 85%
F Completamente alcanzado	Existe evidencia de un enfoque completo y sistemático, y la plena realización del atributo definido en el proceso de evaluación. No hay debilidades significativas en relación a este atributo.	>85% al 100%

Adaptado de ISACA, 2015b, p.45.

2.4 Metodología para la Implementación del Sistema de Gestión de Continuidad basado en la Norma ISO 22301

Para la implementación del Sistema de Gestión de Continuidad de Negocio es fundamental contar con el apoyo de la gerencia de la organización, con esa directriz y los objetivos del Sistema de Gestión de Continuidad claros y establecidos es necesario realizar las siguientes fases y actividades: (Adaptado Segovia A., 2016, P.8.-13)

Tabla 7
Metodología de Implementación de un Sistema de Gestión de la Continuidad basado en la norma ISO 22301.

#	Fase	Actividad
1	Identificar los requerimientos del proyecto.	Definir el contexto de la organización.
2	Definir el alcance del proyecto.	Identificar el campo de aplicación del SGCN y sus exclusiones.
3	Validar la intención de la dirección	Formular la Política de Continuidad de Negocio.
4	Establecer las responsabilidades de los participantes.	Determinar las habilidades y condiciones de los responsables.
5	Identificar los riesgos de incidentes disruptivos.	Realizar el Análisis de Riesgo.
6	Identificar prioridades y objetivos de continuidad.	Realizar el Análisis de Impacto del Negocio.
7	Determinar prioridades y recursos necesarios para su mitigación.	Establecer las estrategias de continuidad.
		Definir los procedimientos de continuidad.
		Identificar el Plan de Continuidad.
8	Definir las pruebas y mecanismos de verificación.	Definir y revisar el plan de pruebas.
9	Realizar auditorías internas.	Establecer los procedimientos de supervisión del SGCN.
		Realizar auditorías internas.
10	Revisar periódicamente los planes y acuerdos de continuidad	Definir el plan de mejoras.

Adaptado de Segovia A., 2016, P.8.-13.

A continuación, se detallan las actividades de cada fase:

2.4.1 Contexto de la organización

De la organización se evaluarán todos los factores de vital importancia para conseguir su finalidad y sus operaciones en busca de alcanzar los objetivos previstos, así como los que afectan a su capacidad para obtener el resultado deseado de su SGCN.

Siendo estos factores externos e internos, se incluyen en los primeros: aspectos políticos, sociales, culturales, financieros, tecnológicos, etc., y en los segundos: objetivos, estrategias, productos, servicios, políticas, sistemas, flujos de información, etc.

Es necesario determinar cuáles son las necesidades urgentes y cuáles son las expectativas exigidas por el SGCN, siempre cuidando de no salirse del aspecto legal y reglamentario. (AENOR, 2015b, p.13-16).

2.4.2 Campo de aplicación del SGCN y sus exclusiones

En el campo de aplicación se señalarán los productos y servicios, localizaciones, funciones, proveedores, procesos y actividades, así como sus interdependencias, las mismas que formarán parte del SGCN; de igual manera se documentará y se explicará qué parte de la organización queda excluida (AENOR, 2015b, p. 16).

2.4.3 Política de Continuidad de Negocio

La alta dirección deberá definir la Política de Continuidad del Negocio, en función de los objetivos de continuidad en concordancia con los objetivos de la organización y sus obligaciones, dado el tamaño de la empresa, su naturaleza y complejidad.

A continuación, se esquematizan las condiciones que debería tener la Política del SGNC.

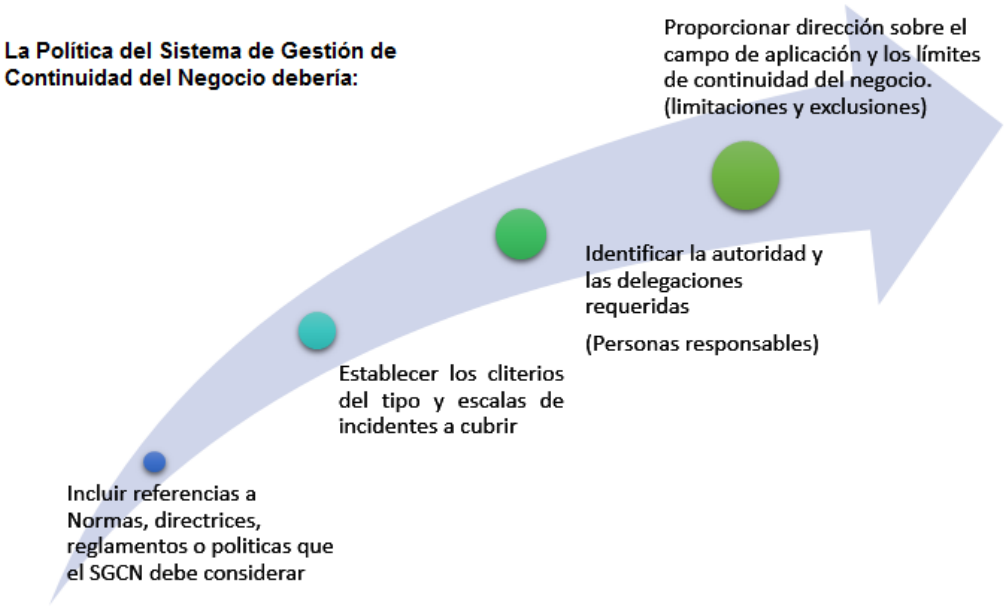


Figura 5 Condiciones de la Política del SGCN.
Tomada de AENOR, 2015b, p.18.

2.4.4 Habilidades y condiciones de los responsables

La dirección debería determinar las competencias que se requieren para todas las funciones del SGCN, así como las responsabilidades y la concienciación, el conocimiento, el entendimiento, los perfiles y la experiencia que se necesita para satisfacerlas. (AENOR, 2015b, p.21).

2.4.5 Gestión de Riesgos

Es el proceso por el cual se analizarán los activos de información y las amenazas a las cuales están sujetos en función de las vulnerabilidades de los mismos, estimando la probabilidad de ocurrencia y la magnitud del impacto. La reducción del riesgo a niveles aceptables se logra tomando acciones preventivas, correctivas o de contingencia. (Adaptado de INEN, 2014, p.14)

Para que la **gestión de riesgos** sea eficaz, la organización deberá cumplir con los siguientes principios en todos los niveles.

- ✓ Crea y protege valor.
- ✓ Es sistemática, estructurada y oportuna.
- ✓ Se basa en la mejor información disponible.

- ✓ Es una parte integral de todos los procesos de la organización.
- ✓ Es fundamental en la toma de decisiones.
- ✓ Aborda explícitamente la incertidumbre, su naturaleza y la forma en la que se puede tratar.
- ✓ Se alinea con el contexto externo e interno del perfil del riesgo.
- ✓ Toma en consideración los factores humanos y culturales.
- ✓ Es transparente e inclusiva, permitiendo a las partes involucradas estar correctamente representadas y hacer que sus puntos de vista se tomen en consideración.
- ✓ Es dinámica, reiterativa y receptiva al cambio.
- ✓ Facilita la mejora continua de la organización. (Adaptado de INEN, 2014, p.7-8)

2.4.6 Análisis de Impacto en el Negocio

El Análisis de Impacto en el Negocio conocido comúnmente como BIA, de sus siglas en inglés (Business Impact Analysis), es un proceso por el cual se determinarán las prioridades y los objetivos de la continuidad de negocio y su recuperación, la finalidad del BIA es:

- Obtener un conocimiento de los productos y servicios esenciales y de las actividades que proporciona la empresa.
- Determinar prioridades y plazos para la reanudación de actividades.
- Identificar la probabilidad de que se requieran recursos esenciales para la continuidad y recuperación. (AENOR, 2015b, p. 32).
- Documentar el impacto.
- Identificar el análisis de impacto desde las diferentes ópticas del negocio pudiendo estos ser: **Estratégico, Táctico u Operacional.**
- Identificar el Punto Objetivo de Recuperación de la información digital o electrónica, necesaria para reiniciar las actividades de la empresa. (RPO).
- Determinar un tiempo objetivo de recuperación de operaciones (RTO).

- Proveer información precisa para toma de decisiones estratégicas. (Adaptado de Flores, S., et al. 2015, P.83).

2.4.7 Estrategia de Continuidad de Negocio

Se buscarán todas las estrategias de continuidad que permitan prevenir la interrupción de las actividades prioritarias que fueron identificadas en el BIA y en la gestión del riesgo. Las estrategias seleccionadas facilitarán la reanudación de las actividades con un nivel de operación y tiempo acordados. (AENOR, 2015b, p. 34).

Al identificar las estrategias de continuidad se deberán considerar todos los recursos disponibles sin minimizar ninguno, a continuación se señalan los recursos.

Tabla 8
Recursos para el SGCN.

Recursos	Detalle
Personal	Tiempo para cumplir funciones y responsabilidades.
	Lista de reserva. Planificación de sucesiones.
	Formación, educación, concienciación y prueba.
Instalaciones	Ubicaciones. (locales alternativos en emergencia)
	Infraestuctura para el trabajo.
Tecnologías	De la Información.
	De las Comunicaciones.
Información Documental	Impresa.
	Electrónica.
Comunicación	Partes interesadas.
Finanzas	Provisión de fondos necesarios disponibles. Compras de emergencia. Reembolso de gastos de personal.
Transporte	Translado de personal a otras ubicaciones alternativas. Garantízar medios logísticas y rutasa.
Proveedores	Compromisos adquiridos. Acuerdos de nivel de servicio.
Suministros	Inventarios mínimos requeridos. Almacenamientos adicionales.

Adaptado de AENOR, 2015b, p. 20.

2.4.8 Procedimientos de continuidad

Se identificarán y documentarán los procedimientos que proporcionen una respuesta ante cualquier incidente disruptivo, que permita reanudar las actividades de la organización en tiempos predeterminados. Los procesos de continuidad deberán ser: específicos, flexibles, enfocados y eficaces. (AENOR, 2015a, P.43)

2.4.9 Plan de Continuidad

Un plan de continuidad del negocio puede ser un procedimiento documentado sencillo o múltiples procedimientos que abarquen todos los requisitos que cubran el campo de aplicación del SGCN. A continuación se muestran los elementos básicos necesarios del mismo:

- Objetivos,
- Funciones y responsabilidades,
- Criterios y procedimientos de activación y desactivación,
- Finalidad y campo de aplicación,
- Procedimiento de implantación,
- Interdependencias e interacciones internas y externas,
- Procesos al flujo de información y documentación,
- Gestión del incidente. (AENOR, 2015b, P.47)

2.4.10 Informe de plan de pruebas.

Se debe diseñar un plan de prueba para validar que la continuidad del negocio funcione como se esperaba; para lograrlo se debe comprobar lo siguiente:

- Sistemas técnicos, logísticos, administrativos, de procedimiento, etc.
- Ejercitar a las personas con responsabilidades dentro de los procedimientos de continuidad.
- Probar las disposiciones y la infraestructura de continuidad del negocio.
- Validar la recuperación de la tecnología y las telecomunicaciones. (AENOR, 2015b, P.54)

2.4.11 Procedimientos de Supervisión del SGCN

Se definirán procedimientos para garantizar el rendimiento y la eficacia del SGCN, los mismos que deberán incluir:

- Establecimiento de métricas cuantitativas y cualitativas.
- Supervisión de la amplitud con la que se cumple la política y los objetivos de continuidad.
- Identificación de cuando se deben realizar la supervisión y la medición.
- Registro de datos y resultados de medición y control para posterior análisis de las acciones correctoras. (AENOR, 2015b, P.56)

2.4.12 Auditorías internas

Se deberán establecer auditorías internas a tiempos programados para garantizar el SGCN y proporcionar a la alta gerencia información sobre la conveniencia y eficacia del trabajo realizado. (AENOR, 2016b, P.59)

2.4.13 Mejoras

Las no conformidades se las debe identificar y se deben aplicar acciones necesarias para controlarlas, contenerlas y corregirlas; hacer frente a las consecuencias y analizar la posibilidad de aplicar acciones para eliminar sus causas desde la raíz.

La mejora continua funciona a todos los niveles dentro del ciclo PDCA, y requiere un proceso que identifique claramente los problemas y el entorno dentro del cual se producen; cada paso se debería crear y mejorar sobre el anterior, de manera que la mejora cubra más aspectos que los que su origen provocaron. (AENOR, 2015b, P.61).

3. CAPÍTULO III. SITUACIÓN ACTUAL DEL CENTRO OPERACIÓN DE TRANSMISIÓN

3.1 Antecedentes

El Centro de Operación de Transmisión se encuentra ubicado al norte de la ciudad de Quito, en una edificación construida hace 41 años, remodelada en el 2004 para albergar a las instalaciones del COT; en el 2015 la edificación se la volvió a adecuar, para acoger a toda la Subgerencia de Operación y Mantenimiento de CELEC EP TRANSELECTRIC y sus diferentes departamentos.

Para entender al Centro de Operación de Transmisión COT en su contexto, es necesario definir su situación actual, ubicándolo dentro de la Subgerencia de Operación y Mantenimiento (S.O.M.), posicionándolo dentro de la Unidad de Negocio TRANSELECTRIC y analizando su misión, así como sus objetivos estratégicos. Todo esto se lo menciona en el Informe de Planificación Operativa 2016 -2017, elaborado por (Subgerencia de Gestión Organizacional y el Departamento de Programación, Seguimiento y Calidad, 2015, p.16).

3.1.1 Misión de la Subgerencia de Operación y Mantenimiento

“Operar y mantener el Sistema Nacional de Transmisión, asegurando la disponibilidad y confiabilidad de los activos a fin de garantizar la continuidad del servicio de transmisión de electricidad, con altos niveles de calidad y seguridad, cuidando el ambiente y las relaciones comunitarias.”

Además de propender el mejoramiento de los procesos y del personal, para satisfacer los requisitos de sus clientes internos y externos.

3.1.2 Objetivos estratégicos

El objetivo estratégico de la Subgerencia de Operación y Mantenimiento, es incrementar la disponibilidad y confiabilidad del S.N.T. de la Unidad de Negocio CELEC EP – TRANSELECTRIC para lo que debe cumplir con los siguientes objetivos operativos:

1. Incrementar la disponibilidad de los activos del Sistema Nacional de Transmisión mediante la supervisión continua, la optimización y cumplimiento de los Planes de Mantenimiento, reposición y adquisición oportuna de equipos, sistemas tecnológicos, repuestos y herramientas necesarias para la operación y mantenimiento del S.N.T.

2. Reducir la frecuencia y el tiempo de interrupciones del servicio de transmisión, operando eficientemente el S.N.T., mediante el uso adecuado de tecnología de punta por parte del personal calificado, conforme a procesos establecidos.

3.1.3 Estructura de la Subgerencia de Operación y Mantenimiento

Para ejecutar sus objetivos la Subgerencia de Operación y Mantenimiento está conformada de la siguiente manera:

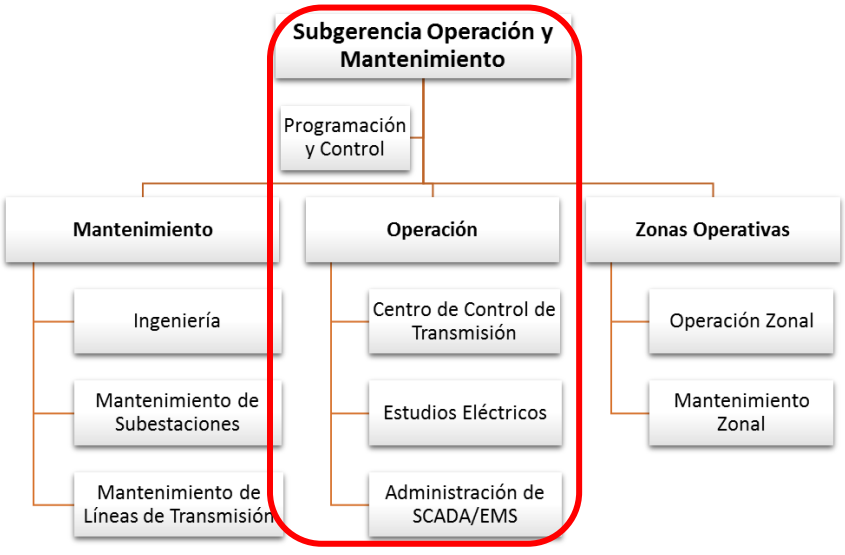


Figura 6 Estructura de la Subgerencia de Operación y Mantenimiento.
Tomado de Subgerencia de Operación y Mantenimiento. 2016, P.4.

El objetivo central del análisis de este trabajo se enfoca en el **Departamento de Operación,** en donde las actividades de sus tres secciones: el Centro de Control de Transmisión o **Centro de Operación de Transmisión**; la **Sección de Estudios Eléctricos** y la **Sección de Administración SCADA/EMS**, hacen posible el permanente monitoreo y control del Sistema Nacional de Transmisión.

3.1.4 Procesos del Departamento de Operación

Para la definición de los procesos es necesario precisar un entorno integral, la Corporación Eléctrica del Ecuador está trabajando para lograr un estándar y un contexto consolidado en lo concerniente al manejo de procesos. CELEC se encuentra formalizando sus procesos y su cadena de valor, los mismos que se muestran a continuación:

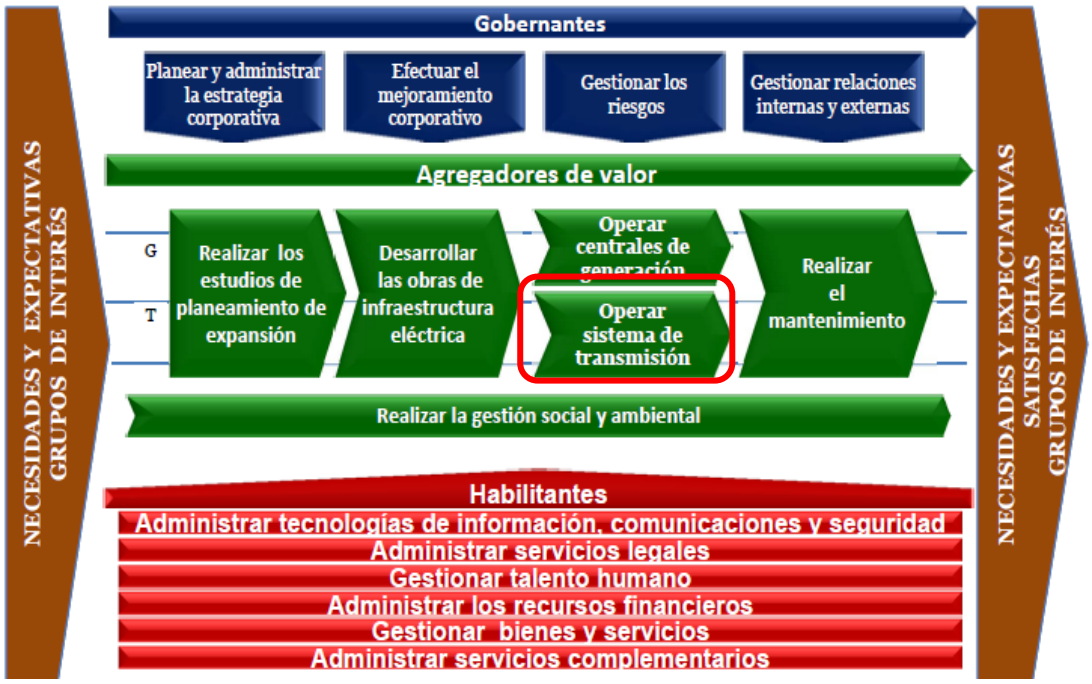


Figura 7 Cadena de Valor y Procesos CELEC EP.
Tomado de Subdirección de Procesos y Calidad, 2015, P.3.

Uno de los macro procesos agregadores de valor de CELEC EP se denomina **"Operar el Sistema de Transmisión**", y para definirlo se lo subdividió en tres procesos, que son:

1. Realizar análisis pre operativo,
2. Operar en tiempo Real el Sistema de Transmisión y
3. Evaluar la operación del sistema de Transmisión.

Los anteriores procesos se están estructurando e implantando en TRANSELECTRIC desde su Matriz CELEC, corresponde hacer un análisis en detalle del momento en el cual se están presentando las actividades del Centro de Operación de Transmisión, sus actuales procesos, procedimientos y actividades aún no formalizados, que también se encuentran en desarrollo.

El detalle del macro proceso Operar el Sistema de Transmisión se lo puede apreciar a continuación en la siguiente figura:

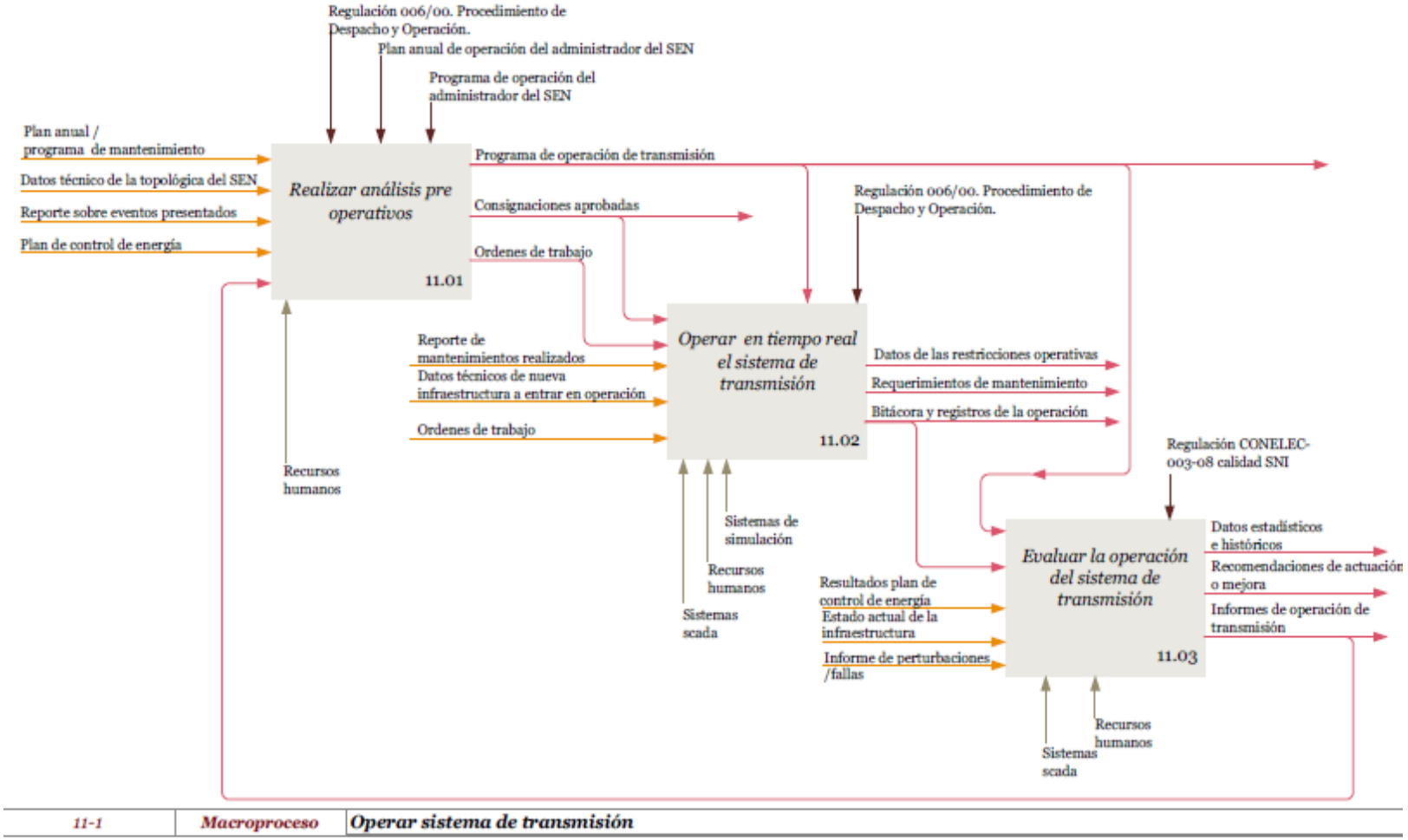


Figura 8 Caracterización de Macroproceso de Operación.

Tomado de CELEC. Anexo 11-1Caracterización Macroproceso. 2014.

3.2 Servicios brindados por el Departamento de Operación

A continuación, se presentan los servicios, procesos y actividades de cada una de las Secciones que conforman el Departamento de Operación que forman parte de este estudio.

3.2.1 Centro de Operación de Transmisión

3.2.1.1 Procesos y actividades del COT

El proceso principal del COT es Operar el Sistema Nacional de Transmisión, asegurando su disponibilidad y confiabilidad, garantizando la continuidad del servicio de transmisión de electricidad. Los procesos del COT se los pueden apreciar a continuación:

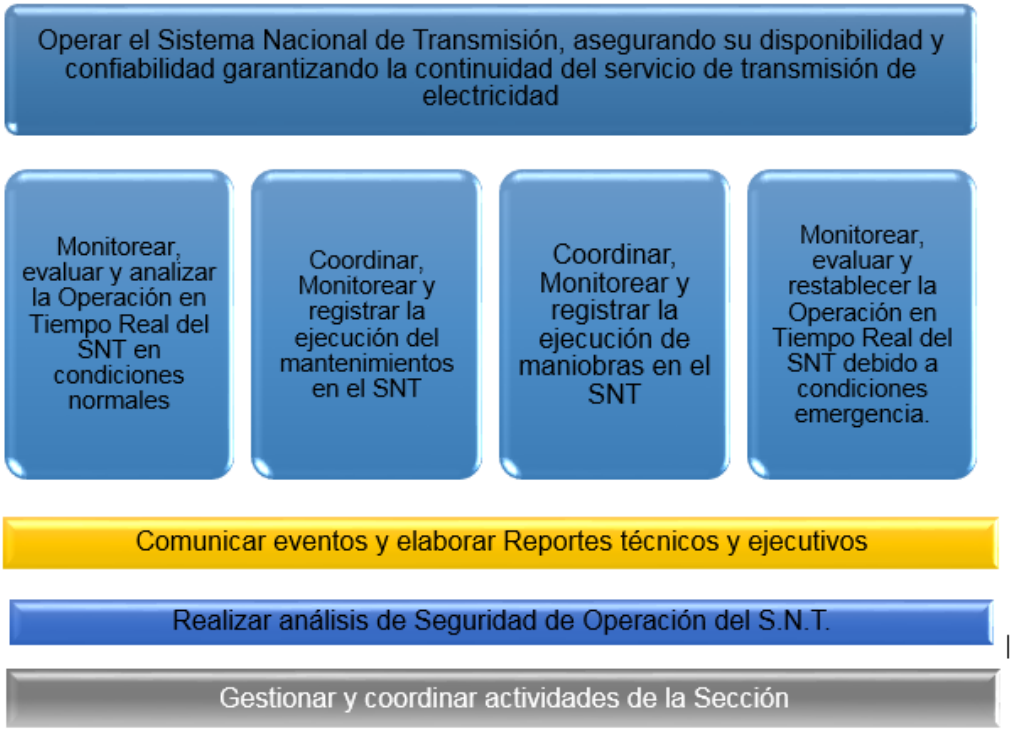


Figura 9 Diagrama de Procesos COT.
Tomado de Torres F., 2016, P.2.

Entre las principales actividades se pueden identificar las siguientes:

1. Supervisar y coordinar en tiempo real la operación del S.N.T. en condiciones normales.

2. Operar y restablecer el S.N.T. en condiciones de emergencia.
3. Realizar el Análisis de Seguridad de la red eléctrica ecuatoriana.
4. Supervisar y coordinar maniobras en el S.N.T.
5. Realizar estudios eléctricos pre-operativos para los mantenimientos con restricción de equipos del S.N.T.
6. Coordinar el mantenimiento y ejecución de órdenes de trabajo en el S.N.T.
7. Elaborar reportes de falla, post operativo diario, informes ejecutivos y en tiempo real sobre las novedades relevantes ocurridas en el S.N.T. (Adaptado de Torres, 2016, p.2)

3.2.1.2 Función Principal del Centro de Operación de Transmisión

El COT cumple su función principal, el transporte continuo de energía eléctrica al Ecuador desde los generadores hasta los distribuidores, haciendo uso principalmente de su sistema SCADA EMS, por sus siglas en inglés (Supervisory Control And Data Acquisition), herramienta que le permite automatizar el monitoreo de los flujos de energía eléctrica y ejecutar acciones de control y mantenimiento sobre los equipos de la red de potencia del Ecuador, el denominado Sistema Nacional de Transmisión.

A continuación se presenta dos figuras tomadas del Sistema SCADA, en la primera se puede apreciar el despliegue utilizado para la supervisión de los indicadores de generación y carga del SNT, en la segunda figura el despliegue que permite el control de los perfiles voltaje sobre el geográfico del Ecuador.

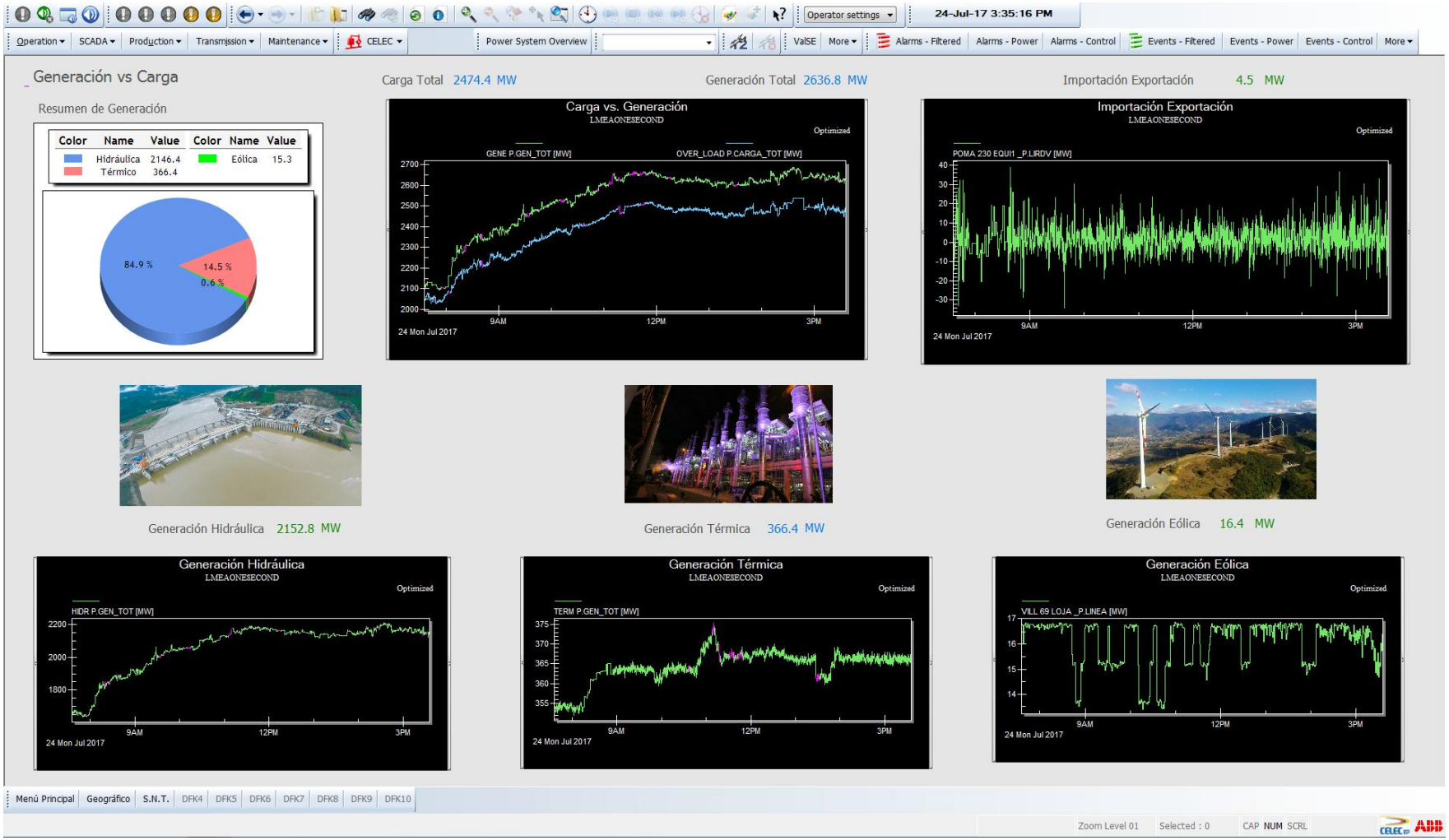


Figura 10 Despliegue Generación vs Carga Sistema SCADA EMS.

Tomado de Brito D., 2016, P. 24.

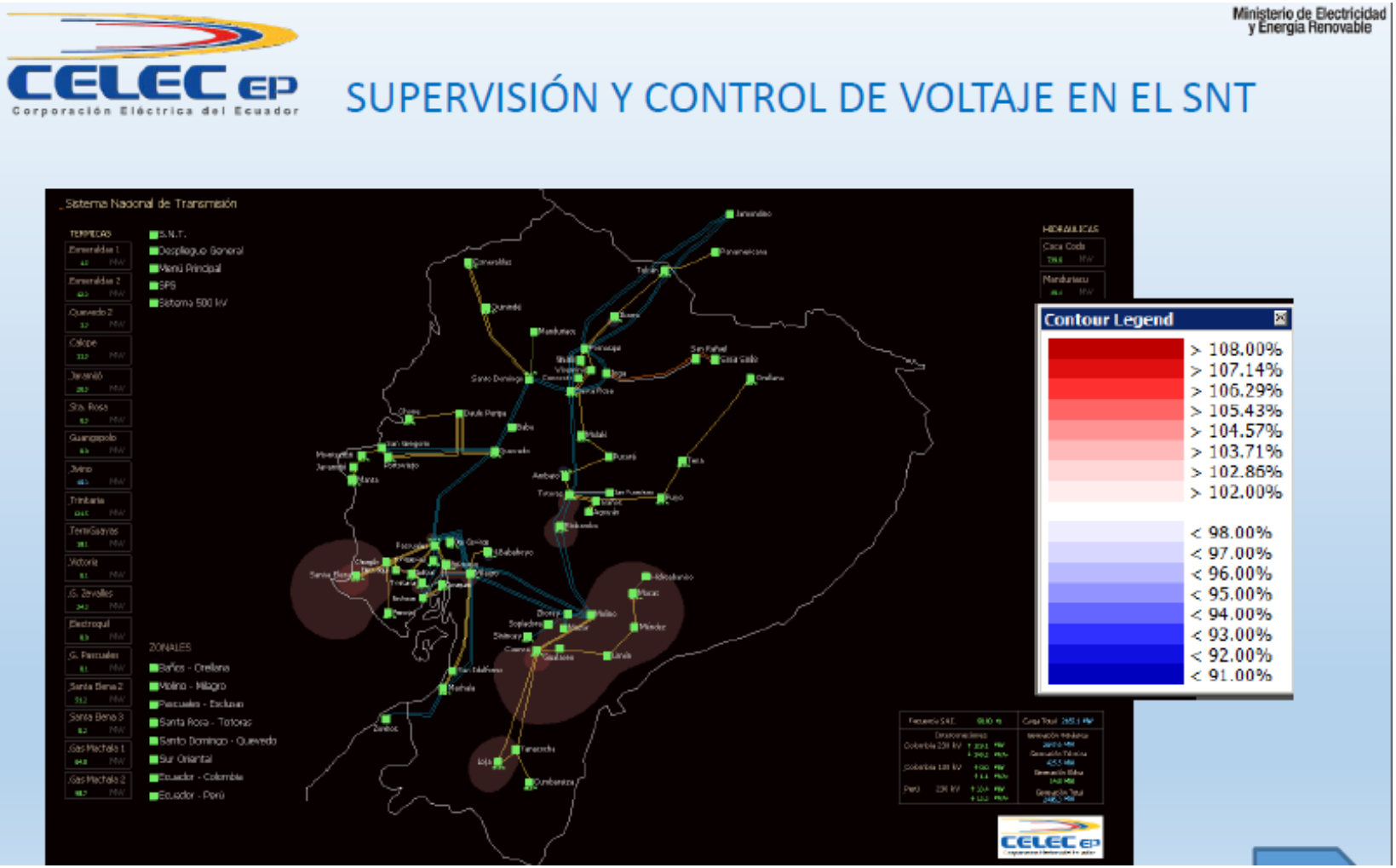


Figura 11 Despliegue de Supervisión y Control de Voltaje del S.N.T.

Tomado de Torres F., 2015, P. 11.

A continuación se presentan las características del Sistema Nacional de Transmisión, activos que son resguardados por el Centro de Operación de Transmisión:

- 17 Subestaciones a 230 / 138 / 69 kV.
- 30 Subestaciones a 138 / 69 kV.
- 3 Subestaciones móviles.
- Más de 2244.82 km de líneas de transmisión de 230 kV.
- Más de 1967.63 km de líneas de transmisión de 138 kV.
- Más de 3500 km de fibra óptica.
- 9130 MVA en capacidad de transformación. (Brito D., 2016, p. 38)

3.2.1.3 Estructura organizacional del COT

Actualmente el COT presenta una estructura plana, conformada por una jefatura y su grupo de operadores, la misma que se puede apreciar en el anexo 3.

3.2.2 Sección de Estudios Eléctricos

3.2.2.1 Procesos y actividades Sección Estudios Eléctricos

El principal proceso de esta Sección es analizar la Operación del S.N.T. mediante la realización de estudios especializados, calibrando y modelando la red eléctrica ecuatoriana, utilizando para estas labores sistemas específicos. A continuación, se presenta el detalle de los mismos. (Gerencia de Operación y Mantenimiento, 2016, P.15). Los procesos de esta sección se los pueden apreciar a continuación:

Figura 12 Estructura de Estudios Eléctricos.
Tomado de Gerencia de Operación y Mantenimiento, 2016, P.15.

Entre las principales actividades de esta Sección se puede identificar las siguientes:

1. Crear los Informes de calidad de Energía periódicos, con el objetivo de cumplir lo establecido en la Regulación CONELEC No. 003/08.
2. Realizar los informes estadísticos de la operación del S.N.T. sobre: cargabilidad en transformadores, líneas y bahías que se conectan a generadoras, distribuidoras o grandes clientes.
3. Tramitar el grupo de consignaciones al CENACE y empresas del Sector Eléctrico afectadas por los mantenimientos programados.
4. Realizar Estudios Eléctricos Especializados en estado estable y dinámico para el ingreso de nuevas instalaciones.
5. Realizar la evaluación de maniobras para restablecimiento de la red de transmisión, incluida la red de 500kV.

(Adaptado de Gerencia de Operación y Mantenimiento, 2016, P.12)

3.2.2.2 Estructura organizacional Sección de Estudios Eléctricos

En la actualidad esta Sección presenta una estructura plana, conformada por una jefatura y su grupo de operadores, la misma que se puede apreciar en el anexo 4.

3.2.3 Administración SCADA EMS

3.2.3.1 Procesos y actividades Administración SCADA EMS

El proceso fundamental de esta Sección es tener disponible el Sistema SCADA EMS y la adquisición de los datos, para de esta forma garantizar la operación y los mantenimientos del S.N.T. (Gerencia de Operación y Mantenimiento, 2016, P.25). Los procesos de esta sección se los pueden apreciar a continuación:

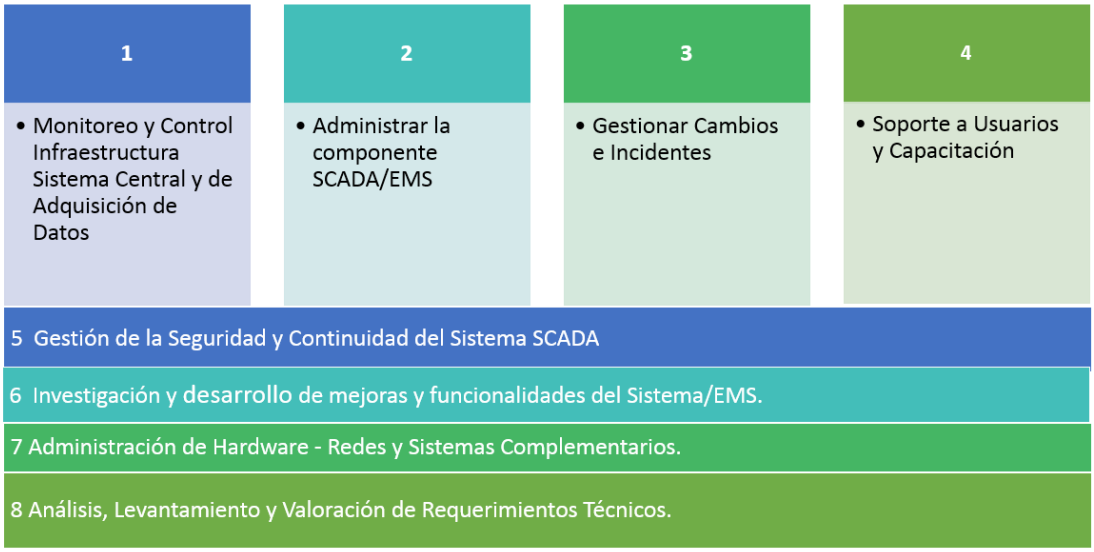


Figura 13 Diagrama de Procesos Administración SCADA EMS.
Tomado de Gerencia de Operación y Mantenimiento, 2016, P.25.

Entre las principales actividades de esta Sección se puede identificar las siguientes:

1. Gestionar y Coordinar la implementación de nuevas instalaciones del S.N.T. en el sistema SCADA EMS coordinadamente con CENACE, así como participar en la recepción y puesta en marcha de sistemas de automatización de subestaciones.
2. Actualizar los componentes del sistema SCADA (Bases de Datos, Enlaces de Comunicación, Despliegues de la interface, reportes históricos) para la operación en tiempo real del Centro de Control debido a la reconfiguración o adecuación del sistema de potencia y control.

3. Monitorear y Gestionar las aplicaciones en tiempo real y modo estudio: Estimador de estado, Despacho de flujo de potencia y Análisis de seguridad.
4. Monitorear y mantener la arquitectura del Sistema SCADA EMS (sistema central, Sistema de adquisición de datos) en sus componentes de hardware y software.
5. Administrar, Configurar y Monitorear equipos de Networking de la red de datos SCADA.
6. Analizar los incidentes y problemas del sistema SCADA/EMS, corregirlos y de ser el caso escalar la solución con el proveedor.
7. Administrar la seguridad informática en la red de datos del SCADA/EMS
8. Gestionar, Monitorear y Controlar los sistemas Complementarios del Centro de Control.

(Adaptado de Gerencia de Operación y Mantenimiento, 2016, P.24).

3.2.3.2 Estructura Administración SCADA EMS

La Sección Administración SCADA/EMS consta de las varias Áreas Funcionales, las mismas, las mismas que se puede apreciar en el anexo 4.

3.2.4 Sección de Programación y Control

El Área de Programación y Control apoya a toda la a Subgerencia de Operación y Mantenimiento. El esquema de procesos de esta sección se detalla continuación:

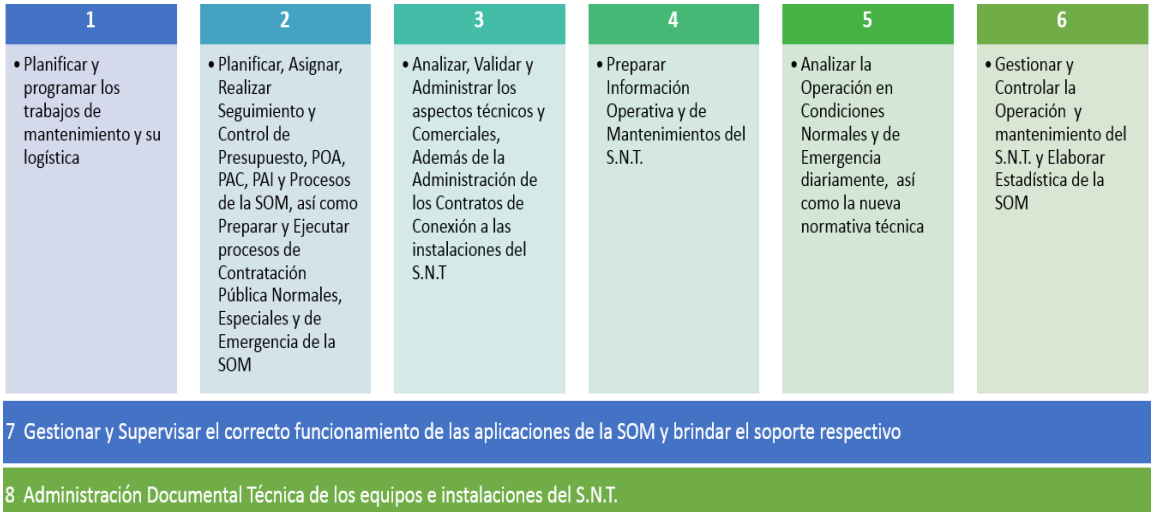


Figura 14 Diagrama de Procesos de Programación y Control.

Tomado de Gerencia de Operación y Mantenimiento, 2016, P.32.

3.2.4.1 Procesos de la Sección de Programación y Control

1. Planificar y programar los trabajos de mantenimiento y su logística.
2. Preparar y Ejecutar procesos de Contratación Pública Normales, Especiales y de Emergencia de la SOM.
3. Planificar, Asignar y Realizar Seguimiento y Control de Presupuesto, POA, PAC, PAI y Procesos de la SOM y revisar y analizar normas.
4. Analizar, Validar y Administrar los aspectos técnicos y Comerciales, Además de la Administración de los Contratos de Conexión a las instalaciones del S.N.T.
5. Preparar Información Operativa y de Mantenimientos del S.N.T.
6. Analizar la Operación en Condiciones Normales y de Emergencia, así como la nueva normativa técnica
7. Gestionar y Controlar la Operación y mantenimiento del S.N.T. y Elaborar Estadística de la SOM. (Adaptado de Gerencia de Operación y Mantenimiento, 2016, P.2-4).

Entre las principales actividades que realizan están:

3.2.4.2 Actividades de la Sección Programación y Control

1. Organizar los mantenimientos en los que participan las zonas operativas, el equipo de mantenimiento y trabajos de la Subgerencia de Proyectos de Expansión y Servicios del S.N.I.
2. Crear y Controlar el Plan Operativo Anual de la SOM.
3. Analizar, Definir y Controlar el Plan Anual de Contrataciones (PAC) de la SOM.
4. Definir y Controlar las inversiones para la Gestión Operativa (IGOS) de la SOM.
5. Elaborar Informes Semanales, Mensuales y Anuales de Gestión y Seguimiento del Comportamiento de la Operación y Ejecución de los Mantenimientos realizados por la SOM.
6. Ejecutar el cálculo de los indicadores de gestión de la Sugerencia de Operación y Mantenimiento para realizar el control de la gestión de la SOM.
7. Analizar y fijar metas para el control de la gestión de la Subgerencia de Operación y Mantenimiento.
8. Levantar la estadística operativa de la Subgerencia de Operación y Mantenimiento para análisis de tendencias y atender requerimientos de clientes internos y externos.
9. Apoyar en el levantamiento de los procedimientos operativos de la Subgerencia de Operación y Mantenimiento en torno a la norma ISO 9001 y realizar su respectivo seguimiento de implementación.
10. Realizar el control de la capacidad de los procesos que se ejecutan en la Subgerencia de Operación y Mantenimiento en las actividades de operar y mantener el S.N.T.

3.2.4.3 Estructura Organizacional de la Sección Programación y Control

El Área de Programación y Control consta de las siguientes Áreas Funcionales, las mismas que pueden ver en el anexo 6.

3.3 Arquitectura Tecnológica e Infraestructura

3.3.1 Arquitectura del Sistema SCADA EMS

A continuación se presenta un diagrama esquemático de la arquitectura del Sistema SCADA EMS en el cual se puede apreciar sus componentes, el núcleo del sistema constituido por los servidores de aplicaciones SCADA, la base de datos con la configuración del modelo de red eléctrica y los servidores que controlan la comunicación y la información entre el COT con las subestaciones y con otros Centros de Control, todos los datos son almacenados en servidores históricos, estos elementos son accesibles a los diferentes usuarios por medio de consolas locales, remotas o desde el Internet. El sistema se complementa con servidores de pruebas, entrenamiento y herramientas de visualización.

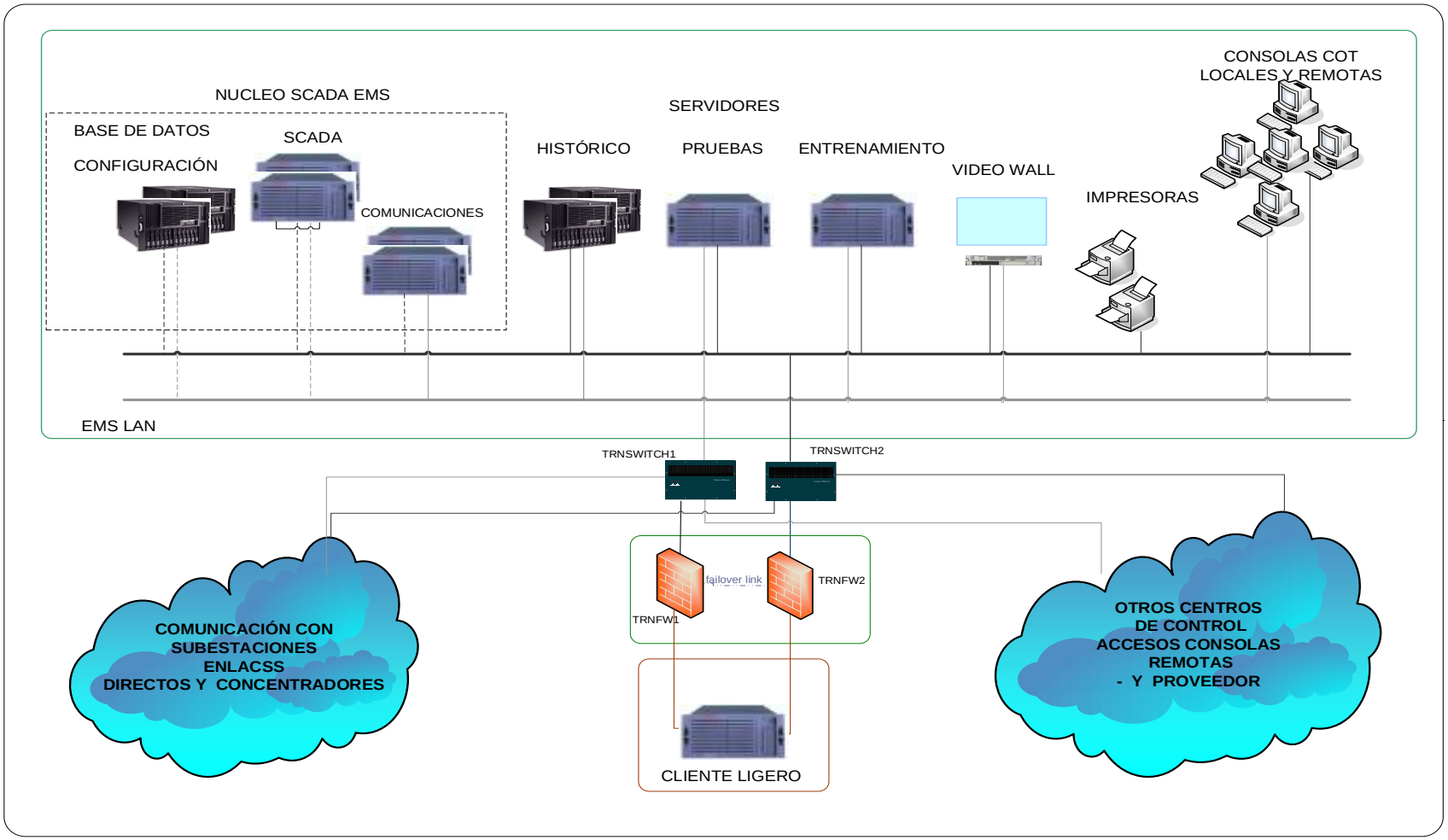


Figura 15 Esquemático de la arquitectura Sistema SCADA EMS

Adaptado de Brito D., 2016, P. 68.

3.3.2 Infraestructura

3.3.2.1 Sistemas Complementarios

Las actividades del COT se las puede ejecutar haciendo uso de una infraestructura base de alta disponibilidad que incluye: un Centro de Datos y Telecomunicaciones, una Sala de Operación y las oficinas de la Subgerencia de Operación y Mantenimiento, estas áreas están provistas de sistemas complementarios que habilitan su correcto funcionamiento, se dispone de:

- Sistema de alimentación de energía ininterrumpida.
- Sistema de climatización temperatura y humedad.
- Sistema de detección y extinción de incendios del Centro de Datos.
- Central telefónica IP.
- Sistema Integrado de alarmas.
- Sistema de Circuito Cerrado de Televisión CCTV.
- Sistema de Control de Accesos.
- Grupo electrógeno (Generador de emergencia).

Sobre esta infraestructura se asientan varios sistemas informáticos que permiten ejecutar las tareas diarias de las diferentes secciones.

3.3.2.2 Sistemas Especializados

A continuación se presenta un compendio de los sistemas tecnológicos que se utilizan en las actividades del Centro de Operación de CELEC EP TRANSELECTRIC, una descripción y el detalle de los sistemas, la sección que los utiliza, así como el área o los responsables de los mismos.

Tabla 9

Sistemas Informáticos del COT -1/3

Sistemas del Centro de Operación de Transmsión (1/3)						
#	Nombre	Descripción	Sección que utiliza			Área Responsable/ *Personal Responsable*
			COT	SCADA	Estudios	
1	**Sistema SCADA**	Sistema que permite realizar el Monitoreo y Control entre el COT y todas las subestaciones del Sistema Nacional, así como entre otros Centros de Control	Usu.	Adm.	Usu.	Administración SCADA EMS/ *Jefe de Sección*
2	**Aplicaciones EMS**	Software especializado que permite el modelamiento de la red eléctrica ecuatoriana, permitiendo el análisis del estado de la misma, previniendo las contingencias sobre el S.N.T. entre otras.	Usu.	Adm.	Usu.	
	Detalle del Sistema	Incluye arreglos de servidores de alta capacidad redundantes entre los que se tienen: - Servidores SCADA EMS. - Servidores de comunicaciones con las subestaciones. - Servidores de comunicación entre Centros de Control. - Servidores servicios Web. - Servidores de almacenamiento de datos histórico. - Servidores de generación de bases de datos de configuración. - Servidores de monitoreo de la red. - Consolas de operación local y remota. - Equipos de networking y seguridad. Se maneja en ambientes de Producción y Desarrollo.				
3	**Sistema de Telecomunicaciones**	Sistema de Telecomunicaciones sobre fibra óptica que permite la integración del Centro de Control con las Subestaciones y entre Centros de Control Regionales.	Usu.	Usu. Adm.	Usu.	- Gerencia de Servicios de S.N.I. - Administración SCADA EMS./ *Técnico de Telecomunicaciones*
4	**Líneas de comunicación directa**	Servicio de comunicación telefónica directa entre los Centros de Control de Transelectric y CENACE.	Usu.	Usu.	Usu.	
	Detalle del Sistema	Corresponden todos los enlaces de comunicación a través de fibra óptica que se establecen desde el Centro de Control con CENACE y con las subestaciones del S.N.T., manejando varios protocolos de comunicación e integrando sistemas antiguos y modernos. Enlaces de comunicación telefónica y de video conferencia directa con CENACE que logran comunicar permanente las dos Salas de Control, garantizando una coordinación operativa.				

Adaptado de Brito D., 2016, P. 62.

Tabla 10
Sistemas Informáticos del COT - 2/3

Sistemas del Centro de Operación de Transmsión (2/3)						
#	**Nombre**	**Descripción**	**Sección que utiliza**			**Área Responsable/**
			COT	**SCADA**	**Estudios**	***Personal Responsable***
5	**Sistema Integrado de Información**	Sistema Informático que integra las diferentes áreas funcionales de Transelectric incluyendo Financiera, Administrativa, Operación, Bodegas, Mantenimiento, etc.	Usu.	Usu.	Usu.	Tecnologías de Información / *Jefe de Tecnologías de Información.*
	Detalle del Sistema	Incluye arreglos de servidores de alta capacidad redundantes entre los que se tienen: - Servidores de Aplicación. - Servidores de Bases de Datos. - Servidores de Réplica. Se maneja en ambientes de Producción y Desarrollo.				
6	**Sistema de Protección Sistémica**	Sistema que permite la protección de los elementos eléctricos y previene una situación más seria al producirse una falla, ejecuta automáticamente la desconexión de carga antes de que se produzca un apagón regional o total.	Usu.	Usu.	Adm.	Sección de Estudios Eléctricos / *Jefe de Grupo de Ingeniería*
	Detalle del Sistema	Incluye arreglos de servidores de alta capacidad redundantes entre los que se tienen: - Servidores de Aplicación. - Servidores de Bases de Datos. - Sistemas de comunicaciones y protecciones automáticas. - Servidores de Réplica. Se maneja en ambientes de Producción, Desarrollo y Capacitación.				
7	**Sistema de Registro de Novedades Operativas**	Sistema que permite registrar los hechos ocurridos durante la operación del sistema. Permite notificar la novedades registradas a las autoridades.	Usu.	Usu.	Adm.	Sección de Estudios Eléctricos / *Jefe de Grupo de Ingeniería*
8	**Sistema de Registro y grabación de llamadas telefónicas**	Sistema que permite el registro de las llamadas entrantes y salientes, de las líneas directas y líneas IP, de la Sala de Operación, las mismas que sirven como respaldo a las instrucciones y órdenes que se generan o se acatan.	Usu.	Adm.	Usu.	Admininstración SCADA EMS / *Técnico de Redes y Comunicaciones*
9	**Sistema de Retroproyección**	Video Wall ubicado en la Sala de Operación, herramienta que es usada para la coordinación operativa y agilita las actividades de operación.	Usu.	Adm.	Usu.	Administración SCADA EMS / Técnicos de Hardware
10	**SIMEN**	Sistema de Medición Comercial	Usu.	x	x	CENACE
11	**SIMEC**	Sistema de Despacho de Generación	Usu.	x	x	CENACE

Adaptado de Brito D., 2016, P. 64.

Tabla 11
Sistemas Informáticos del COT - 3/3

Sistemas del Centro de Operación de Transmsión (3/3)						
#	Nombre	Descripción	Sección que utilizan			Área Responsable/ *Personal Responsable*
			COT	SCADA	Estudios	
12	**Correo Electrónico corporativo**	Programas para envío y recepción de correos	Usu.	Usu.	Usu.	Tecnologías de Información / Técnicos encargados de servidores
13	**Internet**	Sitio Web de CELEC EP Transelectric y acceso al Internet.	Usu.	Usu.	Usu.	- Gerencia de Servicios del S.N.I. - Tecnologías de Información / Técnicos encargados de servidores
14	**Herramienta de Respaldo corporativo**	Herramienta que permite el respaldo de los datos en los equipos y sistemas corporativos	Usu.	Usu.	Usu.	Tecnologías de Información / Técnicos encargados de servidores
15	**Herramientas de Respaldo de SCADA**	Herramienta que permite el respaldo de los datos en la red SCADA.	Usu.	Adm.	Usu.	Administración SCADA / Técnicos de Hardware
16	**Herramienta de Manejo de antivirus corporativo**	Herramienta que controla los equipos computacionales ante la presencia de virus informáticos	Usu.	Usu	Usu.	Tecnologías de Información / Tecnicos encargados de servidores
17	**Herramienta de Manejo de antivirus red SCADA**	Herramienta que controla los equipos computacionales ante la presencia de virus informáticos en la red SCADA	Usu.	Adm.	Usu.	Tecnologías de Información / Tecnicos de Hardware
18	**Herramienta de modelamiento eléctrico**	Herramienta que permite modelar la red eléctrica y hacer estudios especializados pre y pos operativos	Usu.	Usu.	Adm.	Sección de Estudios Eléctricos / Jefe de Grupo de Ingeniería

Adaptado de Brito D., 2016, P. 68.

3.4 Análisis de situación actual del COT respecto de las mejores prácticas en Continuidad de Negocio

Para llegar a la definición de la situación actual del COT respecto a las mejores prácticas se realizó la evaluación del nivel de capacidad de los procesos del Centro de Operación de Transmisión con relación a procesos de: EDM03 Asegurar la Optimización del Riesgo, APO12 Gestionar el Riesgo, DSS04 Gestionar la Continuidad.

Los objetivos del análisis fueron:

- Determinar sobre los procesos **EDM03**, **APO12**, **DSS04** los siguientes índices:

    - Rating de evaluación de metas del proceso,
    - Rating de evaluación de prácticas clave y
    - Rating de evaluación de productos
- Determinar el grado capacidad de estos procesos.
- Determinar y recomendar acciones sobre dichos procesos.

Para poder cumplir con los objetivos se empleó los siguientes procedimientos:

- Se realizó la ponderación a juicio de experto de la matriz Evaluación del nivel 1 de capacidad de procesos.
- Entrevistas con el personal encargado de los procesos para poder determinar el funcionamiento e integración.
- Verificación física de la documentación de los procesos involucrados.
- Verificación de metas, prácticas y productos de cada proceso a ser evaluados.

La documentación solicitada fue la siguiente:

- Planificación Estratégica de la Corporación.
- Norma y Política de Seguridad de la Información de la CELEC.
- Clasificación de Activos de Información de la Corporación.
- Procesos y procedimientos de las secciones evaluadas.
- Contexto de la organización.
- Requisitos legales, regulaciones y evidencias que se cumplen
- Campo de aplicación del SGCN y exclusiones.
- Política de Continuidad del negocio.
- Objetivos de Continuidad del negocio.

- Metodología para el Análisis de Riesgos de la Corporación y del análisis de impacto de negocio.
- Estrategia de Continuidad del negocio y sus opciones consideradas.
- Procedimientos de Continuidad, de gestión del incidente y de recuperación.
- Informes de pruebas.
- Auditorías internas.
- Las revisiones de la dirección.
- Las no conformidades y las acciones correctoras. (Adaptado de AENOR, 2015b, P.25)

Después del análisis de la ponderación de la matriz de evaluación de nivel 1 de capacidad de procesos se obtuvo el valor promedio del nivel de capacidad para los tres procesos analizados:

- EDM03 Asegurar la Optimización del Riesgo es de 22.78%
- APO12 Gestionar el Riesgo es de 21.81%
- DSS04 Gestionar la Continuidad es de 33.38%

Con lo que se determina que el nivel de capacidad de estos procesos tiene un logro promedio de 25.99%, lo que indica según la norma ISO /IEC 15504 que está entre (>15% y 50%) es decir **P "Parcialmente alcanzado"**, existe una cierta evidencia de los logros de la evaluación de dichos procesos. (Adaptado de Coronel, K. (s.f.). P.7).

El desarrollo de este análisis se lo puede apreciar en el anexo 8.

Como resultado del análisis sobre los tres procesos evaluados, **EDM03**, **APO12**, **DSS04** se encontraron algunas novedades, como son:

- El Departamento de Seguridad de la información de CELEC, cuenta con un procedimiento formal de gestión de riesgos, dentro de su Norma de Seguridad, el cual se encuentra en una fase inicial de implementación, se cumplió con la fase de difusión del proyecto, ya se realizó el levantamiento de los activos de información de todas las instalaciones críticas, se encuentra en la etapa de verificación de amenazas y vulnerabilidades, para el COT. (Adaptado de CELEC EP, 2015b. P.5).

  Se recomienda continuar con la implementación de la gestión de riesgos e identificar los activos críticos cuya afectación pueda influir en la continuidad del negocio del COT y definir acciones de mitigación sobre los mismos.

- Sobre el proceso de continuidad se han implementado varios mecanismos de control para manejar la disponibilidad especialmente de los sistemas e infraestructura del Centro de Operaciones con índices altos; no se tienen procedimientos formales para el tratamiento de continuidad, no se cuenta con la documentación sobre continuidad formalizada, se espera contar con proyectos adicionales para cumplir este objetivo, por condiciones de emergencia sobre el volcán Cotopaxi se habilitó en la provincia del Guayas un sistema SCADA que brindaría un respaldo en caso de ser necesario.

  Se recomienda implementar un Sistema de Gestión de Continuidad que permita viabilizar de una manera adecuada las estrategias de continuidad, el diseño de la implementación de este sistema es el objetivo de este trabajo de titulación.

4. CAPÍTULO IV. DISEÑO DEL SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO PARA COT

Con la finalidad de realizar el diseño para implementación del Sistema de continuidad para el COT, se coordinaron y realizaron talleres con los dueños y el personal del macroproceso de la Operación del S.N.T. analizando procesos y subprocesos habilitadores.

4.1 Objetivos del SGCN para el Centro de Operación de Transmisión

- Mantener la Operación del COT a niveles de servicio aceptados y requeridos por sus clientes externos e internos.
- Atender a las exigencias legales y reglamentarias.
- Proteger los activos de información del COT
- Garantizar la integridad, disponibilidad, confidencialidad de la información que se maneje durante la operación del S.N.T. en caso de una emergencia.
- Minimizar el impacto causado por los eventos disruptivos.
- Definir una Política de Continuidad de Negocio para el COT.

4.2 Identificar los Requerimientos del Proyecto

Para cumplir con la primera fase que permite la identificación de los requerimientos, establecida dentro de la metodología propuesta para la implementación del SGCN, se realizó la definición del contexto.

4.2.1 Contexto de la organización

Para la definición del contexto se consideró a CELEC EP TRANSELECTRIC en su entorno empresarial con un enfoque dirigido al Centro de Operación de Transmisión y sus principales funciones y responsabilidades, del análisis se establecieron clientes externos e internos en sus diferentes entornos.

4.2.1.1 Clientes Externos (Entorno)

Político

- El ***Ministerio de Electricidad y Energía Renovable***, encargado de regir el sector eléctrico ecuatoriano, pendiente de la transmisión de energía y la incorporación de los nuevos proyectos eléctricos, es el organismo encargado de ejecutar las directrices y objetivos nacionales. *(Adaptado de Brito D., 2016, P. 13).*

Legal

- La **Agencia de Regulación y Control de la Electricidad, ARCONEL**, constituye el ente regulador del Sector estratégico de la electricidad. Entrega las directrices para el Transmisor de energía al cual se debe reportar. (Adaptado de Brito D., 2016, P. 14).
- El ***Operador Nacional de Electricidad, CENACE***, órgano técnico que actúa como operador técnico del Sistema Nacional Interconectado, SNI y administrador comercial de las transacciones de bloques energéticos, responsable del abastecimiento continuo de energía eléctrica al mínimo costo posible. (CENACE, 2014), trabaja estrechamente con el COT, para realizar las actividades diarias.

Reglamentario

- Regulación ***No. CONELEC – 003/08***, ***CALIDAD DEL TRANSPORTE DE ELECTRICIDAD Y DEL SERVICIO DE TRANSMISIÓN Y CONEXÓN EN EL S.N.I.*** obliga a TRANSELECTRIC a operar sus equipos y define los índices de calidad de servicio que éste debe prestar.

- Regulación ***No. ARCONEL – 003/16, REQUERIMIENTOS PARA LA SUPERVISIÓN Y CONTROL EN TIEMPO REAL DEL S.N.I.*** define la obligatoriedad de la entrega de la información por parte del Transmisor de energía al CENACE, adicionalmente menciona que el Centro de Control de TRANSELECTRIC, podría ser un respaldo del Centro de Control de CENACE.

- ***Plan de Operación,*** Presenta las restricciones que se dan en el S.N.T. y de igual manera marca los cronogramas para la incorporación de nuevos proyectos e instalaciones.

Internacional:

- ***Interconexiones con Colombia y Perú***, el comercio de energía a nivel regional se da a través de las instalaciones de TRANSELECTRIC cuyo grado de disponibilidad cuando se requiera debe ser el mayor.
- ***Proveedores de los Sistemas,*** La participación de los proveedores tiene un rol fundamental en el desempeño de las actividades del COT en especial cuando existen contratos de mantenimiento los cuales pueden ser preventivos y/o correctivos.

Nacional:

- El principal cliente externo de las actividades que desarrolla el COT, es la ***comunidad*** desde el ***entorno social***, ya que una demora en la reposición de una falla en el servicio, implica dejar de entregar energía a vastos territorios en el país, lo que conlleva problemas en todos los sectores como: el productivo, empresarial, hospitalario, público en general, etc., adicionalmente genera a CELEC EP TRANSELECTRIC multas y sanciones por incumplimiento de regulaciones.

4.2.1.2 Clientes Internos

Para completar el contexto de la organización fue necesario determinar los clientes internos:

Departamentos y Secciones

- ***CELEC EP***, la finalidad de la Corporación es la provisión de servicio eléctrico y éste debe responder a los principios de obligatoriedad, generalidad, uniformidad, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad, TRANSELECTRIC se sujeta a los lineamientos definidos por su Matriz. (Adaptado de CELEC EP. 2015).

- ***Departamento de Seguridad Informática de CELEC***, es el encargado de la gestión de la seguridad para la Corporación, esta entidad vela por el cumplimiento de los procesos y la Política de Seguridad integrada con la continuidad del negocio.

- ***Sección de Mantenimiento***, incluyen: Equipo Primario, Líneas de Transmisión, Protección – Control y Medición, áreas que realizan un trabajo en conjunto con el COT, detectando la falla y realizando mantenimientos especializados, garantizando de esta manera la máxima disponibilidad. Existen los Planes de Mantenimiento anual, mensual y semanal que influyen en las actividades operativas del COT. (Subgerencia de Operación y Mantenimiento. 2016, P.4)

- ***Subgerencia de Expansión***, encargada de implementar los nuevos proyectos, ligada muy estrechamente con operación ya que las nuevas instalaciones no deben causar problema alguno al incorporarse en el S.N.T., esto se encuentra documentado en el Plan de Expansión.

- ***Subgerencia Servicio del S.N.I. (Telecomunicaciones)***, encargada de dar soporte y mantener las comunicaciones entre el COT, las subestaciones y otros Centros de Control del Sector.

- ***Zonas Operativas,*** responsables de los mantenimientos preventivos y/o correctivos de las Zonas, coordinan directamente las maniobras con el COT. (Adaptado de Subgerencia de Operación y Mantenimiento. 2016, P.38)

- ***Subgerencia Administrativa Financiera***, encargada del manejo de los recursos económicos para cualquier actividad operativa, así como de coordinar el talento humano responsable de realizar las actividades tanto operativas como de continuidad.

Políticas internas

- ***La Política de Seguridad de la Corporación,*** aprobada y puesta en vigencia desde el 2015, define y controla la continuidad de todas las Unidades de Negocio, gestiona con cada una de ellas la implementación y control para los procesos de Continuidad y Seguridad. (Adaptado de CELEC EP. 2015c. p.7)

- ***Objetivos Estratégicos***

  - ✓ Incrementar la disponibilidad de los activos del Sistema Nacional de Transmisión mediante la supervisión continua, la optimización y cumplimiento de los Planes de Mantenimiento, reposición y adquisición oportuna de equipos, sistemas tecnológicos, repuestos y herramientas necesarias para la operación y mantenimiento del S.N.T.

  - ✓ Reducir la frecuencia y el tiempo de interrupciones del servicio de transmisión, operando eficientemente el S.N.T., mediante el uso adecuado de tecnología de punta por parte del personal calificado, conforme a procesos establecidos. (Subgerencia de Operación y Mantenimiento. 2016, P.3)

Oportunidades futuras

- ***Operación del sistema de extra alta tensión 500 kV****,* a partir del 2020 CELEC EP TRANSELECTRIC operará y mantendrá el sistema de 500 kV que en la actualidad se encuentra en manos extranjeras. (Adaptado de Brito D., 2016, P. 33).

- ***Sistemas de información****,* la incorporación de nuevas herramientas y tecnologías que permitan la adecuada supervisión, operación y mantenimiento del S.N.T. los sistemas entre los que se puede nombrar son: SCADA EMS, Sistema de Análisis de Perturbación de Fallas, Sistema de Registros de Eventos, Protección Sistémica y Sincrofasores, que integrados con las soluciones de tecnología como: el Sistema Integrado de Información, Herramienta de Gestión Documental de Gobierno, Internet, correo electrónico y ofimática permiten cumplir con los objetivos operativos del COT.

La información anteriormente señalada se la obtuvo de los (Talleres definición de Clientes Internos y Externos, 2017) y su formato se lo puede analizar en el Anexo 9.

4.3 Definir el alcance del Proyecto

4.3.1 Campo de aplicación del SGCN

El Sistema de Gestión de Continuidad del Negocio para el Centro de Operación de Transmisión, se enfocará a su macro proceso: Operar el Sistema Nacional de Transmisión, con análisis de los subprocesos involucrados directamente con las áreas del COT, Administración SCADA, Estudios Eléctricos y Programación y Control con sus actividades fundamentales que agregan valor.

El análisis es para el Centro de Operación de Transmisión COT ubicado al norte de la ciudad de Quito en Ecuador.

4.3.2 Exclusiones

Se excluyen las demás áreas de CELEC EP TRANSELECTRIC, se asume que los otros departamentos tecnológicos de la Unidad de Negocio, habilitadores para el COT, tendrán las herramientas disponibles a través de soluciones de contingencia propias, de esta manera se apoyará la continuidad de la Operación del COT, con estos departamentos se firmarán acuerdos de nivel operacional, para garantizar su servicio.

4.4 Validar la intención de la dirección

4.4.1 Política de Continuidad de Negocio

La CELEC ha desarrollado y aprobado su Política de Seguridad de Información que rige para todas sus Unidades de Negocio, ésta se encuentra en proceso de implementación. La mencionada política define entre otras: referencias a las normas utilizadas y escalas de incidentes, proporciona la dirección sobre los campos de aplicación; en su introducción presenta el siguiente texto sobre la *continuidad de negocio*.

“Para asegurar la continuidad operativa de los sistemas de información y cumplir con los objetivos de negocio, es necesario llevar a cabo una gestión de riesgos que permita preservar la confidencialidad, integridad y disponibilidad de la información ante nuestros clientes y ante las distintas partes interesadas”. (CELEC, 2015c, P.2)

En el apartado específico sobre la **Política de Gestión de la Continuidad de Negocio** indica:

a) “Los Responsables de las Áreas de los Sistemas de Apoyo y del Núcleo del Negocio con el apoyo del Equipo de Seguridad de Información deben elaborar, documentar, implementar y mantener actualizados los procedimientos operativos para garantizar la continuidad de operaciones al nivel requerido en caso que ocurra una contingencia.

b) Cada área involucrada debe designar al personal de respuesta a incidentes que cuente con la responsabilidad, autoridad, experiencia y competencia necesarias para actuar ante una contingencia.

c) Los planes de continuidad de operaciones deben ser probados periódicamente de acuerdo a la criticidad del sistema de información.

d) La coordinación en producción y pruebas de los planes de continuidad de negocio y contingencia será responsabilidad del Oficial de Seguridad de Información Corporativa, mientras que la elaboración estará a cargo del responsable del proceso al que el plan cubre.” (CELEC, 2015c, P.10).

4.5 Establecer las responsabilidades de los participantes

A continuación, se presenta la definición de los responsables designados en Centro de Control, sus las competencias y las tareas que debe cumplir dentro del Sistema de Gestión de Continuidad, así como los respectivos coordinadores de cada equipo.

4.5.1 Responsables y Tareas del SGCN

- ✓ **Líder del SGCN**
  - Gerente de la Unidad de Negocio TRANSELECTRIC.

Gestor de la implementación del SGNC dentro de su ámbito de mandato, promoviendo su realización, delegando responsables, evaluando y aprobando reportes de la efectividad en la ejecución.

- ✓ **Comité del SGCN**

Conformado por los siguientes miembros:

- Subgerente de Operación y Mantenimiento.
- Subgerente Administrativo – Financiero.
- Oficial de Seguridad de la Corporación.
- Subgerente de Gestión Organizacional (TIC).
- Subgerente de Servicios del SNI (Telecomunicaciones)
- Supervisor de Operación.

Coordinado por: Subgerente de Operación y Mantenimiento.

Equipo de responsables con las siguientes tareas:

a) Definir y aprobar las guías, instructivos, procesos y estrategias de continuidad, así como los recursos para garantizar su implementación.

b) Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información frente a incidentes de seguridad imprevistos y eventos programados. (ej. simulacros).
c) Dar seguimiento a los cambios que pueden comprometer a los activos de información, frente a riesgos o amenazas, que pueden afectarlos.
d) Evaluar y coordinar la implementación de controles específicos de continuidad del negocio para sistemas o servicios.

El Coordinador de este comité cumplirá las siguientes actividades esenciales:

a) Emitir la Declaratoria de Falla Masiva de Centro de Operación de TRANSELECTRIC.
b) Solicitar la recuperación del COT
c) Difundir la Declaratoria de Restablecimiento de Operación Normal del COT.

- ✓ **Equipo de Evaluación de Incidentes**
    - Jefe del COT.
    - Operador del COT Tercera consola.
    - Jefe de SCADA EMS.
    - Técnico de SCADA.
    - Técnico de Hardware y Software.
    - Técnico de Redes y Seguridad.
    - Oficial de Seguridad de la Corporación.
    - Técnico de Telecomunicaciones.

Coordinado por: Oficial de Seguridad de la Corporación.

Las tareas de este equipo son:

a) Al ocurrirse un evento disruptivo este equipo deberá analizar y evaluar el incidente y el grado de impacto que tiene sobre la capacidad que disponga el Centro de Control para seguir prestando sus servicios.
b) Registrará el evento y autorizará la emisión de Falla Total del COT.

c) Al recibir el reporte notificando de que las condiciones son óptimas para reiniciar las labores, se registrará la petición, posteriormente se coordinará y finalmente se notificará la reanudación de las operaciones.

- ✓ **Equipo de Recuperación de Negocio**
    - Jefe del COT.
    - Operador del COT.
    - Operador del COT de Contingencia en otra provincia
    - Jefe de SCADA EMS.
    - Técnico SCADA.

Coordinado por: Jefe de COT.

Responsables con las siguientes acciones:

a) Viabilizar la continuidad del negocio siguiendo los planes establecidos para las diferentes estrategias.
b) Responsabilizarse de la continuidad de la operación mientras dure el proceso de contingencia.
c) Cuando el sistema esté restablecido entregar el control de las operaciones al Centro principal.

- ✓ **Equipo de Recuperación de Tecnología**
    - Técnico SCADA
    - Técnico Aplicaciones EMS.
    - Técnico de Hardware y Software.
    - Técnico de Redes y Seguridad.
    - Técnico de Tecnologías de Información.
    - Técnico de Telecomunicaciones.

Coordinado por: Técnico SCADA

Las actividades de este grupo son las siguientes:

a) Definir y ejecutar los planes y procedimientos de continuidad con la finalidad de recuperar el servicio de los sistemas en caso de falla.

b) Restablecer el nivel de servicio aceptado en las estrategias de continuidad.
c) Coordinar con los proveedores de los sistemas externos e internos para ejecutar recuperaciones de los equipos o sistemas necesarios tanto del sistema de contingencia como del principal.
d) Evaluar y reportar los niveles de servicio disponible de la solución de contingencia, así como los avances en la solución del sistema comprometido.
e) Verificar y probar que las soluciones implementadas permiten restablecer el normal funcionamiento del equipo principal, reportar el avance del trabajo y en el caso de finalizar con éxito, solicitar la reanudación de operaciones normales.

- ✓ **Equipo de Recuperación de Finanzas y Logística**
    - Delegado del Departamento Administrativo Financiero.
    - Encargado de Bodegas y suministros.

Coordinado por: Delegado del Departamento Administrativo Financiero.

Equipo responsable de disponer la logística, el transporte, así como del componente financiero oportuno para cumplir con los requerimientos de continuidad, de igual manera facilitar el incremento de personal o cambio de funciones en la estructura organizacional para responder a estas nuevas exigencias.

- ✓ **Equipo de comunicación**
    - Delegado de Comunicación corporativa.

Encargado de ejecutar el Plan de Comunicación de Contingencia, convirtiéndolo en el único vocero oficial durante el incidente disruptivo hasta su recuperación total, de las actividades del COT y de sus encargados ante los clientes internos y externos lo que evitará cualquier tipo de mala interpretación y falsas expectativas.

4.6 Identificar los riesgos de incidentes Disruptivos

4.6.1 Análisis de Riesgos

El análisis de riesgos se lo realizó basándose en la metodología interna de la Corporación CELEC, establecida para este propósito, la cual se basa en las normas ISO 31000, que fueron documentadas en este marco teórico. La incorporación de esta metodología permite identificar, evaluar y gestionar los riesgos según sus lineamientos y consideraciones.

Dado que la información que se maneja es confidencial solo se presentarán los resultados en compendio del trabajo realizado, en varias sesiones de trabajo y talleres para estos objetivos, se darán ejemplos de los procedimientos para la obtención de los mismos.

4.6.2 Identificación de los activos

Como primera fase se realizó la identificación de los tipos de activos de información para el Centro de Operación de TRANSELECTRIC, considerando los siguientes tipos:

Nota: **Activo de Información** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (CELEC EP, 2015a, P.9)

- **Servicios.**
  - Procesos de negocio que se ofrece al interno del COT o se entregan a la ciudadanía. (Servicios que proporcionan los diferentes sistemas que aportan a la operación).

- **Datos e información.**
  - Bases de Datos (Base de configuración del modelo eléctrico, Base de datos en Tiempo Real, Base de Datos Histórica, etc.), archivos de configuración (de servidores de los sistemas, de networking, etc.), documentación, manuales de usuario, contratos, licencias de sistemas, registro de pruebas e información de las subestaciones, entre otros.

Aplicaciones de Software.

- Software de aplicación involucrados en la Operación (Sistema SCADA, Aplicaciones EMS, Sistema de Análisis de Perturbaciones, Protección Sistémica, Sistema Integrados de Información, etc.), sistemas operativos, aplicativos desarrollados (Sistemas de manejo de eventos, reporte Post operativo, Reporte SOE, etc.),correo electrónico, Internet.

Equipos informáticos.

- Servidores (desde el contexto de hardware todos los sistemas que habilitan la Operación), Computadores Personales (entre otras consolas de los sistemas locales, remotas y de repuesto), portátiles (equipos de trabajo del personal y equipos que permiten el acceso a los sistemas a través de cliente ligeros), dispositivos móviles, etc.

Redes de Comunicación.

- Aquellas que dan soporte a la Corporación para el movimiento y flujo de información. (equipos como: firewalls, routers, switches y sistemas de comunicación de fibra óptica, etc.)

Soporte de la información.

- Medios físicos que permiten el almacenamiento de la información por un largo intervalo de tiempo. (incluyendo discos duros, sistemas para el manejo de respaldo y cintas, etc.)

Equipamiento auxiliar.

- Soporte a los sistemas de información relacionados, como equipos de climatización especializado, Servicio de energía ininterrumpida, Sistema de Detección y extinción de incendios, Circuito Cerrado de Televisión, Central de telecomunicaciones, entre otros.

Instalaciones.

- Lugar donde se alojan los sistemas de información (Centro de Datos principal y alterno).

Personal.

- Personal interno (administradores de los diferentes sistemas y personal necesario para la Operación del COT), subcontratado, proveedores, etc.

Intangible.

- Tales como reputación e imagen de la organización.

(Adaptado de CELEC EP, 2015a, P.5-7)

A continuación se muestra en resumen los diferentes tipos de activos del COT:

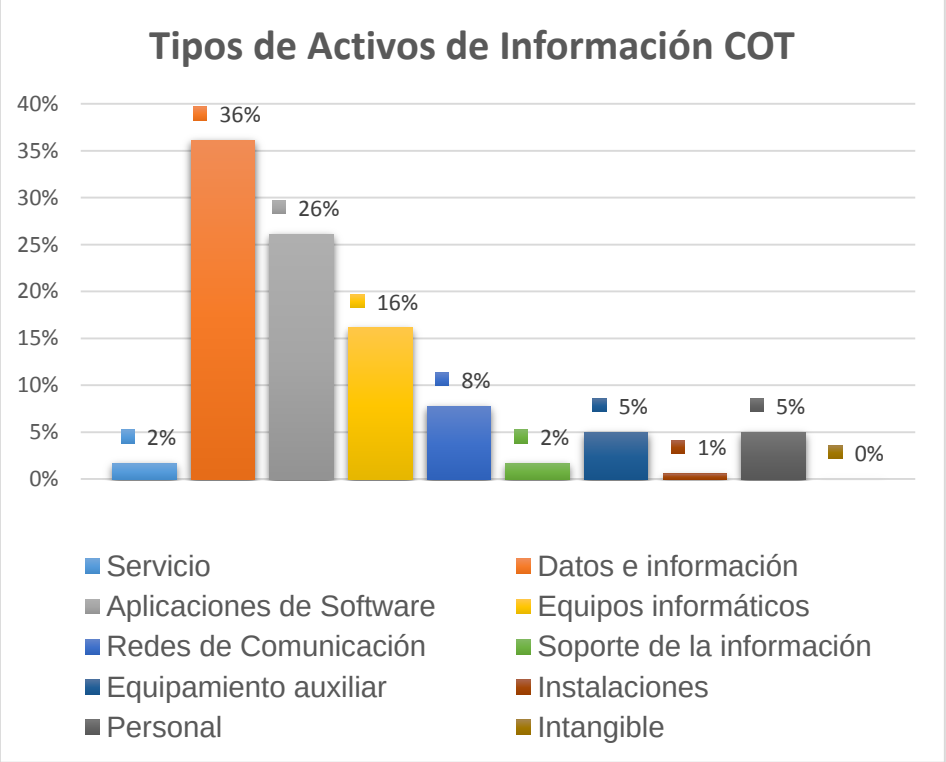


Figura 16 Tipos de Activos de Información del COT

Tomado de Talleres de Gestión de Riesgos COT, 2017.

Luego de realizar la tipificación de los activos de información se realizó una valorización en función de la afectación de la **confidencialidad, integridad y disponibilidad de la información,** esto permite profundizar el conocimiento e importancia del COT, obteniendo el valor total de los activos de información, la **clasificación** e **importancia** de los mismos.

Con respecto a la confidencialidad los criterios sobre los activos de información y sus resultados fueron los siguientes:

Tabla 12
Criterios valoración de confidencialidad de activos del COT.

Valoración	**Descripción:** El conocimiento o divulgación no autorizada de la información que maneja el activo:
Muy Alto	Tiene consecuencias a nivel Operativo de la Corporación.
Alto	Tiene consecuencias a graves para la Corporación.
Medio	Tiene consecuencias a moderadas para la Corporación.
Bajo	No tendrá consecuencias negativas para la corporación.

Adaptado de CELEC, 2016b, P. 9.

Los resultados obtenidos para la clasificación de la confidencialidad de los activos de información del COT son los siguientes:

Figura 17 Clasificación de Confidencialidad Activos Información COT.
Tomado de Talleres de Gestión de Riesgos COT, 2017.

Con respecto a la integridad los criterios sobre los activos de información y sus resultados fueron los siguientes:

Tabla 13
Criterios valoración de integridad de activos del COT

Valoración	**Descripción:** El daño o modificación de información que maneja el activo:
Muy Alto	Tiene consecuencias a nivel Operativo de la Corporación.
Alto	Tiene consecuencias a severas para la Corporación.
Medio	Tiene consecuencias a moderadas para la Corporación.
Bajo	No tendrá consecuencias negativas para la corporación.

Adaptado de CELEC, 2016b, P. 9.

Los resultados obtenidos para la clasificación de la integridad de los activos de información del COT son los siguientes:

Figura 18 Clasificación de Integridad Activos de Información COT.
Tomado de Talleres de Gestión de Riesgos COT, 2017.

Con respecto a la disponibilidad los criterios sobre los activos de información y sus resultados fueron los siguientes:

Tabla 14
Criterios valoración de disponibilidad de activos del COT.

Valoración	Descripción:
Muy Alto	El activo de Información debe estar siempre disponible para evitar consecuencias a nivel Operativo de la Corporación.
Alto	El activo de información puede no estar disponible, máximo 1 hora, para evitar consecuencias negativas para la Corporación.
Medio	El activo de información puede no estar disponible un máximo 8 horas, sin presentar o causar consecuencias negativas para la Corporación.
Bajo	El activo de información puede no estar disponible, por 8 horas o más, sin presentar o causar consecuencias negativas para la Corporación.

Adaptado de CELEC, 2016b, P. 9.

Los resultados obtenidos para la disponibilidad de los activos de información del COT son los siguientes:

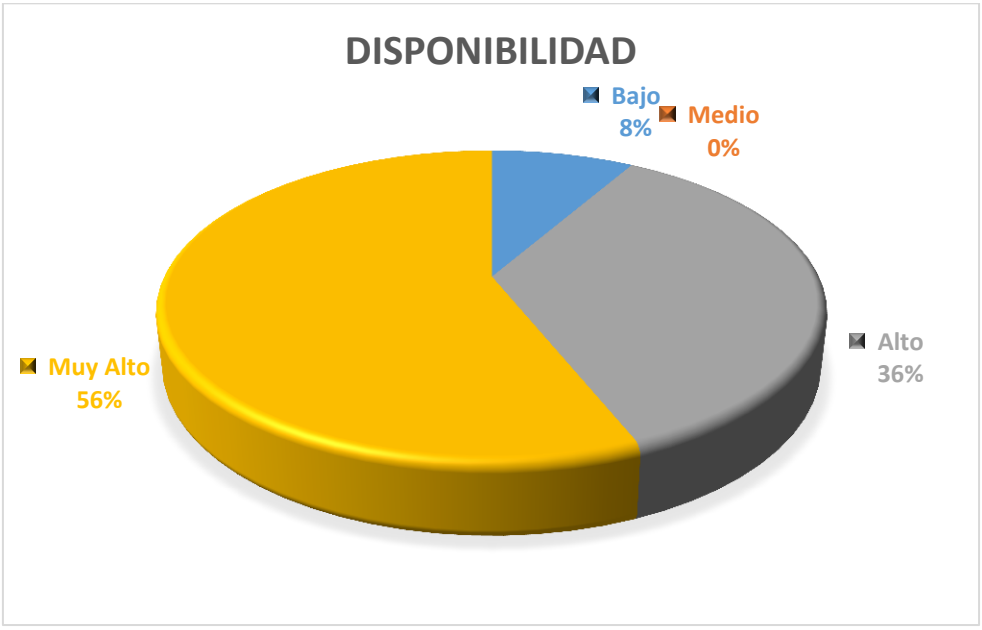


Figura 19 Clasificación de Disponibilidad Activos de Información del COT. Tomado de Talleres de Gestión de Riesgos COT, 2017.

A continuación se presenta el **valor total de los activos de información** que corresponde al valor promedio entre los tres criterios analizados de confidencialidad, integridad y disponibilidad, los valores muy alto corresponden a los **activos de infraestructura crítica**, que afectan directamente la Operatividad del Centro de Control de Transmisión, los valores altos denotan los activos de información que **habilitan el adecuado desempeño y operación** de los activos críticos. (Adaptado de CELEC, 2016b, P. 9).

A continuación se presente el resultado de la valoración total de los activos de información del COT.

Figura 20 Valor Total de los Activos de Información del COT.
Tomado de Talleres de Gestión de Riesgos COT, 2017.

En base a la ponderación sobre los activos de información y con un análisis en detalle sobre criterios anteriormente señalados se clasificó la información del COT, de acuerdo a los siguientes criterios:

Tabla 15
Criterios de clasificación de la información del COT.

Clasificación	Descripción
Confidencial	Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidades de negocio, potencial fraude o requisitos legales. Información a la que debe tener acceso sólo personal autorizado.
Restringida	Información privilegiada en donde su divulgación no está autorizada, puede derivar en impactos financieros y legales.
Uso Interno	Activo de Información sensible, interno a áreas o proyectos a los que debe tener acceso controlado y solo con autorización personal externo
Pública	Activo de Información que puede conocer el personal interno o externo.

Adaptado de CELEC, 2016b, P. 4.

El resultado de la clasificación de la información que se maneja en el COT se lo que presenta a continuación:

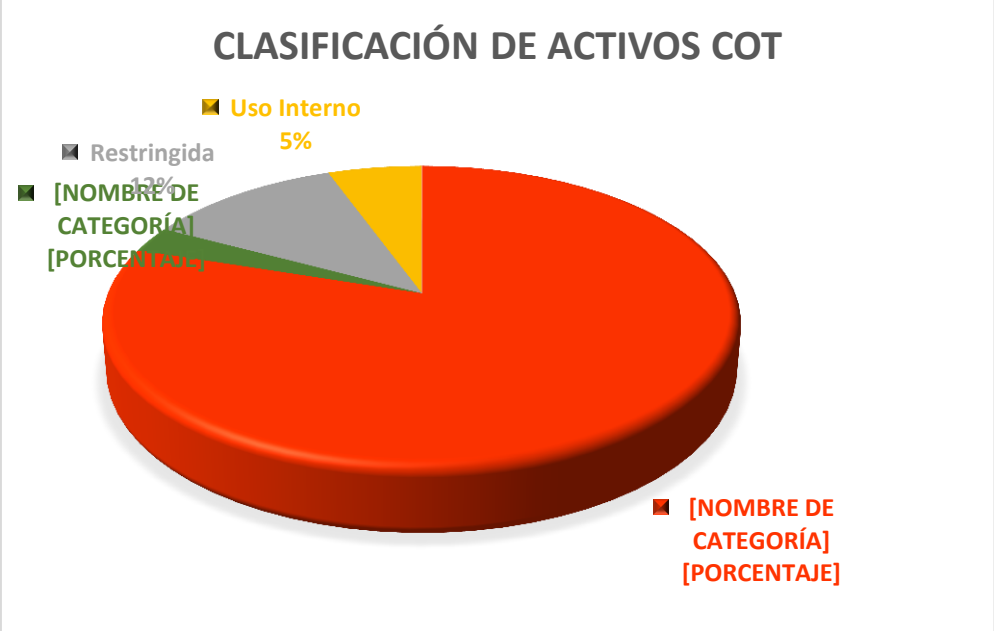


Figura 21 Clasificación de Activos de Información del COT.
Tomado de Talleres de Gestión de Riesgos COT, 2017.

Adicionalmente se logró identificar la importancia de los activos de información que fueron clasificados de acuerdo a la descripción de los siguientes valores:

Tabla 16
Importancia de los activos de Información.

Valor	Descripción
Crítico	**ALTA probabilidad de pérdida operativa de los procesos de giro de negocio así como de lograr los objetivos estratégicos**.
Grave	En caso de pérdida o difusión no autorizada hay una **POSIBLE probabilidad de pérdida objetivos y metas del proceso o procesos vinculados.**
Importante	En caso de pérdida o difusión no autorizada hay una **POSIBLE** probabilidad de **pérdida reputación, imagen y credibilidad.**
Prescindible	En caso de pérdida o difusión no autorizada hay una **BAJA probabilidad** de **afectación a las labores diarias o bienestar del personal.**

Adaptado de CELEC, 2016b, P. 10.

El resultado de la importancia de los activos del COT se representa a continuación:

Figura 22 Importancia de Activos del COT.
Tomado de Talleres de Gestión de Riesgos COT, 2017.

Para la recopilación de la información sobre los activos y la elaboración de estos talleres se utilizó el formulario Identificación de activos de Información Anexo 9.

4.6.3 Identificación de amenazas, vulnerabilidades y consecuencias

Una vez identificados y valorados los activos de información se determinan las amenazas, vulnerabilidades y consecuencias que afectan a los activos identificados como críticos, graves e importantes. (Adaptado CELEC, 2016b, P. 10). Por ser la primera vez que se realizó este análisis se decidió realizar la determinación para todos los activos.

Se identificaron como amenazas cualquier acción o actividad, sean éstos: desastres naturales, errores humanos (accidentales o deliberados), ataques internos o externos, fallas de servicios, entre otros, que pueden afectar a cada activo de información o varios, provocando no estos queden inoperable o afecte su desempeño de las actividades del COT. Al identificar las amenazas es posible anticiparse a los efectos de las mismas. (Adaptado CELEC, 2016b, P. 10-11).

Para las vulnerabilidades se detectó el origen para que la amenaza se pueda producir, con la finalidad de prevenir, detectar o corregirlas, se consideró las consecuencias como el efecto de producirse la amenaza. (Adaptado CELEC, 2016b, P. 11).

El formulario para la elaboración de la matriz para la determinación de amenazas, vulnerabilidades y consecuencias se lo presenta en el anexo 10.
Una vez identificadas las amenazas es necesario valorarlas en función de los criterios de probabilidad e impacto. (Adaptado de CELEC, 2016b, P. 11).
Los criterios que se usaron para calificar la probabilidad de ocurrencia fueron los siguientes:

Tabla 17
Criterios de Valoración de Probabilidad.

Probabilidad de ocurrencia		**Descripción**
Alta	3	✓ Es muy probable que ocurra el evento. ✓ La probabilidad de ocurra es siempre o casi siempre. ✓ Puede ocurrir 3 o más veces al año.
Medio	2	✓ Es probable que el evento ocurra. ✓ La probabilidad que ocurra es posible. ✓ Puede ocurrir 2 veces al año.
Baja	1	✓ Es excepcional que ocurra el evento. ✓ Probabilidad que ocurra es remota. ✓ Puede ocurrir una vez al año.

Tomado de CELEC, 2016b, P. 11.

Los criterios que se usaron para calificar el impacto deben ser especificados en términos del grado de daño o costo que representan para el Centro de Control y a su vez a la Corporación, dentro de los que se puede mencionar:

- ✓ Criticidad de los activos que se están analizando.
- ✓ Nivel de clasificación de los activos de información impactados.
- ✓ Afectación a la disponibilidad, integridad y confidencialidad de la información.
- ✓ Pérdida de la operación del Centro de Control.
- ✓ Pérdida en valores financieros.
- ✓ Incumplimientos de requisitos legales, reglamentarios y contractuales. (Adaptado de CELEC, 2016b, P. 12).

Los criterios para calificar el nivel de impacto se muestran a continuación:

Tabla 18
Criterios de Valoración de Impacto.

Probabilidad de ocurrencia		**Descripción**
Grave	3	✓ Interrupción total de la Operación y procesos de apoyo. ✓ Pérdida de información irrecuperable del negocio clasificada como confidencial. ✓ Pérdidas financieras con graves consecuencias para la organización.
Moderado	2	✓ Interrupción parcial de la operación y procesos de apoyo. ✓ Pérdida de información recuperable del negocio clasificada como confidencial. ✓ Pérdidas financieras con leves consecuencias para la organización.
Menor	1	✓ Interrupción mínima de la operación y procesos de apoyo. ✓ Pérdida de la información del negocio clasificada como de uso interno. ✓ Pérdidas financieras sin consecuencias para la organización.

Tomado de CELEC, 2016b, P. 12.

4.6.4 Evaluación del riesgo

La evaluación del riesgo se realiza tomando en consideración el valor estimado del activo, la probabilidad de ocurrencia de una amenaza y su impacto. Se determina con la siguiente fórmula.

*Riesgo = Probabilidad * Impacto*

Los posibles valores asignados para probabilidad e impacto, son combinados para establecer la matriz de criticidad. (Tomado de CELEC, 2016b, P. 13).

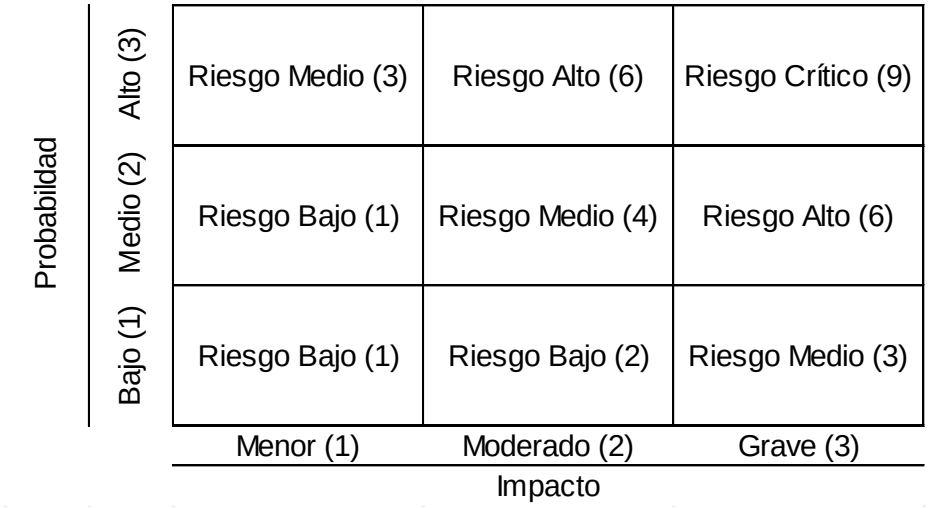


Figura 23 Matriz de Criticidad.

Tomado de CELEC, 2016b, P. 13.

A continuación se presenta la clasificación del nivel de los riesgos:

Tabla 19
Clasificación de nivel de riesgos.

Riesgo	Nivel de Riesgo
Crítico	Nivel de riesgo cuyo impacto es considerado como **inaceptable** para la Corporación, y se debe buscar una **solución inmediata** para llevar el riesgo a un nivel tolerable Se sugiere suspender las actividades relacionadas hasta que las condiciones de riesgo sean modificadas.

Alto	Nivel de riesgo es considerado **inadecuado** para la Corporación y se debe buscar solución a corto plazo (menor a 90 días) y llevar el riesgo a una zona aceptable. Se recomienda operar en condiciones especiales y limitadas.
Medio	Presenta un nivel de riesgo controlable, el cual debe ser mitigado con técnicas que permitan reducir la severidad en la afectación o la probabilidad de la materialización del riesgo. Se requiere tomar acciones correctivas en (menos de 180 días).
Bajo	Niveles de riesgo que se consideran aceptables en el desarrollo de las actividades. El propietario del activo lo administra con procedimientos permanentes.

Adaptado de CELEC, 2016b, P. 13-14.

Se consideraron las amenazas y vulnerabilidades que pueden sufrir los activos de información, los mismos que podrían producir afectaciones e interrupciones a la Operación normal del COT, sin efectuar ninguna acción de mitigación y se obtuvieron los **riesgos inherentes** que se muestran a continuación.

Figura 24 Riesgos inherentes del COT.

Tomado de Talleres de Gestión de Riesgos COT, 2017.

Se estimó que el **COT tiene 20% de riesgo crítico** sobre sus activos, valor que se considera inaceptable y que debe ser **atendido de forma inmediata** para no poner en peligro su operación, un nivel de riesgo **alto de 56%** que debe ser tratado para **llevarlo a un nivel aceptable** y un nivel medio de 24% que debe ser atendido e implementado acciones correctivas para disminuir su afectación.

4.6.5 Criterios de Aceptación del Riesgo

La Corporación para sus activos de información ha establecido como **aceptable** los rangos de **bajo y medio,** debido a que su probabilidad de ocurrencia o su impacto está en **rangos tolerables para la Operación del COT,** en el caso de materializarse una o varias amenazas. (Adaptado CELEC, 2016b, P. 14).

4.6.6 Tratamiento del Riesgo

La mitigación o tratamiento del riesgo, comprende la priorización e implementación de controles que reduzcan los riesgos. (Adaptado CELEC, 2016b, P. 14).

4.6.7 Análisis de controles

Los controles permiten hacer frente a las amenazas, se definió que éstos pueden ser procedimientos, instructivos, políticas, normativas, estándares, guías técnicas, aplicaciones, software, hardware, dispositivos físicos, comunicación, contratos de servicios con proveedores externos e internos, etc. (Adaptado CELEC, 2016b, P. 12).

Los controles que se definieron fueron: **controles preventivos** si se aplican antes de la ocurrencia del incidente disruptivo que afecte la Operación, **controles detectivos**, si se aplican durante el incidente o **controles correctivos** se aplican después de ocurrido el incidente. (Adaptado CELEC, 2016b, P. 12).

4.6.8 Implementación de controles

Se definieron una lista de controles y acciones de tratamiento para mitigar el nivel de riesgo de los activos de información, los cuales de manera general se presentan según la clasificación de los tipos de activos y los controles definidos para éstos.

Instalaciones

Las instalaciones del Centro de Operación de Transmisión podrían estar sujetas a diversas amenazas como: desastres naturales, terremotos, erupciones volcánicas, inundaciones, etc., que pueden causar daños severos a su infraestructura imposibilitando su funcionamiento, se propone:

- ✓ Habilitar y poner en funcionamiento el Centro de Contingencia ubicado en la provincia del Guayas, dotándole de todos los recursos necesarios, entre los que se puede destacar: recursos tecnológicos, medios de comunicación, así como el personal con sus funciones específicas, tanto en situaciones normales como de emergencia, levantando rutinas de monitoreo y control sobre esta nueva instalación.

Servicios Auxiliares

Los sistemas complementarios permiten realizar las normales actividades del COT, estos sistemas a pesar de sus condiciones de redundancia y alta disponibilidad, con las que fueron diseñadas, en caso de una falla severa pueden comprometer de gran manera la continuidad de la operación del COT, para esto se propone:

- ✓ Realizar una actualización de los Sistemas Complementarios del Centro de Control de Transmisión, dada la obsolescencia tecnológica que están presentado los equipos.

- ✓ Establecer contratos de mantenimiento preventivo y correctivo con niveles de servicio, sobre los elementos de los sistemas complementarios del COT garantizando su disponibilidad.

- ✓ Establecer rutinas de pruebas y monitoreo para los equipos de los sistemas complementarios, así como implementar sistemas automáticos de monitoreo y alarmas asociadas a los mismos que permitan prevenir y alertar ante cualquier falla de estos sistemas.

Equipos informáticos

Arquitectura del Sistema SCADA (hardware y networking) y sus componentes están sujetos a daños de sus elementos para lo cual se propone:

- ✓ Mantener y extender los contratos de soporte de partes y piezas con niveles de servicio con el proveedor de hardware y networking.

- ✓ Implementar niveles de servicio internos con las áreas que habilitan la operación del COT, para garantizar los recursos tecnológicos necesarios para sus funciones.

Aplicaciones de software

Se detectó problemas con los procesos de las actualizaciones de software y correcciones de errores del sistema SCADA por parte del suministrador, que han generado suspensiones de servicio, para lo cual se propone:

- ✓ Trabajar con el suministrador del sistema SCADA EMS, con quien se establecerá un control sobre los accesos al Sistema Central, con la finalidad de auditar cambios de componentes no controlados.

- ✓ Iniciar en forma inmediata con las especificaciones técnicas, responsables, procedimientos y cronogramas de la nueva actualización del Sistema SCADA EMS, dado que al ser la principal herramienta del COT, debe causar el menor impacto sobre la continuidad de la operación del S.N.T.

Datos e información.

Como se había mencionado el COT no tiene formalizado sus procesos ni procedimientos esto hace que las actividades sean realizadas con informalidad, una mala ejecución de una actualización de componentes fundamentales o configuraciones de los componentes del núcleo del sistema podrían generar paros en la operación, por tal razón se definió:

- ✓ Formalizar los procesos, procedimientos e instructivos necesarios para el desarrollo de las diferentes actividades dentro del Centro de Control, se definieron responsables para su elaboración e implementación de los mismos, así como se establecieron los índices primarios para su control y mejoramiento en tiempos establecidos.

- ✓ Revisar y actualizar si fuera del caso todos los planos técnicos y manuales de usuarios, administración y de configuración de los sistemas complementarios, componentes del Sistema SCADA EMS, así como de los desarrollos internos.

- ✓ Definir procedimientos, herramientas y responsables de la administración de la información digital e impresa del Centro de Operación de Transmisión, estableciendo un solo repositorio de la misma, para evitar versiones no controladas de documentos y fuga de información, eliminando copias no autorizadas. De igual manera cada documento para su difusión deberá estar controlado su versión, registrado y autorizado.

- ✓ Se implementarán procedimientos y rutinas de monitoreo y control para los componentes del SCADA EMS, del COT y de las demás áreas relacionadas con la Operación del Sistema de Transmisión.

- ✓ Se generarán procedimientos específicos para aplicaciones de negocio propias del desarrollo de las actividades, ajenas a las rutinas diarias, con la finalidad de disponer de una base de conocimiento detallada de los componentes del Sistema SCADA EMS y del COT.

Servicios

El COT dispone de una herramienta, el cliente ligero parte del sistema SCADA, que permite la conexión remota de varios usuarios, esto se realiza a través del Internet, por tal motivo se extremar todas las prevenciones con referencia a la seguridad de información, para evitar cualquier tipo de incidente invasivo que genere alteraciones en el servicio del Sistema SCADA.

- ✓ Realizar una Auditoría Cibernética para determinar el nivel de seguridad de las aplicaciones expuestas al Internet, parte del Sistema SCADA e implementar las mejoras que de ésta se presenten, con la finalidad de disponer el mayor grado de seguridad y disponibilidad de los servicios brindados por el COT.

Dada la importancia de los activos que se controlan desde el COT, toda la infraestructura del Sistema Nacional de Transmisión, se deben extremar las medidas de seguridad para todos los componentes de los sistemas asociados su Operación.

- ✓ Se analizarán y corregirán de ser el caso los diferentes permisos y perfiles de usuarios de las soluciones informáticas, sistemas y los equipos del Centro de Operación, documentando y formalizando las acciones que sean generados de este control.

- ✓ Se trabajará en conjunto con el Departamento de Seguridad de la CELEC con la finalidad de cumplir con la Norma de Seguridad implementada, la cual define e incluye las bases e introduce los marcos referenciales para la gestión de la Continuidad, incluyendo su Norma, para lo cual se seguirá un proceso de aprendizaje a través de charlas y talleres de difusión y cumpliendo sus controles, sus informes y auditorías periódicas.

- ✓ Llevar un control, con procedimientos definidos, sobre el manejo herramienta de antivirus, manejo de malware y respaldos del CCT, registrando diariamente la ejecución y adecuado funcionamiento de estas soluciones, comprobando además su validez y definiendo un lugar adecuado para el almacenamiento de los medios en el caso de los respaldos de información. Esto permitirá en el caso de algún evento que requiera reponer la información o algún servidor crítico hacerlo con la agilidad requerida.

- ✓ Integrar y alinearse con los objetivos estratégicos con el Departamento de Tecnologías de la Información, analizando y corrigiendo todos los servicios brindados en conjunto con la finalidad de ser un soporte adecuado para los procesos del negocio.

Personal

- ✓ Se deberá gestionar en conjunto con el Departamento de Talento Humano la formalización de los contratos definitivos, de igual manera implementar un plan de carrera e incentivos de todo el personal que labora en las diferentes Secciones y Áreas estratégicas del Centro de Operación, buscando así evitar la alta rotación de personal que se ha presentado en los últimos tiempos, o que al no definir planes claros sobre el talento humano se puedan presentar deserciones futuras de personal técnico.

En base a estos controles se determinó el indicador de **Criticidad de Riesgo Residual**, que se obtiene sobre la misma matriz, pero implementando los controles respectivos, en base de lo cual se tiene lo siguiente:

Figura 25 Riesgo residual del COT.
Tomado de Talleres de Gestión de Riesgos COT, 2017.

Se ha propuesto **reducir todos los riesgos críticos** que existen actualmente en el COT a través de un adecuado tratamiento y seguimiento de los mismos, de cumplirse lo esperado todo permanecerá con nivel de **22% de riesgo alto**, **porcentaje aceptado** por la institución dado que se ha definido un cronograma semestral de verificación de cumplimiento de los controles, enfocando a la reducción de riesgos residuales en un período de tiempo no mayor a un año.

A continuación, se puede apreciar la forma en que se dará el tratamiento de los riesgos, lo que muestra que la implementación de los controles en su mayoría depende de los participantes en el proceso de operación:

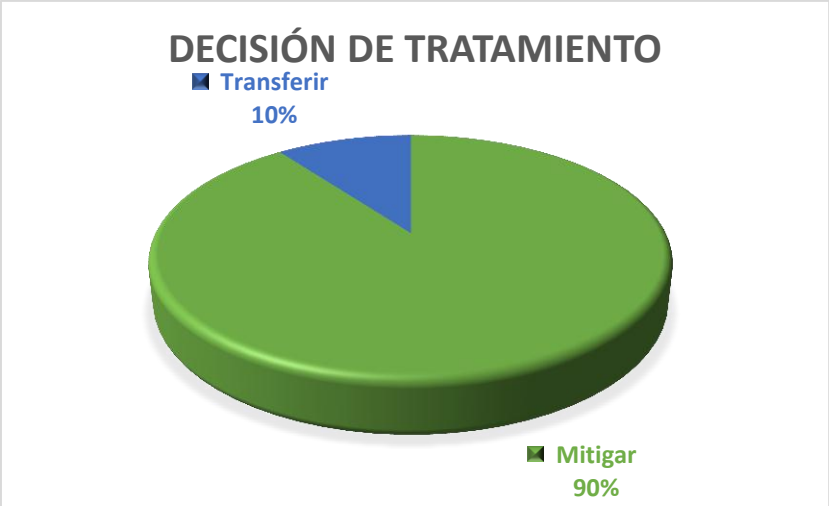


Figura 26 Decisión de tratamiento de riesgos del COT.
Tomado de Talleres de Gestión de Riesgos COT, 2017.

Del análisis se puede acotar que en su mayoría los controles implementados son preventivos sobre los correctivos como se aprecian en la siguiente gráfica:

Figura 27 Tipos de controles implementados en el COT.
Tomado de Talleres de Gestión de Riesgos COT, 2017.

Es muy importante el manejo que se realice de todos los controles, ya que como se puede apreciar existe una falla considerable en el proceso documental, tanto de los activos de información como de los controles de los riesgos, esto se lo puede verificar en la figura siguiente:

Figura 28 Documentación de riesgos de controles del COT
Tomado de Talleres de Gestión de Riesgos COT, 2017.

Un ejemplo de la matriz con la que se trabajó para la elaboración del análisis de la gestión de riesgos se lo presenta en el anexo 11.

4.7 Identificar prioridades y objetivos de continuidad

4.7.1 Análisis de Impacto de negocio

Para el análisis de Impacto de Negocio se validó la Operación del S.N.T. bajo el **contexto de la organización**, definido en el numeral 4.2.1 de este documento, enfocando los posibles impactos de una pérdida de continuidad en la entrega de servicio, considerando criterios como: el impacto **social y económico** con las posibles pérdidas financieras, el **cumplimiento de regulaciones** y obligaciones legales; el deterioro de la **imagen** y la **reputación**, de igual forma cuán fundamentales son las operaciones en la razón de ser del COT.

Posteriormente se analizó el principal proceso del COT con todos los subprocesos involucrados definidos en cada una de las secciones que apoyan la operación en tiempo real detallado en el numeral **3.2 Servicios brindados por el Departamento de Operación** y se llegó a la selección de **procesos y actividades mínimas requeridas**, de igual manera se estableció los **tiempos y recursos necesarios para la reanudación** de dichas actividades, estas definiciones se las alcanzó luego de varios talleres y reuniones con las jefaturas de las secciones involucradas y su personal técnico.

4.7.2 Impacto de Negocio para Operación del S.N.T.

Al producirse un incidente disruptivo sobre el COT y que esto provoque que no pueda Operar el S.N.T. podrían presentar los siguientes impactos analizados desde varios criterios:

- ✓ **Social y Económico:**

  Siendo el suministro de energía un pilar fundamental de la economía de todo país, una falla en la reposición del servicio causa serios problemas a la población en general en todos los aspectos; productivos, de salud, de seguridad, educativos, social, etc. Una demora excesiva en el restablecimiento del servicio eléctrico por ausencia del COT, traería pérdidas económicas considerables para el Ecuador, según un estudio del valor de la energía no suministrada, según Resolución de Directorio del CONELEC Nro. 025/11 de 14 de abril de 2011 vigente hasta la actualidad, define el costo de la energía no suministrada a nivel nacional 1.533 USD/kwh.

Para tener una panorámica del impacto de no disponer del suministro de energía a nivel nacional se realizaron análisis y cálculos en función del costo de la energía no suministrada, los totales de consumo ecuatoriano y valores de la implementación, requerimientos y condiciones establecidas para el Centro de Operación Alterno, con lo que se obtuvo que la inversión de la implementación del **Sitio Alterno es 35.2% del costo** de **una hora de energía no suministrada** en **Ecuador**, **en** período de **máxima demanda**. (Datos de Taller de Impacto de Negocio, 2017). Este cálculo se lo puede observar a continuación:

Impacto Económico Implementación de Centro de Operación Alterno

Datos:	
Costo energía no suministrada (USD/kwh).	$ 1,53
Energía suministrada al Ecuador en hora pico (Mwh).	3714,5
Energía suministrada al Ecuador en hora pico (kwh).	3.714.500,0
Cálculos:	
Costo de Energía no suministrada en el Ecuador en hora pico (USD).	**$ 5.683.185,0**
Costo del Centro de Control Alterno (Definido por el proveedor) (USD)	**$ 2.000.000,00**

Conclusiones:

- El costo de implementar el Centro Alterno es 35.2 % del costo de una hora de energía no suministrada en el Ecuador en la hora pico.
- La inversión del Centro Alterno se paga en 21 minutos de energía no suministrado al país en período de demanda máxima.

Figura 29 Impacto económico de Implantación de COT Alterno.
Tomado de Talleres de Impacto de Negocio, 2017.

El Valor de energía no suministrada al Ecuador en hora pico se tomó de los datos de CENACE, mismo que se detalla a continuación:

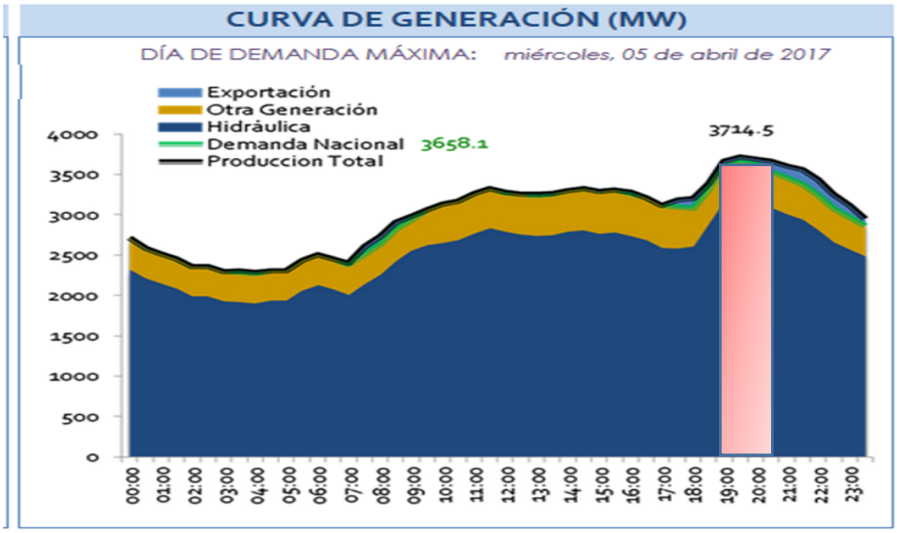


Figura 30 Curva de Generación

Tomado de www.cenace.org.ec/docs/InformacionOperativa. 2017.

El anterior análisis se lo realiza desde el impacto que produce a la sociedad, no se está considerando desde el punto de CELEC EP TRANSELECTRIC y las regulaciones y normativas a las cuales está sujeta.

✓ **Cumplimiento de Regulaciones:**

Las siguientes Regulaciones, entre otras se aplican para el desarrollo de las actividades del COT y sus obligaciones, las mencionadas regulaciones se encuentra en vigencia desde su promulgación.

✓ El Consejo Nacional de Electricidad, en su momento organismo rector del Sector Eléctrico, definió las funciones del COT en su Regulación sobre la **Administración Técnica y Operativa del Sistema de Transmisión 014/99:** adicionalmente enuncia que "*El Trasmisor deberá contar con un centro de operación del sistema de transmisión para cumplir sus funciones*" (CONELEC, 1999, P.3).

- ✓ En la resolución del CONELEC **0125/00** detalla todos los **Procedimientos de despacho y Operación del Sistema Nacional Interconectado** y las funciones y tareas de todos los actores del Sector eléctrico, dentro de este documento se menciona que los objetivos de estos procedimientos son *reducir al mínimo posible el tiempo de restablecimiento del S.N.I., considerando prioritario la integridad de las personas, la conservación de los equipos y la continuidad del servicio*. (CONELEC, 2000, P.93).

- ✓ Por la regulación **Procedimientos del mercado eléctrico mayorista en el numeral** 6.12.3 **asignación de sobrecostos** a los agentes se indica que los *sobrecostos derivados de las restricciones operativas* serán asignados a cada uno de los *agentes y/o el transmisor que los provoquen*, los mismos que servirán para compensar a los generadores que entraron sobre el despacho económico. (CONELEC, 2000a, P.39).

- ✓ En la regulación de **Calidad de transporte de electricidad** define los niveles y procedimientos de **evaluación de la calidad de servicio** de trasmisión y conexión del S.N.T., adicionalmente estipula explícitamente el *número de desconexiones y valores límites que el Transmisor debe cumplir* (Adaptado CONELEC, 1998, P.22).

- ✓ Adicionalmente a las regulaciones CELEC EP TRANSELECTRIC define **indicadores anuales de gestión**, para cumplir con las expectativas planteadas, esto se informa a los organismos de control y son analizadas en detalle en el proyecto de Gobierno por Resultados GPR, instrumento que permite evaluar al Poder Ejecutivo ecuatoriano sobre el cumplimiento de sus metas institucionales de diferentes sectores. (SENPLADES., 2013, P.93).

Los indicadores que TRANSELECTRIC declara cumplir son muy específicos sobre componentes esenciales de la operación diaria, como Disponibilidad de líneas de transmisión de 230 kV y 138 kV y Transformadores de potencia.

A continuación, se presenta un esquema de los indicadores del año 2016 y parte del 2017 para transformadores declarados para el GPR, el cumplimiento de estos índices se lo puede hacer utilizando todas las herramientas tecnológicas necesarias que dispone el COT, de no disponer de las condiciones necesarias para efectuar sus normales labores y precautelar la vida de los equipos y las instalaciones, resultaría muy complicada cumplir con las metas anuales definidas.

Figura 31 Disponibilidad de Transformadores

Tomado de Subgerencia Operación y Mantenimiento., 2017, P. 3.

El diagrama anterior corresponde a los datos tabulares de los indicadores de transformadores para el año 2016 y el avance del 2017 en relación a las metas, se los puede apreciar a continuación:

Tabla 20
Indicadores de disponibilidad de transformadores.

		2016			2017		
MES	ELEMENTO	Resultado	Meta	IGRP	Resultado	Meta	IGRP
Enero	TRAFOS	99,81	99,59	100,22%	99,86	99,69	100,17%
Febrero	TRAFOS	99,82	99,59	100,23%	99,84	99,69	100,15%
Marzo	TRAFOS	99,83	99,59	100,24%	99,84	99,69	100,15%
Abril	TRAFOS	99,84	99,59	100,25%		99,69	
Mayo	TRAFOS	99,82	99,59	100,23%		99,69	
Junio	TRAFOS	99,82	99,59	100,23%		99,69	
Julio	TRAFOS	99,83	99,59	100,24%		99,69	
Agosto	TRAFOS	99,87	99,59	100,28%		99,69	
Septiembre	TRAFOS	99,87	99,59	100,28%		99,69	
Octubre	TRAFOS	99,90	99,59	100,31%		99,69	
Noviembre	TRAFOS	99,88	99,59	100,29%		99,69	
Diciembre	TRAFOS	99,86	99,59	100,27%		99,69	

Tomado de Subgerencia Operación y Mantenimiento, 2017, P. 3.

Como se aprecia las metas de disponibilidad de los transformadores para cada mes son elevadas y necesitan de toda capacidad tecnológica instalada para cumplir con estos índices.

- ✓ **Imagen y reputación:**

  La imagen institucional se vería degradada rápidamente en el caso de una demora de más de dos horas en el restablecimiento del servicio por ausencia del COT; considerando adicionalmente que una vez que TRANSELECTRIC habilita su servicio, les corresponde a las empresas distribuidoras normalizar el servicio en las ciudades, lo que a percepción del usuario final podrían ser más de 3 o hasta 4 horas, en el peor de los casos, sin servicio de electricidad por culpa del Transmisor.

Con lo señalado anteriormente, en referencia al contexto que rodea al Centro de Operación de Transmisión, se llegó a definir como crítica la Operación del S.N.T. y que la falta de la herramienta para que el COT desempeñe sus labores causaría serios impactos tanto para el desarrollo de las actividades de la sociedad, provocando serios y fuertes problemas de reglamentarios y económicos para CELEC.

Por tal motivo es fundamental disponer inmediatamente de otra instalación alterna, en el caso de que la principal falle, que permita cumplir con el proceso de supervisar y controlar la red eléctrica ecuatoriana, esto permitió definir un **tiempo de recuperación de 0 horas.**

Este análisis de Impacto de Negocio estratégico para el COT del proceso de Operar el Sistema Nacional de Transmisión se lo puede apreciar a continuación:

BIA ESTRATEGICO

Valor	Impacto
3	Alto
2	Medio
1	Bajo

Producto o Servicio	Operación del Sistema Nacional de Transmisión						
MTPD	La electricidad por ser un servicio básico, todos los esfuerzos serán enfocados a la recuperación del servicio a la comunidad y por ende la necesidad de disponer o reponer el Centro de Control es crítico.						
RTO	0 hora						
	Tiempo (Horas)						
Impactos	0	1	2	3	4		Razón (Intolerable - qué factores fueron considerados para decidir en qué punto llegó a ser intolerable cada valor del impacto)
Imagen Reputación	2	2	3				La imagen institucional se vería degrada rápidamente en el caso de una demora mayor a 2 horas en el restablecimiento del servicio por ausencia del COT.
Pérdida Financiera	3						Ante una demora excesiva en el restablecimiento del servicio eléctrico por ausencia del COT, la población del Ecuador se ve perjudicada en el valor de la enegía no suministrada, según Resolución de Directorio del CONELEC Nro. 025/11 de 14 de abril de 2011 vigente hasta la actualidad el costo de la Energía no suministrada a nivel nacional es de 1.533 USD/kWh.
Cumplimiento Regulaciones	3						CONELEC - 14 /99. CONELEC - 006/00. CONELEC - 007/00. CONELEC - 003/08. ARCONEL - 003/16.
Operación	3						La operación del SNT no podría ejecutarse sin el COT.
Social / Ambiental	3						La falta del COT tiene un impacto directo sobre la accesibilidad del suministro de energía eléctrica a la población.

Figura 32 Identificación de impacto de negocio del COT.

Tomado de Talleres de Impacto de Negocio, 2017.

4.7.3 Análisis de Impacto de Negocio de los procesos operativos

Para el Análisis de Impacto de negocio para el COT, se enfocará a su macro proceso **Operar el Sistema de Transmisión,** analizando sus tres subprocesos: Realizar análisis pre operativo, Operar en Tiempo Real el Sistema Nacional de Transmisión y Evaluar la operación del S.N.T.

Con estos antecedentes analizando el estado de complejidad y el entorno nacional, se llegó a la siguiente definición:

- ✓ Para la Operación del Sistema Nacional de Transmisión es indispensable contar con t**odas las herramientas del Centro de Control de Transmisión**, todas los subprocesos y actividades serán replicadas en el caso de una falla del sistema principal, para lo cual es fundamental y básico disponer del personal y los recursos técnicos necesarios para supervisar, monitorear y de ser posible controlar todo el S.N.T.

- ✓ En el supuesto de presentarse una Falla Total del COT actual, se implementará y se proveerá de todas las facilidades para tener un Centro Alterno.

De igual forma se ha contemplado realizar los análisis de impacto para los procesos de apoyo necesarios y habilitantes para la operación requeridos por el COT de sus áreas y secciones involucradas, de todas las actividades definidas para las secciones se escogió las que son necesarias para complementar las actividades del COT y que serán requeridas en el COT alterno.

4.7.3.1 Impacto de Negocio de la Sección SCADA EMS

La principal herramienta para la Operación del S.N.T. constituye el Sistema de monitoreo en tiempo real, el Sistema SCADA EMS y puesto que se definió que la necesidad es tener el COT siempre disponible, la Sección Administración SCADA deberá proveer todo su contingente y cumplir este requerimiento.

Se habilitará el mencionado Centro con todos los medios tecnológicos, aplicaciones necesarias para cumplir con sus funciones requeridas; es importante señalar que este proceso conlleva realizar trabajos en conjunto con las diferentes áreas de la Unidad de Negocio, como el Departamento de Tecnologías de Información, Subgerencia de Telecomunicaciones y la Gerencia Financiera y de Recursos Humanos.

Del análisis la **Administración SCADA EMS, realizará todas sus actividades paralelamente en el Centro Principal como en su Sitio Alterno,** garantizando la funcionalidad de los dos Centros. En caso de presentarse la necesidad de utilizar solo el Centro Alterno por alguna contingencia, **excluirá las siguientes actividades**:

a) Gestionar y participar en la implementación de nuevas instalaciones del S.N.T. en el sistema SCADA EMS coordinadamente con CENACE.
b) Participar en la recepción y puesta en marcha de sistemas de automatización de subestaciones.
c) Monitorear y Controlar los sistemas Complementarios del COT.

Estas actividades mientras dure la emergencia, serán suspendidas para garantizar la consolidación de sus bases de datos y registros del Sitio Alterno, enfocando todo su esfuerzo en garantizar la disponibilidad del alterno y recuperación del Centro Principal.

El **proceso** establecido para viabilizar la continuidad de esta sección es **Administrar el componente del Sistema Central**.

4.7.3.2 Análisis de Impacto de negocio para el Área de Programación y Control

De esta **Sección** en el caso de una **emergencia** serán requeridas **dos actividades esenciales**:

a) Planificar y Programar los trabajos de mantenimiento y logística.
b) Analizar la Operación en Condiciones Normales y de Emergencia.

Estas a**ctividades están en estrecha relación con el día a día del COT** y serán realizadas **incluso en el caso de estar en contingencia**:

La primera actividad constituye la **planificación y programación de todos los trabajos de mantenimiento** de las **Zonas Operativas**, este proceso se lo hace con **una semana de antelación**, por lo cual el encargado debe presentar su trabajo semanal disponiendo de siete días para su elaboración y entrega al COT.

Los **mantenimientos urgentes y diarios pasarán a ser coordinados y administrados directamente por el COT**, que no tendrá problema con asumir dichas actividades. El personal responsable para la ejecución de estas tareas puede trabajar desde otra ubicación, no necesariamente en las instalaciones de los Centros de Control, a través de un acceso remoto a las aplicaciones corporativas para el manejo y registros de las órdenes de trabajo y planificación de los mantenimientos.

El segundo proceso es **Analizar la Operación en Condiciones Normales y de Emergencia,** esta actividad no requiere la presencia de los responsables en las instalaciones de los Centros, pero en el caso de darse una contingencia es de fundamental importancia informar oficialmente como se efectuó la Operación del S.N.T.

Cabe anotar que para la entrega de estos reportes se los debe **realizar a día caído de operación,** y que el encargado de recuperar la fuente de la información es el COT, con lo que se garantizará la entrega de los datos disponibles para la elaboración de este informe. El personal de Programación y Control, es el encargado de validar y consolidar los datos y la generación de éste y todos los reportes necesarios para su efecto.

4.7.3.3 Análisis de Impacto de Negocio para el Área de Estudios Eléctricos:

Las funciones definidas para garantizar la continuidad en el desenvolvimiento de las actividades del COT, para el Área de Estudios eléctricos son:

a) Gestionar y Coordinar Consignaciones con CENACE.
b) Analizar la Seguridad y Confiabilidad del S.N.T.

La primera constituye parte de la **elaboración y validación en detalle técnico de los mantenimientos y rutinas de trabajo** que se realizan **cada semana** en el COT y constatar que no exista ningún tipo de inconveniente técnico en su ejecución; actividad que se realiza en conjunto con personal de CENACE, nuevamente se debe señalar que los mantenimientos y trabajos urgentes serán coordinados por el COT, en el caso de ser requeridos durante una fase de emergencia.

Para la elaboración de estas actividades los responsables de esta área necesitan la información de las zonas operativas y trabajar en conjunto con los diferentes encargados de las diversas empresas eléctricas, adicionalmente requieren disponer de acceso remoto a los sistemas corporativos para el proceso de las órdenes de trabajo, mecanismos de comunicación y mensajería.

Para el **segundo proceso** que es **Analizar la Seguridad y Confiabilidad del S.N.T.**, que constituye la **generación de un reporte periódico** o **por evento debido a un incidente en la red eléctrica**, dentro de un **tiempo definido o posterior a una falla**, constituye un complemento al reporte de fallas generado por el COT. Se requiere que el responsable de la elaboración de este informe disponga de un acceso remoto al sistema SCADA y a los aplicativos de análisis de red eléctrica corporativos, adicionalmente necesita medios de comunicación, Internet y mensajería.

A continuación se presenta un resumen de los procesos requeridos para la Operación del S.N.T. así como de los tiempos objetivos de recuperación.

Tabla 21
Procesos y subprocesos imprescindibles para el negocio COT.

PROCESO	SUB - PROCESO	RTO-Proceso
OPERAR EL S.N.T.	Operar en Tiempo Real el SNT.	0 Horas
	Administrar el componente SCADA del Sistema Central.	0 Horas
	Analizar la Seguridad y Confiabilidad del SNT.	1 dia
	Gestionar y Coordinar Consignaciones con CENACE	1 semana
	Analizar la Operación en Condiciones Normales y de Emergencia	1 dia
	Planificar y programar los trabajos de mantenimiento y logistica.	1 semana
RTO= Tiempo objetivo tiempo de recuperación		

Tomado de Talleres de Impacto de Negocio COT, 2017.

4.8 Determinación prioridades y recursos necesarios para su mitigación

4.8.1 Establecer estrategias de continuidad.

Para cumplir con las expectativas del Análisis de impacto de negocio y del análisis de riesgos y continuar con la Operación del Sistema Nacional de Transmisión, se plantean las siguientes estrategias de continuidad:

Habilitar el Centro de Control Alterno de Contingencia, para lo cual se realizará una reubicación y redistribución de las actividades y de los recursos, transfiriendo **todo el monitoreo y control del S.N.T.,** durante la contingencia, se trabajará desde esta instalación en la cual se dispondrá de todas las herramientas tecnológicas que dispone el Centro Principal, comunicaciones y recursos, así como existirá un turno de operadores que seguirá trabajando permanentemente.

Es necesario indicar que las condiciones operativas para este Centro Alterno son con menores recursos que el Centro principal, con un nivel de servicio acordado, es decir no se dispone del mismo número de consolas de trabajo, líneas telefónicas, sistema de retroproyección, pero se cuenta con un puesto de trabajo con las condiciones necesarias para tener un adecuado nivel de supervisión y control de las subestaciones del S.N.T.

Actualmente este sistema, que fue implementado para precautelar la operación en caso del volcán Cotopaxi, sin entrar en operación tecnológicamente cuenta con el **51.5% de visibilidad independiente del Sistema eléctrico ecuatoriano** (Dato de los Talleres de Análisis de Impacto del Negocio, 2017), lo que a futuro permitirá disponer de la supervisión de todas las subestaciones. Es necesario exponer que con un **sólo cambio de configuración en los componentes de la red de datos de los Centros de Control,** entre CENACE y CELEC EP Transelectric la visibilidad del sistema se incrementaría al **78.7%**.

La sección **SCADA EMS entregará y coordinará las herramientas y procedimientos de monitoreo para garantizar la funcionalidad del Sitio Alterno durante la etapa de desarrollo normal de actividades y en contingencia**.

Para los **procesos de soporte de Programación y Control y Estudios Eléctricos,** requeridos para la Operación en emergencia, es necesario disponer de **soluciones alternativas temporales, habilitando conexiones remotas hacia el Centro Alterno,** adicionalmente contar con los sistemas corporativos y de comunicaciones necesarias, estos sistemas estarán a cargo de los departamentos de Tecnología y Telecomunicaciones respectivamente

Para cumplir con las estrategias definidas se podrán habilitar las consolas remotas para apoyar las actividades de Operación durante la contingencia, en el edificio matriz de TRANSELECTRIC; examinando las condiciones existentes en estas instalaciones, se ha verificado que se dispone de consolas remotas del SCADA y las comunicaciones adecuadas, para que en un determinado nivel de contingencia, se podría monitorear remotamente el S.N.T. utilizando estos recursos conectados al sistema de Contingencia.

Adicionalmente se ha **analizado la opción de coordinar y formalizar el respaldo entre Centros de Control** que se mantiene con **CENACE**, legalmente en la Regulación de ARCONEL 006-2016 se menciona que el COT, podrá considerarse como respaldo del Centro del Operador de Energía, pero no define el escenario inverso. Cabe recalcar que en algunas ocasiones por situaciones inesperadas cada Centro ha solventado los incidentes del otro, pero no existe actualmente un acuerdo formal para cubrir dicha contingencia. Es necesario fortalecer convenios y formalizar procedimientos y estrategias para velar por la continuidad operativa de las dos instituciones. Algo importante de recalcar es que los dos centros de control no previenen una situación de emergencia en toda la zona norte del Ecuador, por estar en la misma ciudad, por esta razón se ha propuesto la habilitación del **Centro Alterno de Contingencia** en la **costa ecuatoriana**.

4.9 Análisis de escenarios y disparadores Plan de Continuidad

4.9.1 Análisis de escenarios

A continuación, se detallan los escenarios en los que, al presentarse un incidente disruptivo, sería necesario aplicar el plan de continuidad, para seguir brindado los servicios del COT.

- **Desastres naturales**

  Terremotos, erupciones volcánicas, inundaciones, incendios, tormentas eléctricas, etc., que pueden causar daños severos a las instalaciones y que imposibiliten seguir laborando desde el COT.

- **Fallos en los equipos y/o fallos en los sistemas esenciales del COT**

  Provocados intencionalmente o presentados durante su funcionamiento.

  - *Falla en los sistemas complementarios:*
    - Sistemas de suministro de energía ininterrumpida.
    - Sistemas de climatización inoperables.
    - Incendios no controlados en la sala de equipos.
    - Inundación en la sala de equipos.
    - Fallo masivo en los de servicios de comunicaciones hacia el Centro de Control, lo que implicaría pérdida de adquisición de datos con subestaciones e incomunicación del COT por pérdida del servicio telefónico propio y externo debido a fallas críticas en el sistema de fibra óptica.

  - *Falla en los sistemas núcleo del Centro de Operación:*
    - Servidores SCADA inoperables.
    - Daño de los arreglos de servidores de comunicación.

- **Ataque destructivo de las instalaciones**

  Vandalismo, terrorismo, acción militar, amenaza que puede ser perpetrada por personal interno, por personas ajenas a la Institución.

- **Indisponibilidad del personal**

  Ausentismo masivo del personal por razones de fuerza mayor, imposibilidad de ingresar a las instalaciones del COT. (Adaptado de CELEC EP. 2015b. P. 11).

4.9.2 Disparadores del plan de continuidad

Durante la operación normal del S.N.T. y de producirse un evento disruptivo descripto anteriormente, el COT procederá a notificar el incidente a la Administración SCADA, quienes analizarán si aplica o no una contingencia; de no ser requerida la declaratoria, gestionará la corrección del incidente, lo implementarán, lo evaluarán y serán los encargados de restaurar el servicio.

En el supuesto caso de que se aplique la generación de contingencia, convocarán al equipo de evaluación del incidente, quienes seguirán el proceso interno definido por la CELEC de Gestión del Incidente de Seguridad de Información y en el caso de ser requerido notificarán a través de su Coordinador la Declaratoria de Falla Masiva en el COT.

1. Luego de recibir la **Declaratoria de Falla Total, el Centro de Contingencia Alterno, inmediatamente tomará el Control e iniciará la operación a un nivel aceptado del S.N.T**., su personal quedará en espera de la notificación de restablecimiento del Centro principal.

2. Mientras tanto el personal encargado del restablecimiento del servicio, garantizará el funcionamiento del Centro Alterno al nivel aceptado, puede ser requerido una validación de los servicios y constatar todas las conexiones a los diferentes puntos del Sistema Nacional de Transmisión, luego de lo cual podrá dar un estado del funcionamiento del COT alterno posterior al incidente.

Paralelamente parte del equipo de recuperación del negocio analizará la viabilidad de soportar al equipo de **contingencia desde otras instalaciones**, dada la complejidad de la Operación, con la finalidad de apoyar en las acciones de monitoreo, supervisión y restablecimiento del Sistema Nacional de transmisión, parte de este equipo cumplirán estas actividades:

3. Analizarán la posibilidad de iniciar las actividades de apoyo al Proceso de Contingencia desde las consolas del edificio matriz de TRANSELECTRIC.

De no tener las condiciones para apoyar la Operación desde estas instalaciones.

4. Analizarán la posibilidad de iniciar las actividades de apoyo el Proceso de Contingencia desde las consolas remotas del Centro de Control de CENACE

De igual forma de no contar con las condiciones necesarias para apoyar la Operación desde esta instalación.

5. Iniciarán el traslado hacia las instalaciones del Centro de Contingencia para soportar la operación que se está dando en el Sitio de Contingencia Alterno.

Desde la Declaratoria de Falla total el equipo de restablecimiento del Negocio entre personal de SCADA, TIC, Seguridad y Telecomunicaciones, iniciarán las tareas de recuperación, hasta lograr la restauración total del servicio, gestionarán la solución, realizarán las pruebas y deberán asegurarse del funcionamiento integral del COT. En elaboración del Plan de continuidad deberán detallarse las actividades de cada responsable para la restauración de forma general ya que los eventos y los mecanismos de recuperación son diversos, pero las funciones de restauración deberán esta claras para cada responsable.

Una vez recibida la Notificación de Terminación de Operación del Centro Alterno.

6. Terminará la Operación en contingencia y Notificará la finalización de Operación Alterna y entregará la operación al Centro Principal. las condiciones y procedimientos de retorno a la operación normal deberá ser detallada a profundidad en la elaboración del Plan de Continuidad.

El proceso de continuidad para el COT se lo puede analizar en detalle en la figura a continuación:

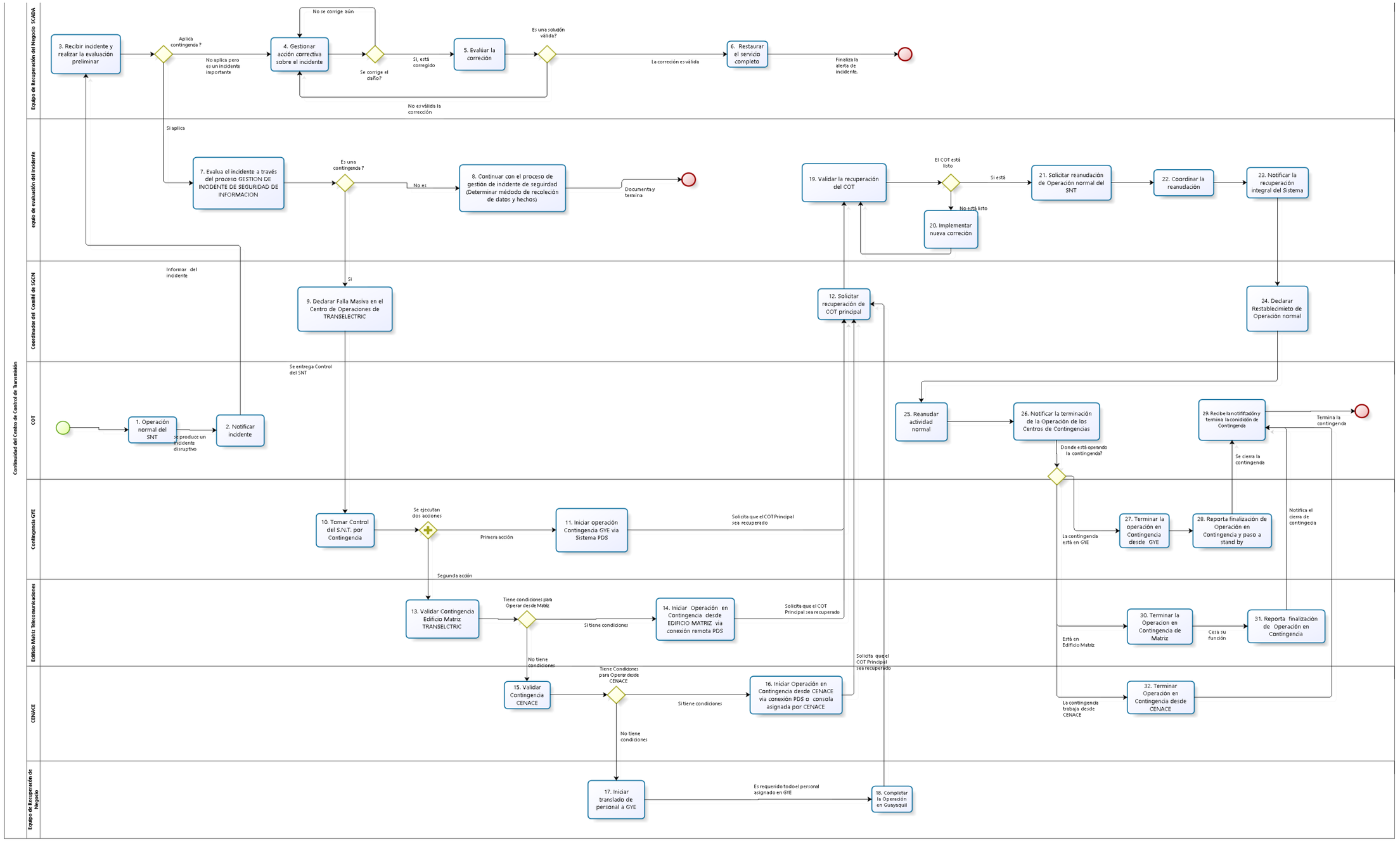


Figura 33 Proceso de Continuidad de Negocio del COT.

Tomado de Talleres de Estrategias de Continuidad, 2017

4.10 Definición de recursos que soporten los procedimientos de continuidad de negocio.

Para garantizar la Operación del S.N.T. se definió la estrategia de **Centro de contingencia alterno, l**os recursos que apoyarán la incorporación de esta solución, se los ha contemplado desde dos puntos de vista, desde la Administración SCADA como suministradores del servicio y desde la concepción del COT como el usuario.

4.10.1 Requerimientos de sitio alterno Administración SCADA

- Personal:

Especialistas que se encargarán de velar por la disponibilidad y la entrega del servicio:

  - Administrador del Componente SCADA (1)
  - Administrador de las Aplicaciones EMS (1).
  - Experto en Hardware y Software del Sistema (1).
  - Experto en REDES (1).
  - Personal De Telecomunicaciones.
  - Personal De Tecnologías de la Información.

- Instalaciones:
  - Se debe disponer de un lugar para trabajar diferente que el Centro de Control de TRANSELECTRIC. Se ha definido tener tres lugares adecuados en una subestación en la zona de la provincia del Guayas:
    - Un espacio provisto de todas las condiciones ambientales y de seguridad para albergar los sistemas informáticos del SCADA alterno y todos los implementos de red necesarios para sus comunicaciones.
    - Un sitio para realizar las actividades propias del personal del COT Alterno.
    - Un puesto de trabajo para el personal de SCADA habilitado para realizar sus tareas de monitoreo y validación del Sistema Alterno.

- Tecnología:

Sistema SCADA de Contingencia

  - Servidor SCADA EMS.
  - Servidor de comunicaciones con las subestaciones.
  - Servidor de comunicación entre Centros de Control.
  - Servidor de servicios Web.
  - Servidor de datos históricos.
  - Servidor de generación de bases de datos de configuración.
  - Consola de operación local.
  - Equipos de redes y seguridad.
  - Aplicaciones EMS.
  - Herramienta de análisis eléctrico.
  - Computador (2) para acceso al sistema corporativo de TRANSELECTRIC.

- Información:
  - Planes y procedimientos de contingencia y continuidad.
  - Procedimientos SCADA EMS.
  - Procedimiento de configuración del sistema SCADA.
  - Acceso al Sistema Integrado de Información y herramientas corporativas.
  - Reportes Operativos y de Falla.
  - Documentación de Operación y Acceso a los repositorios de Información.
- Transporte
  - Vehículo para transporte para las opciones del Apoyo a los Centro de Control.
  - Movilización para el transporte de personal de emergencia hacia el COT alterno. (incluyendo: pasajes aéreos, movilización interna etc.)
- Finanzas
  - Se deberá definir partidas presupuestarias y cajas de dinero para cubrir los presupuestos de emergencia. (Personal, alimentación, movilización, servicios para la operación, etc.)

- Proveedores
    - Canales de comunicación operativos con las UTR de las subestaciones para la visibilidad del S.N.T.
    - Líneas telefónicas disponibles fijas y móviles con las subestaciones y el CENACE.
    - Acceso y monitoreo de los diferentes sistemas esenciales para la operación del COT.
    - Acceso a los sistemas corporativos:
        - Sistema integrado de información.
        - Sistema de Registro de novedades.
        - Correo electrónico.
        - Internet.
        - Ofimática.
- Suministros
    - Servicios Básicos: Agua, Luz, Servicios sanitarios, alimentación, entre otros.
    - Teléfonos fijos (telefonía IP y líneas directas) y móviles para la comunicación con las subestaciones.
    - Líneas de comunicación directa con el CENACE.
- Inventarios
    - Sistema de Contingencia (1).
    - Consola de sistema (1).
    - Consola del cliente ligero (Thin Client) (2).
    - Computador corporativo (2).
    - Sitio para trabajar:
        - Escritorio (1).
        - Computador portátil (2).
        - Enseres de oficina, etc.

4.10.2 Requerimiento de sitio alterno COT.

- Personal:

Operador del COT alterno, Personal entrenado que pueda realizar las actividades. Un Puesto de Operador (4 personas para cubrir turnos de 24 horas, su actividad será de trabajo normal en la Zona Sur, es decir coordinará las actividades y mantenimiento de la zona del Guayas y territorios aledaños, en condiciones normales y en caso de una emergencia operará y será el responsable del Sitio Alterno)

- Instalaciones:
    - Se debe disponer de un lugar para trabajar diferente que el Centro de Control de Transelectric, con equipos y sistemas para realizar y cumplir con el Proceso de Operar el S.N.T.
- Tecnología:
    - Acceso a un Sitio Alterno.
    - Una consola remota al sistema SCADA EMS del Sistema Principal.
    - Computador (1) para acceso al sistema corporativo de Transelectric.
    - Herramienta de análisis y estudios eléctricos.
    - Acceso al Sistema Integrado de Información y herramientas corporativas.
- Información:
    - Planes y procedimientos de contingencia.
    - Toda la información y datos operativos.
    - Plan semanal de mantenimiento y consignaciones.
    - Acceso al Sistema Integrado de Información, herramienta corporativa.
    - Reportes Operativos y de Falla.
    - Documentación de Operación y Acceso a los repositorios de Información.
- Transporte
    - Vehículo para transporte para las opciones de apoyo del Centro de Alterno al Matriz y/o CENACE.
    - Movilización para el transporte de personal de emergencia hacia el COT alterno. (incluyendo: pasajes aéreos, movilización interna, etc.)

- Finanzas
    - Se deberá definir partidas presupuestarias y cajas de dinero disponibles para cubrir los presupuestos de emergencia. (Personal, alimentación, movilización, servicios, etc.)
- Proveedores
    - Sistema SCADA alterno operativo a nivel acordado.
    - Comunicaciones con las Subestaciones para la visibilidad del S.N.T.
    - Líneas telefónicas disponibles fijas y móviles.
    - Disponer líneas directas para comunicación con el CENACE.
    - Acceso a los diferentes sistemas necesarios para la operación del COT, detallados en el numeral 3.3.2.2 Sistemas Especializados.
    - Acceso a los sistemas corporativos:
        - Sistema integrado de información.
        - Sistema de Registro de novedades.
        - Correo electrónico.
        - Internet.
        - Ofimática.
- Suministros
    - Servicios Básicos: Agua, Luz, Servicios sanitarios, Alimentación, entre otros.
    - Teléfonos fijos (telefonía IP y líneas directas) y móviles para la comunicación con las subestaciones.
    - Líneas de comunicación directa con el CENACE.
- Inventarios
    - Sistema de Contingencia (1)
    - Consola de sistema (1)
    - Consola del cliente ligero (Thin Client) (2)
    - Computador corporativo (1)
    - Sitio para trabajar:
        - Escritorio (1),
        - Computador portátil (2),
        - Enseres de oficina, etc.

Lo anteriormente señalado constituye lo mínimo requerido para la operación del Sitio alterno, se deberá disponer de los requisitos en las otras opciones de Centro Alterno, para habilitar el Centro de Apoyo en Matriz y/o CENACE.

4.10.3 Requerimientos para procesos Sitios Remotos

Los requisitos para los procesos de las secciones de Estudios eléctricos y para Programación y Control, se los puede ver como uno sólo ya que la estrategia para solventar éstos es una solución de Trabajo Remoto; se ha planificado que esto podría hacérselo desde las oficinas del Edificio Matriz de Transelectric o desde los hogares de los responsables, de tal forma se tiene lo siguiente:

- Personal:

Especialistas que se encargarán de realizar los procesos establecidos para la emergencia

  - Responsable de Estudios Eléctricos (1)
  - Responsable de Programación y Control (1)

- Instalaciones:
  - Disponer de un sitio de trabajo desde el cual realizar las tareas de los procesos de Estudios eléctricos y para Programación y Control, podría ser un lugar en las instalaciones del edificio matriz o con las condiciones necesarias y accesos respectivos podría trabajarse desde sus residencias.
- Tecnología:
  - Acceso al sistema SCADA del Centro Alterno a través de la herramienta del Cliente Remoto (Thin Client).
  - Computador para acceso remoto a los sistemas corporativos de TRANSELECTRIC.
  - Teléfonos fijos y móviles para la comunicación con las subestaciones y las empresas eléctricas.
- Información:
  - Planes y procedimientos de contingencia y continuidad.
  - Plan semanal de mantenimiento y consignaciones.
  - Información de las Zonas Operativas.

    - Acceso al Sistema Integrado de Información y herramientas corporativas.
    - Reportes Operativos y de Falla.
    - Documentación de Operación y Acceso a los repositorios de Información.
- Transporte
    - Capacidad de transporte al sitio de trabajo alterno asignado.
- Finanzas
    - Presupuesto para pago de transporte y telefonía móvil de ser necesario.
- Proveedores
    - Cliente Remoto (Thin client) al SCADA alterno.
    - Líneas telefónicas disponibles fijas y móviles con las subestaciones y el CENACE.
    - Acceso a los sistemas corporativos:
        - Sistema integrado de información.
        - Sistema de Registro de novedades.
        - Correo electrónico.
        - Internet.
        - Ofimática.
- Suministros
    - Teléfonos fijos (telefonía IP y líneas directas) y móviles para la comunicación con las subestaciones.
- Inventarios
    - Computador corporativo (1)
    - Lugar disponible para trabajar:
        - Escritorio (1),
        - Computador portátil (1),
        - Enseres de oficina, etc.

El formato que se utilizó para la definición de los recursos se lo puede apreciar en el anexo 14.

4.11 Estructura del Plan de Continuidad

Una vez definida la estrategia de continuidad se deberá desarrollar el Plan de Continuidad, a pesar de no ser objetivo de este proyecto de titulación la obtención de este documento, a continuación se presenta la estructura general de este plan:

Plan de continuidad

Control de documento

Datos generales del documento

Control de Aprobaciones

1. Introducción

1.1. Objetivos y Alcance del Plan de continuidad.

1.2. Vigencia.

1.3. Propiedad.

1.4. Supuestos del Plan de continuidad.

1.5. Exclusión del plan de continuidad.

2. Organización, conformación de equipos y responsabilidades

2.1. Comité de Continuidad.

2.2. Coordinador del Plan.

2.3. Equipos del Recuperación y Continuidad.

3. Notificación - invocación – escalamiento

3.1. Criterios de activación

3.2. Procedimiento de activación

3.2.1. Diagrama de flujo de la activación.

3.3. Proceso de Notificación y comunicación.

3.3.1. Diagrama de flujo de la comunicación.

3.3.2. Datos de contactos.

3.3.2.1. Internos principales, Internos alternos.

3.3.2.2. Contactos externos

4. Lista de tareas

5. Información de soporte.

6. **Actividades críticas del negocio.**
   6.1. Procedimientos de aplicación.
7. **Recursos de recuperación**
8. **Interdependencias e interacciones internas y externas.**
9. **Flujo de información.** (De cada proceso crítico)
   9.1. Flujo funcional de los documentos del proceso.
   9.2. Flujo técnico por donde fluye la información.
10. **Plantillas y formularios.** (Adaptado de Flores, S., et al. 2015, P.162-163).

4.12 Definir las pruebas y mecanismos de verificación

4.12.1 Plan de Pruebas

Se ha planificado realizar un plan de pruebas para todos los componentes y documentos involucrados en las estrategias de continuidad, A continuación se presenta el detalle y periodicidad sugerida para las pruebas de verificación del SCGN:

Tabla 22
Tipos de prueba y Periodicidad

Nombre de la Prueba	Descripción	Periodicidad.
Discusiones de escenarios.	Se efectúan reuniones de trabajo donde se debe identificar un escenario de siniestro y se debate sobre si las acciones descritas en el plan de recuperación son adecuadas.	Cada 6 meses.
Pruebas de mesa	Analizar a profundidad las acciones de remediación para responder a un escenario de siniestro en particular.	
Puesto de mando	Simular un escenario lo más cercano a la realidad de lo que puede pasar en términos de presión a la que se ve sometida el equipo que debe gestionar la recuperación	Una vez cada dos años mínimo.
Pruebas unitarias	Pruebas enfocadas al equipamiento haciendo uso de medios de recuperación	Una vez al año.
Simulacros	Ejercicio más real en relación al evento que puede producirse, que permiten probar la eficacia de la respuesta ante un incidente.	Por lo menos 1 vez cada tres años.

Adaptado de SECURITYARTWORK..2016.

4.12.2 Mecanismos de Verificación

A continuación se presenta en detalle lo que fue definió en los Talleres Validación y Mejoramiento del Plan de Continuidad, 2017 como requerimiento en detalle de la validación técnica del Centro de Control Principal y del Alterno, y de los servicios remotos.

- ✓ **Validación técnica del COT Principal y Sitio alterno**
  - Comprobación de operatividad de componentes y herramientas del Sistema SCADA.
  - Validación y comprobación de canales de comunicación con las Unidades de Terminal Remota (UTR) de las subestaciones y porcentaje de visibilidad del Sistema.
  - Aplicaciones de energía EMS con modelo convergente y herramienta de análisis eléctrico disponible.
  - Reporte de la aplicación de análisis eléctrico integrada al sistema SCADA.
  - Reporte de Sistema SCADA; arquitectura de los sistemas, accesos locales y remotos, registros de logs, infraestructura de la sala de servidores, manejo de antivirus y respaldos.
  - Consolas del sistema SCADA y corporativas disponibles con capacidad de ingresar a los sistemas de contingencia y principal
  - Disponibilidad de generar reportes históricos del sistema SCADA, validación y actualización de los mismos.
  - Sistemas corporativos accesibles; Internet, correo electrónico, antivirus corporativo, ofimática, entre otros.
  - Accesos a información digital a través de los repositorios corporativos y documentación escrita actualizada y controlada.
  - Validación de accesos y permisos de usuarios así como de horarios.
  - Reportes generados por Operación: periodicidad, responsabilidad, publicación y almacenamiento de los mismos.

- ✓ **Validación técnica de los servicios remotos**
  - Equipos operativos, sistemas y antivirus actualizados, ofimática disponible.
  - Cliente de comunicación y seguridad de red configurada para atender las conexiones remotas a los Centros de Control Principal y Alterno, así como herramientas de acceso a soluciones corporativas y repositorios.
  - Registro de conexiones: usuarios, sesiones iniciadas, concluidas y tiempo de uso.
  - Disponibilidad de la herramienta de acceso remoto.
- ✓ Validación de implementación y control de procesos, procedimientos, instructivos, manuales, archivos de configuración y demás documentos.
- ✓ Validación de implementación de controles sobre los activos de información.
- ✓ Validación sobre usuarios y controles para generación y dada de baja de los mismos.

Para todos los controles se han definido responsables, tiempos de ejecución y planes de implementación. (Adaptado de Talleres Validación y Mejoramiento del Plan de Continuidad, 2017)

4.13 Realizar auditorías internas

4.13.1 Procedimientos de monitoreo y control para el SCN.

Para realizar un correcto monitoreo y control del Sistema de Gestión de Continuidad se lo realizará a través de procedimientos de seguimiento por parte de cada uno de los responsables de la implementación de los controles y serán evidenciados y documentados en auditorías internas.

4.13.2 Auditorías internas

Las auditorias o revisiones del Sistema de continuidad analizan los controles relacionados con los activos de información, para la ejecución de las mismas se basarán en los lineamientos para las Auditorías de Seguridad definidas por la Corporación, que consideran lo siguiente:

- *Responsable de las Auditorias*: que serán los encargados de la Gestión del plan de auditorías y de supervisión de la aplicación de la misma.

- *Equipo Auditor:* cuya responsabilidad será determinar el alcance de las auditorías, revisar los procedimientos y los formularios y comprobar la exactitud de los hechos, generar los informes y preservar las evidencias de las auditorías.

Estipula las siguientes normas generales:

a) Las auditorías pueden ser programadas semestralmente para el SGCN o anuales, para las demás auditorias relacionadas con los activos de información del COT, cumpliendo compromisos contractuales o ser requeridas por el Departamento de Seguridad de la Corporación, para lo cual se deben indicar con claridad el objeto y alcance.

   A Continuación, se presenta el cronograma y una breve descripción de las auditorías a realizarse en el COT, la finalidad de las estas auditorías es permitir identificar posibles elementos que podrían ser considerados como amenazas para el Sistema SCADA y sus componentes, una vez identificados, podrán ser controlarlos y de esta manera seguir con la alta disponibilidad requerida.

Tabla 23
Auditorías Sistema SCADA

Auditorías del Sistema SCADA EMS	
Objetivo	Consistirá en el control de las funcionalidades del Sistema SCADA-EMS. Permitirá mantener la fiabilidad operacional de su sistema; anticiparse a los problemas; conocer el estado y desempeño del sistema, detectando puntos de mejora. (Requerimiento contractual con el proveedor)

Periodicidad:	Anual
Fechas	Mayo 2017: Auditaría del Sistema luego de la primera actualización del SCADA. Enero 2018: Auditaría del Sistema previa a la segunda actualización. Mayo 2019: Auditaría del Sistema, una vez finalizada la segunda actualización

Adaptado de CELEC EP. 2012a. P.130.

Tabla 24
Auditorías de Seguridad de Información

Auditorías del Seguridad de Información	
Objetivo	Analizar los controles relacionados con la seguridad sea esta física o lógica, orientada a la protección de la información que garantice su integridad y disponibilidad. (Responsabilidad del Departamento de Seguridad de Información de la CELEC.)
Periodicidad:	Anual.
Fechas	Agosto 2017: Auditoría al COT

Adaptado de CELEC EP. 2017. P.4.

Tabla 25
Auditoría de Configuración Seguridad Cibernética

Auditoría de Configuración de seguridad Cibernética	
Objetivo	Realizar una verificación de configuración de seguridad cibernética, basándose en estándares aplicables a la instalación y configuración de los sistemas SCADA como los estándares NERC-CIP. (Requerimiento contractual con el proveedor)
Periodicidad:	Anual.
Fechas	Enero 2018: Validación de seguridad luego de la primera actualización. Mayo 2019: Validación del seguridad, una vez finalizada la segunda actualización

Adaptado de CELEC EP. 2012a. P.201-202.

Tabla 26
Auditoría del Sistema de Continuidad de Negocio

Auditoria del Sistema de Gestión de Continuidad de Negocio	
Objetivo	Realizar una verificación de los componentes del SGCN, validando entre otros sus estrategias e indicadores definidos, así como Plan de Continuidad. (Responsabilidad del Comité de SGCN y el Departamento de Seguridad de la Corporación)
Periodicidad:	Semestral
Fechas	Julio 2018: evaluación de indicadores de efectividad del plan y ejecución de controles. Diciembre 2018: evaluación de indicadores y propuesta de mejoras para el 2019.

Adaptado de Talleres de Gestión de Riesgos. 2017.

b) El Equipo Auditor interno debe ser totalmente independiente del objeto de la auditoría, asegurando la imparcialidad y objetividad de la misma.

c) Para la elaboración de auditorías se debe tomar en cuenta como documentación mínima (criterios de auditoría):

- ✓ Organigrama de los servicios y/o áreas con descripción de funciones y responsabilidades.
- ✓ Identificación de los responsables de la información, servicios, seguridad, procesos, procedimientos que serán objeto de la auditoría o revisión.
- ✓ Descripción detallada de los sistemas y/o servicios de información a auditar dentro de los cuales pueden ser software, hardware, comunicaciones, equipamiento auxiliar, ubicaciones y similares.
- ✓ Norma Técnica de Seguridad de Información de la Corporación.
- ✓ Informe de Análisis de Riesgos.
- ✓ Informe de Análisis de Impacto de Negocio.
- ✓ Estrategias de Continuidad establecidas.
- ✓ Planes de Continuidad.
- ✓ Pruebas de la ejecución del Plan de continuidad.

- ✓ Información de controles de seguridad aplicados e implementados.
- ✓ Informes de auditorías previas de seguridad internas o externas realizadas los sistemas y/o servicios de información, incluidos en el alcance de la auditoría o revisión de seguridad.
- ✓ Informes de seguimiento de deficiencias detectadas en auditorías previas de seguridad relacionadas con el objeto de la auditoría o revisión de seguridad.
- ✓ Lista de proveedores externos cuyos servicios se ven afectados o entran dentro del alcance de la auditoría, y evidencias del control realizado sobre estos servicios. (Adaptado de CELEC, 2017)

Como parte del proceso de auditorías del sistema de Continuidad se trabajará con un formato que se muestra en el anexo 16.

4.14 Revisar periódicamente los planes y acuerdos de continuidad

4.14.1 Mejoras

Las mejoras sobre el sistema de Continuidad de Negocio, se deberán registrar y gestionar en base a la definición de los indicadores de gestión para la administración de los riesgos.

Será necesario validar los tiempos de implementación de los controles, el estado del tratamiento de los mismos, analizar las acciones efectuadas para su consecución, así como verificar los resultados sobre la acción y que observaciones se deben dar, presentando un reporte el cual se lo puede apreciar en el anexo 17. (Adaptado de Talleres de Gestión de Riesgos. 2017).

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Se concluye que luego de este trabajo CELEC EP dispone de una metodología que le permite realizar la implementación de un Sistema de Gestión de la Continuidad, en este caso en particular se ha orientado el análisis para el Centro de Operación de TRANSELECTRIC, pero puede ser aplicable para los otros centros de misión crítica de la Corporación, ya que incorpora las fases y actividades que permiten identificar procedimientos, estrategias y recursos de continuidad.

Del **análisis del estado actual** del Centro de Operación de Transmisión se logró lo siguiente:

- Se verificaron los **procesos del COT** dentro los **macro procesos agregadores** de valor de la Corporación, que responden a los objetivos estratégicos que permiten cumplir la misión y visión empresarial.

- Se estableció que el **nivel de capacidad de los procesos** involucrados en **riesgos y continuidad,** definidos **por COBIT 5,** es **parcialmente alcanzado**, según la norma ISO/IEC 15504.

- Se identificó las áreas de TRANSELECTRIC, los **sistemas tecnológicos** y demás **recursos involucrados y requeridos** directamente en la **Operación** del Sistema Nacional de Transmisión.

Se concluye que al determinar la situación actual se encontraron puntos relevantes que fueron de ayuda para determinar la metodología adecuada para el sistema de gestión de continuidad.

Del **análisis de riesgo de los activos del COT**, se obtuvo los siguientes resultados:

- Se logró **identificar los tipos de activos de información**, clasificando todos los elementos fundamentales que permiten cumplir con las tareas de control y monitoreo del Sistema Nacional de Transmisión.

- Con respecto a la **confidencialidad** de los **activos de información** manejados por el COT, se estableció que el **80%** tiene un **valor de muy alta,** es decir que el conocimiento o divulgación no autorizada de la misma tiene **consecuencias a nivel Operativo** y que **11% tiene un valor de alto** es decir que su divulgación no autorizada tiene **consecuencias graves sobre la Corporación.**

- Con respecto a la **integridad** de los **activos información**, se estableció que el **5%** tiene **un valor de muy alto,** es decir que el daño o modificación de la información tiene **consecuencias a nivel operativo,** además se obtuvo que el **84%** tiene un **valor de alto** lo que generaría **consecuencias severas para la Corporación** de darse un daño o modificación de la información.

- Con respecto a la **disponibilidad** de los activos **de información** del COT se obtuvo que **56%** de los mismos tienen un valor **muy alto** es decir **deben estar siempre disponible** para **evitar consecuencias a nivel operativo** de la Corporación y **36%** de los activos tienen un **nivel alto** que significa que los activos pueden tener **un máximo de indisponibilidad de una hora** para **evitar las consecuencias** negativas para la Corporación.

- Se definió que el **80%** de la **información manejada por COT** es **confidencial**, de alta sensibilidad sobre decisiones estratégicas, impacto financiero y requisitos legales, **12%** es **restringida** cuya divulgación no autorizada puede derivar en impactos financieros y legales, el **5%** de la información es **de uso interno** es decir que se debe tener control para áreas y procesos de la corporación y requiere autorización para el personal ajeno a la institución y el **3%** de la información es **pública.**

- Sobre el **riesgo inherente** se concluyó que el COT tiene un **20% riesgo crítico** sobre sus activos, valor considerado **inaceptable** para la Corporación y debe ser atendido de forma inmediata para no poner en peligro la Operación. **56% nivel alto** lo que implica que se debe buscar solución a corto plazo menor a 90 días. Un 2**4% nivel medio** definido como controlable que requiere acciones correctivas en menos de 180 días para disminuir su riesgo.

- Se definió **controles para cada uno de los tipos de activos definidos**, que permitan llevar a estos riesgos a niveles aceptados para la Corporación, **eliminando totalmente el riesgo crítico,** disminuyendo al **22% el riesgo alto** porcentaje aceptado por la institución, ya periódicamente se deberá realizar la verificación del cumplimiento de los controles.

Los resultados del análisis de riesgos permitieron dar una visión completa de los aspectos vulnerables del COT evaluarlos y administrarlos de una forma integral con la finalidad de minimizar los riesgos y aprender a controlarlos para aumentar la disponibilidad del servicio de la Operación del S.N.T.

Del análisis de impacto de negocio sobre la Operación del Sistema Nacional de Transmisión se definió lo siguiente:

- Una pérdida o demora en la entrega del servicio de monitoreo y control del Sistema Nacional de Transmisión traería varios inconvenientes para la Corporación: social y económicamente causaría serios problemas para la población ecuatoriana en varios aspectos, como productivos, de salud, seguridad entre otros, adicionalmente TRANSELECTRIC debería cubrir multas y sobrecostos de energía no suministrada y estaría incumpliendo regulaciones puntuales y obligaciones legales además de traerle pérdidas de imagen y reputación.

- Se priorizó que el COT debería cumplir con su principal proceso de Operar el S.N.T. y todas las tareas que se hacen en sus subprocesos también se las seguirán ejecutando, se definió las actividades mínimas requeridas de cada una de las secciones que apoyan al Centro de Operación de Transmisión así como se definió tiempos, los recursos humanos y tecnológicos necesarios la ejecución de las mismas.

- Se establecieron estrategias de continuidad para seguir con el proceso de Operar el S.N.T. en caso de una falla del COT, se estableció la habilitación del Centro de Control Alterno de Contingencia, así mismo se planteó Servicio Sitios Remotos para los procesos específicos de apoyo a las labores del COT.

- Se plantearon una serie de escenarios en los cuales podrían disparar el plan de continuidad, siendo estos desastres naturales, fallas en equipos y sistemas esenciales del COT, ataques destructivos de las instalaciones e indisponibilidad del personal.

- Se estableció un proceso de Continuidad de la Operación del COT y los roles y responsabilidad de los involucrados en el mismo, así como se definió en detalle los requerimientos de cada una de las estrategias de continuidad.

El impacto de negocio del COT permitió identificar las actividades fundamentales del negocio y así como los mecanismos, estrategias y recursos necesarios para continuar con un nivel de servicio acordado, aspectos esenciales en la elaboración del Sistema de Gestión de Continuidad.

La incorporación del Centro de Contingencia Alterno, es un proyecto complejo que debe seguir un proceso sistemático, que involucra la concientización de la importancia del mismo y comprende actividades básicas como son: la habilitación de medios de comunicación adicionales, integración con sistemas tecnológicos sofisticados aparte del sistema SCADA, entre otros lo que conllevará a cambios de esquemas y procedimientos operativos instituidos.

Se cuenta con una estrategia documental y se estructura el plan de implementación del Sistema de Continuidad de Negocio para el COT, proponiendo un sistema de mejora continua que permitirá conseguir en un período no mayor a dos años, de un Centro de Control de Contingencia Alterno, operativo al 100%.

Es necesario contar con el apoyo directo de las máximas autoridades para el desarrollo del sistema de Gestión de la Continuidad del COT, ya que además de aportar con nuevas iniciativas, necesita alinear ideas y proyectos aislados para encontrar una sinergia adecuada, que responda a los objetivos estratégicos de la empresa, definir responsables, dirigir recursos financieros, tecnológicos y participar en la elaboración de planes, cronogramas y controles para que el cumplimiento de este sistema se realice.

5.2 Recomendaciones

Por la complejidad que involucra el COT con el cúmulo de servicios que necesita, si bien se está planificando y se implementará en toda su operatividad el Sitio Alterno, es igual de necesario e imperioso fortalecer todos los sistemas complementarios y especializados del Centro de Operación Principal, cuyos elementos han sido identificados con sus riesgos y sus respectivos controles, que permitan minimizar los efectos que puedan presentarse ante cualquier incidente disruptivo.

Es fundamental llevar un seguimiento y monitoreo del cumplimiento de los controles levantados sobre los activos de información, considerando que se propusieron mejoras importantes en todos los aspectos relacionados con la operación del S.N.T., entre los cuales se tienen: revisión de la seguridad para los servicios externos del COT, la formalización de procedimientos, instructivos y procesos, así como aspectos que tienen que ver con el manejo del talento humano, en cuyas manos radica la responsabilidad del Centro de Operación.

Se recomienda desarrollar el Plan de Continuidad, con el apoyo de las jefaturas de las secciones del Departamento de Operación y Mantenimiento e involucrar a los responsables del COT para que en conjunto diagramen la mejor solución y se comprometan con el proyecto de la implementación del Sistema de Gestión de Continuidad.

Se recomienda implementar un puesto de trabajo con personal que trabaje inicialmente 12 horas en el Sitio Alterno, dotándole de las facilidades para el desarrollo de sus labores, el mismo que servirá de apoyo puntual y específico para las tareas que realiza el COT específicamente en su Zona Operativa, posteriormente ya consolidado y con todos recursos, ocupará el lugar definido en la estrategia de continuidad, cubriendo todas las funciones de soporte del principal en un esquema de 24 horas los 7 días de la semana.

Sería recomendable la incorporación de otras estrategias de continuidad, tales como viabilizar los procedimientos de operación desde las consolas del Centro de Operación desde el edificio matriz de CELEC EP TRANSELECTRIC o desde las consolas del CENACE, que son necesarias como apoyo a las tareas del Centro de Operación Alterno hasta que su proyecto sea completado.

Se recomienda difundir y compartir la metodología y los resultados con el personal que labora en el Departamento de Operación y Mantenimiento a todos los niveles, ya que los diferentes criterios y puntos de vista podrán apoyar la ejecución del Sistema de Gestión de la Continuidad y permitirán aumentar la resiliencia ante evento disruptivo que pueda ocurrirle al Centro de Operación de Transmisión.

REFERENCIAS

Alexander, A. (2007). Diseño y Gestión de un Sistema de Seguridad de Información.

Amores, L. (2014). Objetivos y Procesos Operativos Administración SCADA EMS.

Asociación Española de Normalización y Certificación [AENOR], (2015a). Norma Sistema de Gestión de Gestión de la Continuidad del Negocio Especificaciones. Norma Española UNE- EN ISO 22301.

Asociación Española de Normalización y Certificación [AENOR], (2015b). Norma Sistema de Gestión de Gestión de Continuidad del Negocio Directrices. Norma Española UNE- EN ISO 22313.

Brito, D., (2016). Taller de adquisición de datos a los Centros de Control del CELEC EP TRANSELECTRIC Y CENACE. [Diapositivas de PowerPoint].

CELEC EP (2012a). Servicios de Mantenimiento y Actualización Continua de los Sistemas SCADA EMS de los Centros de Control de CELEC EP – TRANSELECTRIC y CENACE, [Documento Confidencial de acceso restringido].

CELEC EP - TRANSELECTRIC. (2012). Reseña Histórica, Recuperado 21 de Septiembre de 2015, de https://www.celec.gob.ec/TRANSELECTRIC.

CELEC EP. (2015). La Empresa, Recuperado 9 de Abril de 2017, de https://www.celec.gob.ec/quienes-somos/la-empresa.html

CELEC EP. (2015a). Seguridad de Información Corporativa, Glosario de Términos - SIC-GLO-001-2015, [Documento Confidencial de acceso restringido].

CELEC EP. (2015b). Seguridad de Información Corporativa, Metodología Para El Análisis De Riesgos - SIC-MET-001-2015, [Documento Confidencial de acceso restringido].

CELEC EP. (2015c). Política de Seguridad de Información - SIC-POL-001-2015, [Documento Confidencial de acceso restringido].

CELEC EP. (2017). Guía Auditoría de Seguridad de Información – SIC-ASI-001-2017, [Documento Confidencial de acceso restringido].

CENACE. (2014), Quiénes somos. Recuperado el 17 de febrero el 2017, de: http://www.cenace.org.ec.

CONELEC. (1998). Calidad del Transporte de Electricidad y del Servicio de Transmisión y Conexión en el Sistema Nacional Interconectado.

CONELEC. (1999). Regulación No. 014/99. Administración Técnica Operativa del Sistema de Transmisión.

CONELEC. (2000). Resolución No. 0125/00. Procedimientos de Despacho y Operación.

CONELEC. (2000a). Regulación No. 007/00. Procedimientos de Mercado Eléctrico Mayorista.

Coronel, K. (s.f.). Modelo de Evaluación de Capacidad de procesos de COBIT 5. [Diapositivas de PowerPoint].

Corporación Eléctrica del Ecuador. (2014). Macroproceso Operar el Sistema de transmisión. Gestionar bienes y servicios.

Flores, S., Araujo, V., & Flores, R. (2015). Sistema de Gestión de Continuidad de Negocio (SGCN) [diapositivas de PowerPoint].

Instituto Ecuatoriano de Normalización [INEN], (2014). Norma Técnica Ecuatoriana NTE INEN ISO 31000. Gestión Del Riesgo – Principios Y Directrices. Primera edición.

ISACA. (2012a). COBIT 5 Procesos Catalizadores. Rolling Meadows, EEUU: ISACA.

ISACA. (2012b). COBIT 5 Un Marco de Negocio y la Gestión de las TI de la Empresa. Rolling Meadows, EEUU: ISACA.

ISACA. (2012c). COBIT 5 Resumen Ejecutivo. [Diapositivas de PowerPoint].

ISO 22301. (2013) ¿Qué beneficios tiene la Norma ISO 22301? Recuperado el 11 de septiembre de 2015, de: http://normaiso22301.com/que-beneficios-tiene-la-norma-iso-22301.

ISO 22301. (2014). El camino hacia el éxito. Recuperado el 11 de septiembre de 2015, de: http://normaiso22301.com/iso-22301-razones-para-decidirse.

Lloyd's Register Quality Assurance España. (2016), ISO 22301 Sistema de Gestión de Continuidad de Negocio, Recuperado el 27 de febrero de 2017, de http://www.lrqa.es/certificaciones/iso-22301-continuidad-negocio

Secretaría Nacional de Planificación y Desarrollo – Senplades., 2013, Quito, Ecuador.

SECURITYARTWORK. (2016), Continuidad de Negocio: Las pruebas (II). Recuperado el 8 de agosto de 2017, de: https://www.securityartwork.es/2016/11/17/continuidad-negocio-las pruebas-ii/

Segovia, A. (2016). ISO 22301: Resumen del Proceso de implementación del CGN. [Diapositivas de PowerPoint].

Seguridad y Salud Laboral. (2016). Plan de Gestión de Riesgos Institucional Centro de Trabajo Carapungo. CELEC EP – TRANSELECTRIC.

Subdirección de Procesos y Calidad. (2016). Cadena de Valor CELEC EP. Corporación Eléctrica del Ecuador. [Diapositivas de PowerPoint].

Subgerencia Gestión Organizacional. (2015). Informe Planificación Operativa 2016 – 2017 Subgerencia de Operación y Mantenimiento.

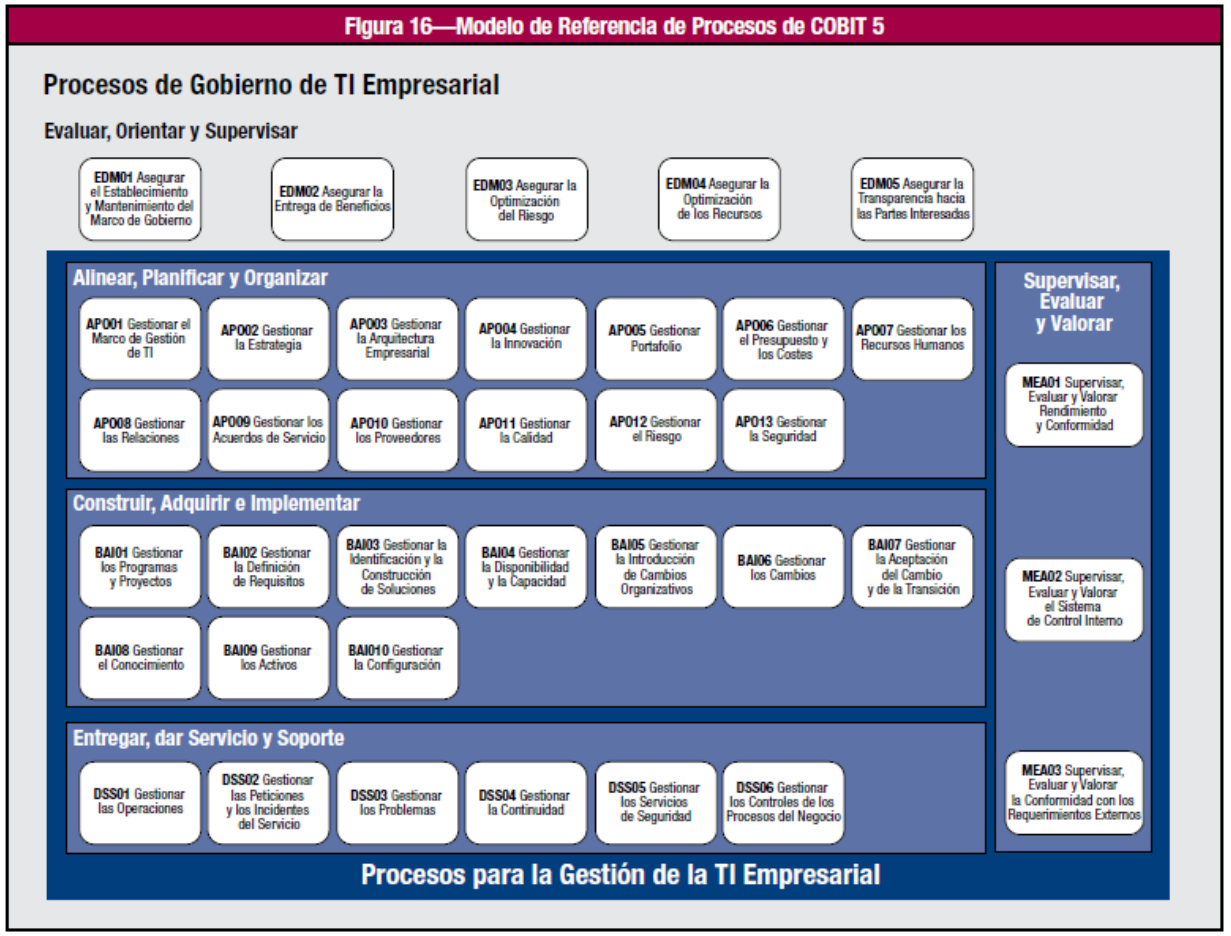
Subgerencia Operación y Mantenimiento. (2016). Informe Cargas de Trabajo. CELEC EP TRANSELECTRIC. [Documento Confidencial de acceso restringido]

Subgerencia Operación y Mantenimiento. (2017). Matriz de Disponibilidad del Sistema Nacional de Transmisión. [Documento Confidencial de acceso restringido]

Torres, F. (2015). Actividades del Departamento de Operación. CELEC EP TRANSELECTRIC. [Diapositivas de PowerPoint].

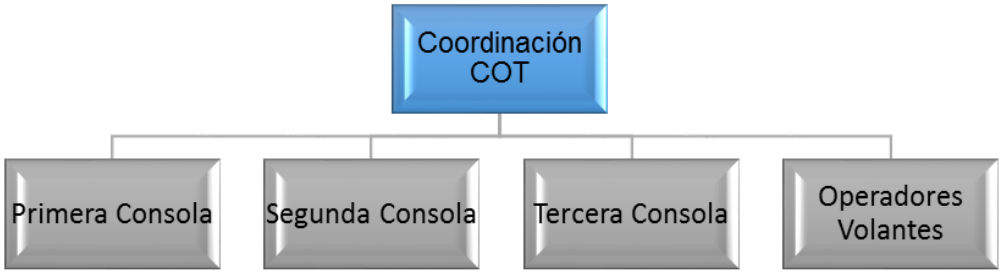
ANEXOS

Anexo 1 Modelo de Referencia de Procesos.



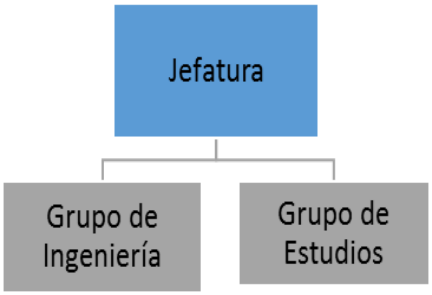
Tomado de ISACA, 2012b, p.33.

Anexo 2 Estructura del Centro de Operación de Transmisión.



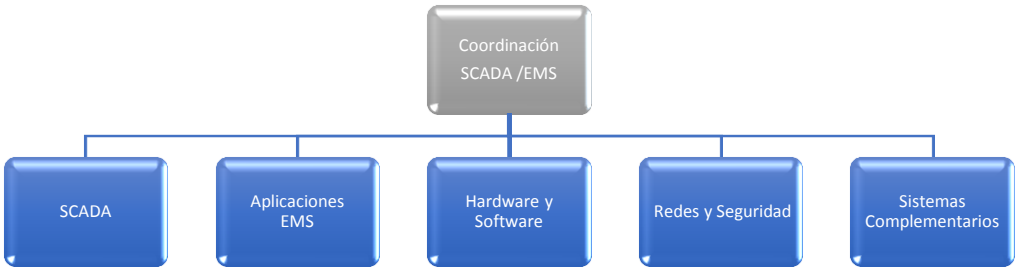
Tomado de Torres F., 2016. P3.

Anexo 3 Diagrama de Procesos Estudios Eléctricos.



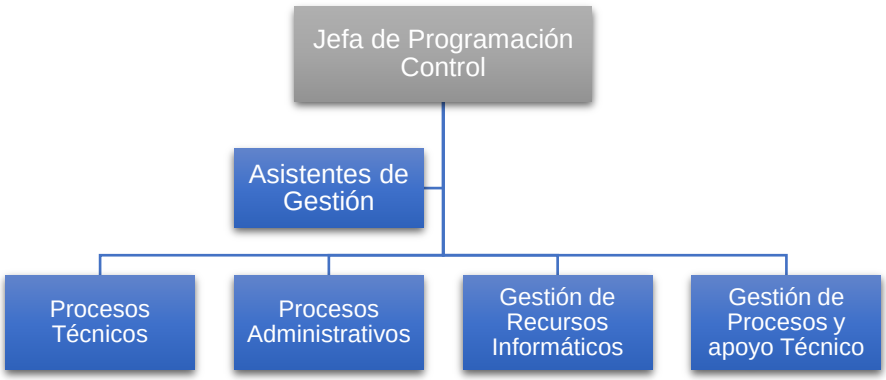
Tomado de Gerencia de Operación y Mantenimiento, 2016, P.17.

Anexo 4 Estructura Administración SCADA EMS



Tomado de Gerencia de Operación y Mantenimiento, 2016, P.22.

Anexo 5 Estructura Programación y Control



Tomado de Gerencia de Operación y Mantenimiento, 2016, P.5.

Anexo 6 Evaluación de nivel de capacidad 1 de procesos (1/3)

Katalina Coronel Hoyos
Gobierno, Riesgos y Cumplimiento de TI

EVALUACIÓN DEL NIVEL 1 DE CAPACIDAD DE PROCESOS
Metas, prácticas clave y productos de trabajo de los procesos

	Metas del proceso	Rating de evaluación de metas del proceso (15, 50, 85, 100)	Prácticas clave	Descripción de las Actividades	Rating de evaluación de prácticas clave (15, 50, 85, 100)	Productos (salidas)	Rating de evaluación de productos (15, 50, 85, 100)
Dominio:	**Evaluar, Dirigir y Monitorear**						
EDM03	**Asegurar la optimización de riesgos**	**26,67**			**15,00**		**26,67**
	1. Los umbrales de riesgo son definidos y comunicados y los riesgos clave relacionados con la TI son conocidos.	50	EDM03.01 Evaluar la gestión de riesgos.	Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.	15	- Guías de apetito de riesgo - Niveles de tolerancia de riesgo aprobados - Evaluación de las actividades de gestión de riesgo	50
	2. La empresa gestiona el riesgo crítico empresarial relacionado con las TI eficaz y eficientemente.	15	EDM03.02 Orientar la gestión de riesgos.	Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo.	15	- Políticas de gestión de riesgos - Objetivos claves a ser monitorizados por la gestión de riesgos - Proceso aprobado para la medición de la gestión de riesgos	15
	3. Los riesgos empresariales relacionados con las TI no exceden el apetito de riesgo y el impacto del riesgo TI en el valor de la empresa es identificado y gestionado.	15	EDM03.03 Supervisar la gestión de riesgos.	Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.	15	- Acciones correctivas para tratar las desviaciones en la gestión del riesgo - Problemas de la gestión de riesgos para la Dirección	15

Adaptado de Coronel, K. (s.f.). P.19.

Evaluación de nivel de capacidad 1 de procesos (2/3)

	Metas del proceso	Rating de evaluación de metas del proceso (15, 50, 85, 100)	Prácticas clave	Descripción de las Actividades	Rating de evaluación de prácticas clave (15, 50, 85, 100)	Productos (salidas)	Rating de evaluación de productos (15, 50, 85, 100)
APO12	**Administrar los Riesgos**	**23,75**			**26,67**		**15,00**
	1. El riesgo relacionado con TI está identificado, analizado, gestionado y reportado.	15	APO12.01 Recopilar datos.	Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.	50	- Datos en el entorno de operación relacionados con el riesgo - Datos en eventos de riesgo y en factores contribuyentes - Elementos y factores de riesgo emergentes	15
	2. Existe un perfil de riesgo actual y completo.	50	APO12.02 Analizar el riesgo.	Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.	15	- Alcance de los esfuerzos de análisis de riesgos - Escenarios de riesgo de TI - Resultados de análisis de riesgos	15
	3. Todas las acciones de gestión para los riesgos significativos están gestionadas y bajo control.	15	APO12.03 Mantener un perfil de riesgo.	Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.	15	- Escenarios de riesgo documentados por línea de negocio y función - Perfil de riesgo agregado, incluyendo el estado de las acciones de gestión del riesgo	15
	4. Las acciones de gestión de riesgos están efectivamente implementadas.	15	APO12.04 Expresar el riesgo.	Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.	15	- Análisis de riesgos e informes del perfil de riesgos para las partes interesadas - Revisión de resultados de evaluaciones de riesgos de terceras partes - Oportunidades para la aceptación de un riesgo mayor	15
			APO12.05 Definir un portafolio de acciones para la gestión de riesgos.	Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio	50	Propuestas de proyecto para reducir el riesgo	15
			APO12.06 Responder al riesgo.	Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.	15	- Planes de respuesta para incidentes relacionados con el riesgo - Comunicaciones del impacto del riesgo - Causas raíz relacionadas con el riesgo	15

Adaptado de Coronel, K. (s.f.). P.19.

Evaluación de nivel de capacidad 1 de procesos (3/3)

	Metas del proceso	Rating de evaluación de metas del proceso (15, 50, 85, 100)	Prácticas clave	Descripción de las Actividades	Rating de evaluación de prácticas clave (15, 50, 85, 100)	Productos (salidas)	Rating de evaluación de productos (15, 50, 85, 100)
DSS04	**Gestionar la continuidad**	**57,00**			**23,75**		**19,38**
	1. La información crítica para el negocio está disponible para el negocio en línea con los niveles de servicio mínimos requeridos.	85	DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance.	Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas.	15	- Política y objetivos de continuidad de negocio - Escenarios de incidentes que causan una interrupción - Valoraciones de las capacidades actuales y lagunas de continuidad	15
	2. Los servicios críticos tienen suficiente resilien	85	DSS04.02 Mantener una estrategia de continuidad.	Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.	15	- Análisis de impacto en el negocio - Requerimientos de continuidad - Opciones estratégicas aprobadas	15
	3. Las pruebas de continuidad del servicio han verificado la efectividad del plan.	85	DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.	Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas	15	- Acciones y comunicaciones de respuesta a incidentes - Plan de Continuidad de Negocio (BCP)	15
	4. Un plan de continuidad actualizado refleja los requisitos de negocio actuales.	15	DSS04.04 Ejercitar, probar y revisar el plan de continuidad.	Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.	15	- Pruebas de objetivos - Pruebas de ejercicios - Pruebas de resultados y recomendaciones	15
	5. Las partes interesadas internas y externas han sido formadas en el plan de continuidad.	15	DSS04.05 Revisar, mantener y mejorar el plan de continuidad.	Realizar una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio.	15	- Resultados de las revisiones de los planes - Cambios recomendados a los planes	15
			DSS04.06 Proporcionar formación en el plan de continuidad.	Proporcionar a todas las partes implicadas, internas y externas, de sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción.	15	- Requerimientos de formación - Resultados de la supervisión de habilidades y competencias	15
			DSS04.07 Gestionar acuerdos de respaldo.	Mantener la disponibilidad de la información crítica del negocio.	85	Probar los resultados de las copias de seguridad de los datos	50
			DSS04.08 Ejecutar revisiones post reanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.	15	- Informe de revisión postreanudación - Cambios aprobados a los planes	15

Adaptado de Coronel, K. (s.f.). P.19.

Anexo 7 Determinación de Contexto

Fecha:

Determinación de Contexto

Organización **Centro de Operación de Transmisión de CELEC EP**

Entorno externos	**Entorno**																					
Partes interesadas fuera de la organización	**Político**	Observaciones	**Legal**	Observaciones	**Reglamentario**	Observaciones	**R. Nacional**	Observaciones	**R. Internacional**	Observaciones	**R. regional / local**	Observaciones	**Social**	Observaciones	**Financiero**	Observaciones	**Tecnológico**	Observaciones	**Económico**	Observaciones	**Medios de comunicación**	Observaciones	**Otro**	Observaciones
#																								
Entorno Interno	**Entorno**																					
Partes interesadas dentro de la organización	**Secciones o Áreas de Transelectric**	Observaciones	**Políticas**	Observaciones	**Objetivos**	Observaciones	**Oportunidades futuras**	Observaciones	**Sistemas de Información**	Observaciones	**Flujos de información**	Observaciones	**Planes**	Observaciones	**Planes**	Observaciones								
#																								

Tomado de Talleres definición de Clientes Internos y Externos, 2017.

Anexo 8 Formulario de Identificación de Activos de Información.

INDENTIFICACIÓN ACTIVOS DE INFORMACIÓN

Inventario y clasificación de activos de información para cada área y/o procesos de apoyo de la Corporación.	
Fecha :	dd/mm/aaaa
Código:	SIC-MAT-ICA-001-2014 (ejemplo, por cada entrevista un número diferente)
Área:	
Unidad de Negocio:	
Proceso/Actividad:	
Nombre Entrevistado	

	PROPIEDAD					TIPO									VALORACIÓN				INFORMACIÓN ACTIVOS												
No ACTIVO	**Nombre Activo**	**Descripción del Activo**	**Custodio (Asignación de Inventario/dueño de aplicación)**	**Propietario (quien administra)**	**Responsable (quién aplica)**	Servicio	Datos e información	Aplicaciones de Software	Equipos informáticos	Redes de Comunicación	Soporte de la información	Equipamiento auxiliar	Instalaciones	Personal	Intangible	Confidencialidad	Integridad	Disponibilidad	Total Propiedades del Activo	**A1** ¿Este activo de información debe protegerse de ciudadanos, proveedores o	**A2** ¿El activo de información debe ser restringido a un número limitado de	**A3** ¿ El activo de información debe ser restringido a	**A4** ¿El activo de información ha sido declarado de conocimiento público, por la	**A5** ¿Al conocer el activo de información, una persona que no debe, causaría daño	**A6** ¿El activo de información puede ser alterado o	**A7** ¿Causaría perjuicio para la Corporación no saber	**A8** ¿Si el activo de información se encuentra dañado o	**A9** ¿Causaría daño no saber a quién se le ha asignado acceso al activo de	**A10** ¿Causaría daño al activo de información, no saber quién accede a qué datos y que	**A11** ¿El activo de información es muy crítico para las	**A12** ¿El activo de información es muy crítico para el servicio	**A13** ¿Si el activo de información queda inhabilitado, el tiempo de tolerancia para su funcionamiento nuevamente sería? (minutos, horas, semanas, meses)
																				CONFIDENCIALIDAD					**INTEGRIDAD**				**DISPONIBILIDAD**			
ACTINF - 001																															
ACTINF - 002																															

Inventario y clasificación de activos de información para cada área y/o procesos de apoyo de la Corporación.	
Fecha :	dd/mm/aaaa
Código:	SIC-MAT-ICA-001-2014 (ejemplo, por cada entrevista un número diferente)
Área:	
Unidad de	
Proceso/A	
Nombre	

	INFORMACIÓN ACTIVOS													
	A14			**A15**			**ACCESO**		**UBICACIÓN**					
No ACTIVO	**El Activo de información en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos estratégicos de la Corporación, de manera:**			Para acceder a estos datos, ¿dónde atacaría para robarlos (alterar, interrumpir)?	Para detener este servicio, ¿dónde atacaría para estropearlo?	Grado de Dependencia (%)	**Usuarios con acceso**	**Permisos de Acceso**	**Físico**	**Electrónico**	**Observaciones**	**Clasificación Final**	**Importancia del Activo**
	Leve	**Importante**	**Grave**										
ACTINF - 001														
ACTINF - 002														

Tomado de Talleres de Gestión de Riesgos COT, 2017.

Anexo 9 Formulario de Identificación de amenazas y vulnerabilidades

AMENAZAS Y VULNERABILIDAD

	Determinación de Amenazas y Vulnerabilidades de los activos de información ident
Fecha :	dd/mm/aaaa
Código:	
Área:	Administración SCADA EMS
Unidad de Negocio:	TRANSELECTRIC
Proceso/Actividad:	Operación del S.N.T.
Nombre Entrevistado	Ing. Luis Amores

Información Activo Identificado			Identificación de Amenazas/Vulnerabilidades			Riesgo Inherente			Controles Existentes		
No.	Activo de Información	PROCESO	Amenazas	Vulnerabilidad	Consecuencias	Probabilidad	Impacto	Criticidad Riesgo Inherente	Controles Implementados	Documentado	Tipo de control
1	Activo de Información										

Tomado de Talleres de Gestión de Riesgos COT, 2017.

Anexo 10 Formulario Manejo de Riesgos

AMENAZAS Y VULNERABILIDAD

Determinación de Amenazas y Vulnerabilidades de los activos de información ident	
Fecha :	dd/mm/aaaa
Código:	
Área:	Administración SCADA EMS
Unidad de Negocio:	TRANSELECTRIC
Proceso/Actividad:	Operación del S.N.T.
Nombre Entrevistado	Ing. Luis Amores

Información Activo Idertentes				Riesgo Residual			Tratamiento del Riesgo					
No.	Activo de Información	Documentado	Tipo de control	Probabilidad	Impacto	Criticidad Riesgo Residual	Decisión de Tratamiento	Acciones de Tratamiento	Responsable Análisis Causal	Areas que participan	Posibilidad De Aplicar Control (costo)	Indicador
1	Activo de Información											

Tomado de Talleres de Gestión de Riesgos COT, 2017.

Anexo 11 Formulario Identificación Recursos Estrategias Continuidad.

Recursos de las estrategias de continuidad

Fecha :	dd/mm/aaaa
Código:	
Área:	Centro de Operación de TRANSELECTRIC
Unidad de Negocio:	TRANSELECTRIC
Proceso/Actividad:	OPERAR EL SNT
Nombre Entrevistado	

Producto / Servicio:		1 D
Proceso:	**Nombre del Proceso**	1 D
Subproceso Seleccionado:		H

	Personas	Instalaciones	Tecnología	Información		Transporte	Finanzas	Proveedores	Suministros	Inventarios
				Impresa	Digital					
#										

Tomado de Talleres Definición de estrategias de Continuidad, 2017.

Anexo 12 Formulario Lista de verificación de controles.

Lista de Verificación de Controles

Nro. de Auditoría

Fecha **dd/mm/aaaa**

Norma de Ref

Nombre Audit

Proceso a Au TRANSELECTRIC

Clausula	Numero	Pregunta	Aplica No Aplica	Tipo de Evidencia	Responsable de suministrar evidencia	Método	Evidencia	Evidencia (adjuntar documento)	Evaluación					Descripción de Hallazgo	Recomendaciones	Calificación	Incumplen %	Cumplimiento por dominio %
									CFM	NCY (3 meses)	NCY (6 meses)	NCM	NCN					

Tomado de Talleres de Mejoras SGCN, 2017.

Anexo 13 Formulario de Mejoras de verificación de controles.

Tratamiento de Controles

Nro. de Auditoría
Fecha **dd/mm/aaaa**
Norma de Referencia _____
Nombre Auditor _____
Proceso a Auditar _____

#	CONTROLES	INDICADOR	ACCIÓN DE TRATAMIENTO	TIEMPO DE IMPLEMENTACIÓN	ESTADO DE LA ACCIÓN DE TRATAMIENTO	ACCIONES REALIZADAS	RESULTADOS DE LA ACCIÓN	OBSERVACIONES

Adaptado de Talleres de Gestión de Riesgos. 2017.