Departamento de Posgrados

Maestría en Auditoría Integral y Gestión de Riesgos Financieros

"Propuesta de Modelo de Gestión de Riesgos de Tecnologías de la Información en las empresas del sector público de Generación hidroeléctrica en la provincia del Azuay bajo la Norma ISO 9001-2015, periodo 2016 - 2017".

Caso de estudio: Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP

Título a obtener

Magíster en Auditoría Integral y Riesgos Financieros

Autor
María Isabel Carrillo Alvarado

Director
Javier Fabián Ordóñez Arízaga

Cuenca – Ecuador
2018

DECLARACIÓN EXPRESA

Las ideas, conceptos, procesos, procedimientos, análisis y resultados constantes en presente trabajo son de exclusiva responsabilidad de la autora.

Ing. María Isabel Carrillo Alvarado

DEDICATORIA

Para mi querida mami, “la abu Ceci”, mi ejemplo de mujer a seguir; para mi hermosa hija, Sofy, que es mi fuerza e inspiración; para mi esposo, Pablo, por su apoyo, amor y comprensión.

Para mis hermanos Sol, Omar y Christian, por su confianza y amor incondicional.

Para mi papi, que me acompaña siempre en mi corazón, seguramente se sentiría feliz con este logro.

AGRADECIMIENTO

A mis compañeros de trabajo, Daniela y Juan Carlos, que, sin duda alguna, colaboraron de manera incondicional para el desarrollo de este trabajo.

A mis compañeros de aula que hicieron de las clases un lugar de aprendizaje, diversión y solidaridad.

A mi director por sus valiosos aportes y dedicación para la culminación del presente.

RESUMEN

En el trabajo de investigación y modelo propuesto, se analizó con el apoyo de la Dirección de Gestión Estratégica, a la Corporación Eléctrica del Ecuador CELEC EP Hidropaute, mediante la identificación de los procesos que se ejecutan en la empresa y los riesgos asociados a estos procesos.

Se planteó conceptos relacionados con el riesgo, específicamente las normativas internacionales ISO 9001: 2015 e ISO 9001:31000.

Debido a que el objetivo del presente trabajo es proponer un modelo de gestión de riesgos de tecnologías de la información, el apartado que se utilizó de la normativa ISO 9001:2015, fue el de Planificación, porque aborda el riesgo y permite incorporar metodologías y procedimientos para gestionarlos.

La decisión de desarrollar un modelo bajo los principios y directrices de la normativa ISO 31000:2009, responde a que esta normativa es aplicable en cualquier ámbito, contexto, empresa y tipo de riesgo, lo que permitiría que el modelo propuesto se adapte sin problema alguno para la gestión de otro tipo de riesgos en la corporación.

Para identificar los riesgos y diseñar el formato de las diferentes fases del modelo de gestión de riesgos, se procedió con entrevistas a un grupo de personas consideradas expertos en los diferentes procesos de la empresa y que pertenecen al departamento de TI, que proporcionaron información respecto a la realidad de la empresa.

Finalmente, la aplicación del esquema metodológico para el desarrollo del modelo de gestión de riesgos, se realizó sobre la información obtenida, que además de permitir la determinación de cuáles son los controles y medidas de tratamiento apropiadas para el caso específico en estudio, proveyó información acerca de la falta de involucramiento de la alta gerencia en temas relacionados con el riesgo y en la necesidad de implementar un sistema de gestión integral de riesgos.

PALABRAS CLAVES

Riesgo, Gestión del riesgo, Normativa, Controles, Tecnología, Información

ABSTRACT

"Corporación Eléctrica del Ecuador CELEC EP Hidropaute" was analyzed in this research work by identifying the processes executed in the company and the risks associated with these processes. This work was developed with the support of the Strategic Management Department. The objective of this study was to propose a risk management model for information technologies. The section of the ISO 9001:2015 planning regulation was used. This addressed risks and allowed the incorporation of management methodologies and procedures. The principles and guidelines of the ISO 31000:2009 standard were considered in order to adapt the proposed model for the management of other types of risks in the corporation. Experts of the different processes of the company belonging to the IT department were interviewed to identify risks and design formats. These interviews provided information of the reality of the company. Finally, the methodological scheme was applied to develop the risk management model on the obtained information. This allowed the determination of controls and appropriate treatment measures for the specific case under study. Information was provided about the lack of involvement of senior management in matters related to risk and the need to implement a comprehensive risk management system.

Keywords: Risk, Risk management, Regulations, Controls, Technology, Information.

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by

Ing. Paul Arpi

ÍNDICE

INTRODUCCIÓN 12
Definición del problema 13
Idea a defender 14
Objetivos 14
- Objetivo General 14
- Objetivos Específicos 15

1. CAPITULO I: RESEÑA HISTÓRICA Y DIRECCIONAMIENTO ESTRATÉGICO DE LA EMPRESA 16
1.1. Reseña histórica 16
1.1.1. El sector de generación hidroeléctrica en la provincia del Azuay 16
1.1.1.1. Complejo Hidroeléctrico Paute Integral 16
1.1.1.2. Central Paute Molino 17
1.1.1.3. Central Paute Sopladora 17
1.1.1.4. Proyecto Paute Cardenillo 18
1.1.1.5. Proyecto Río Zamora – Santiago 19
1.2. Direccionamiento Estratégico de la Empresa 19
1.2.1. Misión 19
1.2.2. Visión 19
1.2.3. Políticas Institucionales 20
1.2.4. Principios y Valores 21
1.2.5. Objetivos Estratégicos y Estrategias 22
1.3. Especificación de procesos empresariales 24
1.3.1. Catálogo de Procesos 24
1.3.1.1. Macroprocesos Gobernantes: 24
1.3.1.2. Macroprocesos Agregadores de Valor: 25
1.3.1.3. Macroprocesos Habilitantes: 25
2. CAPÍTULO II: MARCO TEÓRICO Y LEGAL 26
2.1. Marco Teórico 26
2.1.1. Definición de Riesgo 26
2.1.2. Definición de Gestión de Riesgo 26
2.1.3. Definición de Gestión de Riesgos empresariales. 26
2.1.4. Marco de Gestión de Riesgos 26
2.1.5. Proceso de Gestión de Riesgos 27
2.1.6. Definición de riesgo de tecnología de la información 27
2.2. Marco Legal 27
2.2.1. Normativa Ecuatoriana a considerar 27
2.2.1.1. Constitución de la República del Ecuador 27

2.2.1.2. Ley Orgánica de Empresas Públicas LOEP. 28
2.2.1.3. Ley Orgánica de la Contraloría General del Estado 29
2.2.1.4. Normas de Control Interno – Contraloría General del Estado 29
2.2.1.5. NTE INEN-ISO 31000 Gestión del riesgo. Principios y directrices. Primera edición 2014 - 07 33
2.2.2. Normativa Internacional a considerar 33
2.2.2.1. ISO 9001-2015 33
2.2.2.2. ISO 31000: 2009 34
2.3. Similitudes y diferencias de las normativas ISO 9001: 2015 y 31000:2009 en aspectos relacionados con la Gestión del Riesgo. 35
2.3.1. Similitudes: 35
2.3.2. Diferencias: 35
2.4. Caso de aplicación: Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP 36
2.5. Metodología de la Investigación 37
2.5.1. Muestreo por Conveniencia 37
3. CAPITULO III: DIAGNÓSTICO DE LA EMPRESA Y ESTABLECIMIENTO DE ESQUEMA METODOLOGICO PARA DESARROLLO DE MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN 38
3.1. Diagnóstico de cumplimiento de Requisitos ISO 9001:2015 38
3.2. Mecanismos de Gestión de Riesgos asumidos por la alta dirección. 42
3.3. Esquema metodológico para el desarrollo del modelo de gestión de riesgos de tecnología de la información 45
3.3.1. Fases de desarrollo de la metodología 45
3.3.1.1. Fase 1: Determinación y descripción de procesos que se desarrollan en la corporación 45
3.3.1.2. Fase 2: Establecimiento del contexto 45
3.3.1.3. Fase 3: Identificación del Riesgo 46
3.3.1.4. Fase 4: Análisis de Riesgo 47
3.3.1.5. Fase 5. Evaluación del Riesgo 48
3.3.1.6. Fase 6. Valoración del Riesgo 50
3.3.1.7. Fase 7. Tratamiento del riesgo 53
3.3.1.8. Fase 8. Monitoreo y revisión 55
3.3.1.9. Fase 9. Comunicación y consulta. 56
4. CAPÍTULO IV: APLICACIÓN DEL ESQUEMA METODOLÓGICO PARA EL DESARROLLO DEL MODELO DE GESTION DE RIESGOS DE TECNOLOGIA DE LA INFORMACIÓN 58
4.1. Fase 1: Determinación y descripción de procesos que se desarrollan en la corporación 58
4.2. Fase 2. Establecimiento del contexto 60
4.3. Fase 3. Identificación de Riesgos 62

4.4. Fase 4. Análisis y Evaluación de los Riesgos Identificados. 62
4.5. Fase 5. Valoración de los Riesgos Identificados 63
4.6. Fase 6. Tratamiento de los Riesgos Identificados 63
4.7. Fase 7. Monitoreo y revisión 64
4.8. Fase 8. Comunicación y consulta 64
5. CONCLUSIÓN 66
6. REFERENCIAS BIBLIOGRÁFICAS 68

ÍNDICE DE TABLAS

TABLA 1. POLÍTICAS INSTITUCIONALES..... 20
TABLA 2. OBJETIVOS ESTRATÉGICOS Y ESTRATEGIAS 22
TABLA 3. ANÁLISIS DE CUMPLIMIENTO DEL SISTEMA DE GESTIÓN DE LA CALIDAD 38
TABLA 4. EVIDENCIA DE ESTABLECIMIENTO DE CONTROLES..... 42
TABLA 5. MATRIZ DE IDENTIFICACIÓN DE RIESGOS..... 47
TABLA 6. DETERMINACIÓN DE LA PROBABILIDAD 47
TABLA 7. DETERMINACIÓN DEL IMPACTO. 48
TABLA 8. MATRIZ DE EVALUACIÓN DEL RIESGO CUALITATIVO 49
TABLA 9. MATRIZ DE ANÁLISIS Y EVALUACIÓN DEL RIESGO 49
TABLA 10. FACTORES PARA VALORACIÓN DEL RIESGO 50
TABLA 11. TIPO DE CONTROL..... 51
TABLA 12. PERIODICIDAD DE CONTROL 51
TABLA 13. EFICACIA DE CONTROL 52
TABLA 14. NIVEL DE RIESGO RESIDUAL 53
TABLA 15. TRATAMIENTO DEL RIESGO..... 53
TABLA 16. MATRIZ MEDIDAS DE TRATAMIENTO DEL RIESGO..... 54
TABLA 17. MONITOREO Y REVISIÓN..... 56
TABLA 18. COMUNICACIÓN Y CONSULTA..... 57

ÍNDICE DE ILUSTRACIONES

ILUSTRACIÓN 1. CADENA DE VALOR DE CELEC EP 24
ILUSTRACIÓN 2. PILARES BÁSICOS DE ISO 31000:2009 34

ÍNDICE DE ANEXOS

ANEXO 1. IDENTIFICACIÓN DEL RIESGO 71
ANEXO 2. ANÁLISIS Y EVALUACIÓN DEL RIESGO 76
ANEXO 3. VALORACIÓN Y EVALUACIÓN DE LOS RIESGOS 79
ANEXO 4. TRATAMIENTO DE LOS RIESGOS 83
ANEXO 5. MONITOREO Y REVISIÓN 87

INTRODUCCIÓN

El sector eléctrico en el Ecuador, ha crecido considerablemente durante los últimos años, esto, en función de los datos proporcionados por el Ministerio de Electricidad y Energía Renovable, que, en su Rendición de Cuentas del 2015, argumentó que la capacidad instalada en generación eléctrica pasó de 4070 MW a 6010 MW, desde 2006 a 2015; y, con la operación plena de las 8 centrales hidroeléctricas, esa capacidad aumentará a 8569 MW en 2017. En la provincia del Azuay, la generación hidroeléctrica juega un papel muy importante, pues proyectos y centrales representativas a nivel nacional, se ubican en esta provincia; tal como es el caso de la Central Hidroeléctrica Sopladora, inaugurada en agosto del 2016, cuya potencia es de 487 MW.

Para llevar a cabo el cumplimiento de los objetivos y razón de ser de las empresas dedicadas a esta actividad, el uso de las tecnologías de información es primordial, desde el nivel administrativo, hasta el nivel técnico.

El talento humano, encargado de llevar a cabo estas actividades, requiere apoyarse del recurso tecnológico, debido a que el uso de la tecnología en las empresas, favorece el incremento de la productividad y la competitividad; sin embargo, este uso expone a la empresa a diversos riesgos de tipo tecnológico.

Como definición del riesgo, se tiene que es el efecto de la incertidumbre sobre los objetivos. El riesgo se mide en términos de impacto y probabilidad. (ISO, 31000: 2009)

El no contar con un sistema de gestión de riesgos de tecnologías de la información en las empresas de este tipo, podría desencadenar problemas graves que impacten a nivel económico y financiero a la entidad, como por ejemplo la falla de un sistema industrial asociado a la generación de energía, provocaría el desabastecimiento de energía al país, pérdidas económicas, y a la disponibilidad, confiabilidad y resiliencia de los sistemas de generación/transporte de energía eléctrica y de telecomunicaciones de acuerdo a la normativa y estándares internacionales.

En la actualidad, la Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP Unidad de Negocio Hidropaute, cuenta con una certificación en la norma ISO 9001-2008, por lo que, en función de este aspecto, la empresa deberá realizar la transición a ISO 9001:2015.

El trabajo a desarrollarse se enfocará en el apartado número **6, Planificación**, de la norma ISO 9001:2015[1], que aborda la gestión de riesgos y está orientado hacia un enfoque preventivo que se acentúa con los aspectos referidos a la Gestión del Riesgo, que consiste en reconocer los riesgos dentro de una organización y llevar a cabo las actuaciones

[1] ISO 9001:2015, Sistemas de Gestión de la Calidad, Requisitos

necesarias para evitar que se produzcan. Plantea, además, la inclusión de métodos o procedimientos para la evaluación, administración, eliminación y/o minimización de los riesgos.

Para la gestión de riesgos, ISO 9001:2015, recomienda que para que los métodos o procedimientos para la evaluación, administración, eliminación y/o minimización de los riesgos, sean efectivos, se debe tomar como guía los principios básicos que establece la Norma ISO 31000, que es una norma internacional que proporciona principios y directrices de carácter genérico sobre la gestión de riesgos[2].

El tratamiento de los riesgos y la consideración de los mismos en todo el sistema de gestión de la calidad, es un factor clave para la toma de decisiones y diseño de estrategias que se ajusten a las necesidades de la organización, pues permite a la alta dirección llevar un registro, medir y controlar todos aquellos eventos que se susciten y que impacten a las operaciones. Un factor a considerar es que no todas las empresas presentan el mismo tipo de riesgos de tecnologías de la información, pues lo que es un punto fuerte en una empresa del sector comercial, podría representar un punto débil en una empresa del sector de energía; por lo que, el presente trabajo de tesis pretende proporcionar una metodología de gestión de riesgos de tecnologías de la información, que se fundamente y guíe por el esquema de la normativa internacional ISO 9001:2015 (apartado 6), para una empresa del sector de generación hidroeléctrica, específicamente CELEC EP Hidropaute.

Definición del problema

La Empresa Pública Corporación Eléctrica del Ecuador CELEC EP, específicamente la Unidad de Negocio CELEC EP Hidropaute, actualmente cuenta con un sistema de gestión de calidad basado en la norma ISO 9001:2008; sin embargo, no se ha dado la importancia debida a la tecnología de la información, ni a la gestión de riesgos.

Al estar, la tecnología de la información, presente en las actividades estratégicas, es esencial que existan controles y procedimientos a seguir para mitigar o aprovechar los efectos derivados de la ocurrencia de un evento de riesgo, ya que al suscitarse un evento negativo podría ocasionar graves daños económicos y de desarrollo de las actividades propias del negocio; lo que deriva en desabastecimiento del suministro de energía en el país y por ende repercusiones a nivel financiero, pues es alta la cantidad de recursos destinados a TICS dentro de la empresa.

[2] ISO 31000:2009, Principios y Directrices para la Gestión de Riesgos

Idea a defender

Los sistemas de gestión de la calidad ISO 9001:2015, incluyen en la actualización la gestión de riesgos en sus procesos, para lo cual recomienda que los métodos y procedimientos que se utilicen para la gestión de riesgos, tomen como guía a los principios establecidos en ISO 31000:2009.

La norma ISO 9001:2015, no es rígida respecto a qué metodología utilizar de manera formal para la gestión de riesgos; es por ello, que el modelo que se propondrá tendrá como base la norma ISO 31000:2009, ya que esta permite gestionar riesgos de manera sistemática, transparente, creíble y dentro de cualquier ámbito y contexto, para el caso de aplicación, concretamente aquellos relacionados con la tecnología de la información, que, aunque está presente en todos los procesos de la empresa, no ha sido considerada como corresponde, exponiendo a la empresa a ser blanco de ataques, sobre todo en aquellos procesos estratégicos y actividades que conforman el Core Business.

Preguntas directrices

- ✓ ¿Es importante para la empresa el tratamiento de riesgos en cada una de las etapas del proceso de gestión de la calidad?
- ✓ ¿Se considera que la identificación y mitigación de riesgos tecnológicos constituye un gasto para la empresa?
- ✓ ¿Cuáles son los principales beneficios del tratamiento de los riesgos tecnológicos en la organización de acuerdo a ISO 9001:2015?
- ✓ ¿Cuáles son las medidas o estrategias a implementar a fin de gestionar los riesgos en una empresa?
- ✓ ¿Cuál es la relación existente entre las normas ISO y las metodologías expuestas en lo que comprende la gestión de riesgos?

Objetivos

- **Objetivo General**

Proponer un modelo de gestión de riesgos de tecnología de la información, basado en la norma ISO 9001:2015, para el tratamiento de una empresa del sector público hidroeléctrico.

- **Objetivos Específicos**

- ✓ Fundamentar teóricamente la gestión de riesgo tecnológico bajo la normativa ISO 9001:2015, y su congruencia con las normativas de general aceptación y la legal vigente en el Ecuador.
- ✓ Identificar los procesos críticos empresariales, los modelos comportamentales de gestión de riesgos asumidos por la alta dirección, y su interrelación con el uso de las tecnologías de la información, determinando aquellos en que se generan niveles de riesgo significativo, para su eventual tratamiento preventivo y correctivo.
- ✓ Evaluar los mecanismos de gestión de riesgo de acuerdo a los modelos y metodologías vigentes y recomendadas para la situación particular planteada.
- ✓ Proponer medidas para el tratamiento de riesgos tecnológicos en las empresas hidroeléctricas de la Provincia del Azuay, bajo la norma ISO 9001:2015 en el periodo 2016-2017.

1. CAPITULO I: RESEÑA HISTÓRICA Y DIRECCIONAMIENTO ESTRATÉGICO DE LA EMPRESA

1.1. Reseña histórica

1.1.1. El sector de generación hidroeléctrica en la provincia del Azuay

1.1.1.1. Complejo Hidroeléctrico Paute Integral

En las provincias del Azuay, Cañar y Morona Santiago se desarrolla el Complejo Hidroeléctrico Paute Integral, conformado por Mazar, Molino, Sopladora y Cardenillo, cuatro centrales en cascada que aprovecharán el agua de la cuenca del río Paute para generar energía limpia y así contribuir al cambio de la matriz energética del Ecuador.

La Unidad de Negocio HIDROPAUTE, parte de la Corporación Eléctrica del Ecuador CELEC EP es la encargada de la operación y mantenimiento, construcción y administración del Complejo Hidroeléctrico más importante del Ecuador. [3]

Central Paute Mazar

El ingeniero Daniel Palacios Izquierdo fue el visionario del accidente topográfico de la Cola de San Pablo, quien en 1961 presenta un informe de los resultados de sus observaciones en Amaluza, a cerca del desnivel del río Paute y propone un túnel para llevar sus aguas hacia una casa de máquinas donde se genere energía hidroeléctrica. En ese mismo año se creó el INECEL e iniciaron las gestiones en torno al proyecto Paute.

En 1964 se contrataron los estudios del desarrollo hidroeléctrico de la Cola de San Pablo y en 1976 se firman los contratos para la construcción de la Fase AB de la central Paute Molino; iniciándose así la construcción del Complejo Hidroeléctrico.

Luego de varios años de espera, en marzo de 2005, se inicia la construcción del proyecto hidroeléctrico Mazar, ubicado en las inmediaciones de la desembocadura del río Mazar. Está constituida por una presa de enrocado con pantalla de hormigón de 166 metros de altura, forma un embalse de 394 hm3 de volumen total y una central subterránea a pie de presa, con

[3] Sitio web Empresa Pública Estratégica CELEC EP Hidropaute: https://www.celec.gob.ec/hidropaute/perfil-corporativo/paute-integral.html

dos turbinas tipo francis, generando desde diciembre de 2010, 85 MW cada una; aportando con aproximadamente 800 GWh/año al Sistema Nacional Interconectado (SNI). La característica principal de Mazar es su gran embalse que permite una mayor regulación del caudal del río Paute, incrementa la energía firme en la central Molino, y además, retiene los materiales sólidos que arrastra el río, contribuyendo a la continuidad operativa del embalse Amaluza.

1.1.1.2. Central Paute Molino

La central más grande del Ecuador, conocida comúnmente como Cola de San Pablo. Fue construida en dos etapas, la primera “Fase AB” entró en operación en 1983 y la “Fase C” en 1991. Genera anualmente 4900 GWh, actualmente, el 35% de la demanda de energía eléctrica del país.

La central Molino está compuesta por la presa Daniel Palacios, que es de tipo arco gravedad y tiene una altura de 170 m, posteriormente, a 8 km en línea recta se encuentra la casa de máquinas en caverna que alberga 10 unidades generadoras tipo Pelton, diseñadas para un caudal de 200 m3/s.

1.1.1.3. Central Paute Sopladora

La Central Hidroeléctrica Sopladora de 487 MW de potencia es la tercera central del Complejo Hidroeléctrico del Río Paute, capta las aguas turbinadas de la Central Molino. La Central se encuentra ubicado en el límite provincial de Azuay y Morona Santiago, cantones Sevilla de Oro y Santiago de Méndez.

Formó parte de las ocho centrales hidroeléctricas que construye el Gobierno de la Revolución Ciudadana, primordiales para el cambio de la Matriz Energética, objetivo fundamental para el desarrollo sustentable del país.

La Central Hidroeléctrica, fue inaugurada el 25 de agosto de 2016 ante la presencia del Señor Presidente de la República del Ecuador. Ha aportado al S.N.I. una energía neta de 2.098.27 GWh desde abril de 2016 hasta junio de 2017.

Conformada por una conexión directa entre los túneles de descarga de la Central Molino y el sistema de carga de la Central Sopladora. La conexión directa consta de un túnel de derivación de flujo que comunica con dos túneles de descarga hacia una cámara de

interconexión subterránea que proveerá el volumen necesario para garantizar el ingreso de 150 m3/seg para el funcionamiento del sistema de generación que consta de tres 3 turbinas Francis de 165.24 MW, alojadas en la casa de máquinas subterránea.

Central Emblemática del estado ecuatoriano, que apoyará en la búsqueda de autonomía energética, remplazando la generación térmica, reduciendo emisiones de CO_2 en aproximadamente 1.09 millones de Ton/año, sustituyendo la importación de energía; durante la fase de construcción, ha generado 3258 fuentes de empleo directo, beneficiando a 16 millones de ecuatorianos.

Durante su construcción 15 mil habitantes de la zona de influencia del proyecto, se beneficiaron mediante la implementación de nuevas prácticas de compensación a través de programas de desarrollo integral y sostenible se implementaron proyectos en Conservación Ambiental que fomenta medidas de adaptación al Cambio Climático, construcción y adecuación de infraestructura educativa; proyectos en infraestructura y vialidad; mejoramiento y equipamiento de centros de salud, construcción y mejoramiento de sistemas de agua potable y saneamiento, fortalecimiento de capacidades agropecuarias y capacitación en atención a turistas, obras ejecutadas por medio de la CELEC EP Unidad de Negocio HIDROPAUTE.

Adicionalmente se han realizado inversiones en la construcción y adecuación de las vías Sevilla de Oro – San Pablo, San Pablo – Quebrada Guayaquil y Guarumales Méndez.

1.1.1.4. Proyecto Paute Cardenillo

ARCONEL, dentro de las funciones establecidas en la Ley de Régimen del Sector Eléctrico, evalúa el comportamiento de la oferta y la demanda de potencia y energía eléctrica, para lo cual actualizó el Plan Maestro de Electrificación para el periodo 2009-2020, mismo que contempla la entrada en operación del Proyecto Hidroeléctrico Paute-Cardenillo, siendo declarado por el Gobierno Ecuatoriano como proyecto prioritario.

El Plan se fundamenta en el uso de energías renovables, como principal alternativa sostenible en el largo plazo, y contempla la ejecución de medianos y grandes proyectos de generación hidroeléctrica, en virtud de lo anterior, en diciembre del año 2010, la Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP por medio de la Unidad de Negocio HIDROPAUTE, suscribió el contrato para la prestación de los servicios de consultoría para la elaboración de los diseños de Prefactibilidad, Factibilidad y Diseño Definitivo para la licitación de la construcción del proyecto hidroeléctrico Paute-Cardenillo.

El proyecto Hidroeléctrico Paute-Cardenillo constituye el escalón final del desarrollo integral de la cuenca media del río Paute, conjuntamente con los proyectos Paute-Mazar, Paute- Molino, y Paute-Sopladora.

La cuarta etapa del aprovechamiento, es el proyecto Paute-Cardenillo, que tendrá una capacidad instalada de 595,65 MW para un caudal de diseño de 180m3/s tomados de las aguas turbinadas de la descarga del proyecto Paute-Sopladora (150m3/s) más las aguas correspondientes a la cuenca intermedia (30 m3/s).

1.1.1.5. Proyecto Río Zamora – Santiago

Por disposición del Ministerio de Electricidad y Energía Renovable, desde el 22 de noviembre de 2011, la Corporación Eléctrica del Ecuador CELEC EP es la encargada del desarrollo del complejo hidroeléctrico del rio Zamora, curso inferior.

La Corporación Eléctrica del Ecuador CELEC EP el 29 de noviembre de 2011, la Gerencia General de CELEC EP delega a la Unidad de Negocio HIDROPAUTE la ejecución de los estudios para el aprovechamiento del potencial hidroeléctrico del Río Zamora.

1.2. Direccionamiento Estratégico de la Empresa

1.2.1. Misión

CELEC EP es una Corporación que focaliza sus actividades en el ámbito de Generación, Transporte de Energía Eléctrica en alta tensión, y al Desarrollo de Nuevos Negocios y Servicios relacionados que contribuyan al interés público y al desarrollo del Ecuador, a través de un modelo de gestión sostenible basado en la eficiencia y viabilidad económica de sus operaciones, responsabilidad social y ambiental y en la innovación.[4]

1.2.2. Visión

Para el año 2021, CELEC EP será un referente mundial, por su componente de provisión de energía limpia altamente confiable; y a nivel nacional, por su posicionamiento empresarial de cercanía a la sociedad y de aporte de nuevos líderes al sector eléctrico. Su modelo de

[4] Sitio web CELEC EP: https://www.celec.gob.ec/hidropaute/perfil-corporativo/filosofia-corporativa.html

gestión estará basado en capacidades empresariales y en la incorporación y convergencia de tecnologías.

1.2.3. Políticas Institucionales

Tabla 1. Políticas Institucionales

ÁMBITO	POLÍTICAS
RESPONSABILIDAD SOCIAL	Minimización de los impactos socio-ambientales, armonizando las operaciones de la Empresa con las expectativas nuestros usuarios y de la comunidad en general, cumpliendo con el marco legal y normativo vigente.
CLIENTES - USUARIOS	Compromiso con la satisfacción y superación de las expectativas de nuestros clientes, a través del cumplimiento y mejora continua de los índices de calidad y costo del servicio entregado.
RIESGOS	Compromiso con la identificación oportuna y manejo correcto del riesgo, para minimizar sus impactos y consecuencias sobre las personas, la comunidad, el ambiente, los activos y los procesos de la Corporación.
PROYECTOS	Fomento de la eficaz y eficiente ejecución de proyectos, buscando incrementar la oferta energética basada en energías renovables, ampliando la cobertura del servicio eléctrico.
SOBERANÍA ELÉCTRICA	Impulso de la autosustentabilidad en la generación eléctrica, con el propósito de abastecer la demanda, eliminando la dependencia en el abastecimiento de energía eléctrica por otros países.
FINANCIERA	Asignación de los recursos financieros, a las unidades de negocio y matriz, en base a las prioridades establecidas a nivel Corporativo.
RECURSOS HUMANOS	Reconocimiento del talento humano como el principal activo de la Corporación, priorizando su desarrollarlo, pertenencia y compromiso bajo un ambiente favorable y de respeto.

NORMATIVA	Aplicación permanente de los principios, estrategias, políticas y procedimientos internos, enfocados en los resultados, bajo una cultura de medición, evaluación y rendición de cuentas.
COMUNICACIÓN	Fomento de una comunicación dinámica, ágil, oportuna, responsable y participativa al interior y al exterior de la organización, desarrollando un lenguaje común y canales de comunicación claros y precisos.
INFORMACIÓN	Compromiso con la administración y protección de la información, considerándola como un activo estratégico, normando su acceso interno y público.
GESTIÓN	Impulso del mejoramiento continuo de la gestión empresarial, incorporando constantemente las mejores prácticas y tecnologías de apoyo y desarrollando la innovación e investigación.
TECNOLOGÍA	incorporación permanente, oportuna y eficiente de innovaciones tecnológicas que aporten a la mejora del servicio y gestión de la organización.
ADQUISICIONES	Compromiso con la adquisición ágil, transparente y oportuna de los bienes y servicios requeridos para el desarrollo de las actividades de la Corporación, precautelando los intereses de la organización, el Estado y la Comunidad.
CONOCIMIENTO	Compromiso con la generación, aprovechamiento, cuidado, difusión e institucionalización del conocimiento en la organización.

Fuente: Corporación Eléctrica del Ecuador

Elaborado por: María Isabel Carrillo

1.2.4. Principios y Valores

- Compromiso
- Trabajo en equipo
- Integridad
- Responsabilidad Socio-ambiental

- Pasión por la excelencia

1.2.5. Objetivos Estratégicos y Estrategias

Tabla 2. Objetivos Estratégicos y Estrategias

OBJETIVOS	ESTRATEGIAS
Mantener la disponibilidad, confiabilidad y resiliencia de los sistemas de generación/transporte de energía eléctrica y de telecomunicaciones de acuerdo a la normativa y estándares internacionales.	Implementar una plataforma de inteligencia operacional de la infraestructura eléctrica. Formular e implementar un plan estratégico de gestión de mantenimiento corporativo. Formular e implementar un modelo de gestión de activos en la Corporación. Fortalecer la capacidad de gestión de protecciones y mecanismos inteligentes asociados. Fortalecimiento de la red eléctrica y de los servicios de telecomunicaciones. Institucionalizar la organización y el desempeño de Comités Técnicos Implementar un Plan Integral de Gestión de Riesgos y Continuidad de las Operaciones, en coordinación con el MEER. Establecer la función de ciberseguridad
Incrementar la oferta de generación y transporte de energía eléctrica en concordancia con el Plan Maestro de Electricidad y las políticas sectoriales.	Culminar con la ejecución de los proyectos de generación y trasmisión. Ejecutar los estudios de prospección de nuevos proyectos según directrices del MEER. Ejecutar nuevos proyectos de expansión en generación y transmisión en cumplimiento del PME y directrices del MEER. Participar en el proceso de planificación de la expansión de generación y transmisión con el MEER y planificar el desarrollo de la red y servicios de telecomunicaciones.
Incrementar la sostenibilidad financiera de la Corporación	Desplegar homologación NIIF incluyendo activación de nueva infraestructura de proyectos Expansión de servicios y nuevos negocios. Desplegar un modelo eficiencia financiera y costeo para las Unidades de Negocio. Fortalecer el negocio de Telecomunicaciones.
	Formular y desplegar la nueva estructura organizacional de toda la Corporación.

OBJETIVOS	ESTRATEGIAS
Incrementar la eficiencia y eficacia institucional.	Implementar un modelo de gestión de datos e información para toma de decisiones corporativas Establecer la capacidad de gestión por procesos. Establecer un plan estratégico de capacitación Establecer un plan de formación de personal para altos potenciales con una visión global de la industria eléctrica. Establecer un plan estratégico de tecnologías IT/OT. Formular e implementar la gestión de portafolios, programas y proyectos basadas en buenas prácticas internacionales Modernizar la plataforma informática de soporte a procesos administrativos y técnicos, con una visión integrada. Fortalecer la capacidad de estudios y análisis comercial.
Incrementar el posicionamiento y el aporte directo en la generación de valor a la sociedad	Fortalecer la capacidad de gestión comunicacional y de relacionamiento externo. Establecer la capacidad de responsabilidad social corporativa y ambiental.
Mantener vigente y ejecutar un plan de transformación digital de la Corporación.	Disponer de un plan estratégico de Smart Grids con una visión colaborativa de otros actores. (Comité REDIE). Establecer en forma programática espacios de análisis de los temas estratégicos de la Transformación digital

Fuente: Corporación Eléctrica del Ecuador

Elaborado por: María Isabel Carrillo

En la actualidad el sistema de gestión de la calidad que mantiene la organización está basado en ISO 9001:2008; mismo que terminó su vigencia el 30 de septiembre del 2017; por lo tanto, es necesario que la empresa empiece su proceso de certificación en ISO 9001:2015.

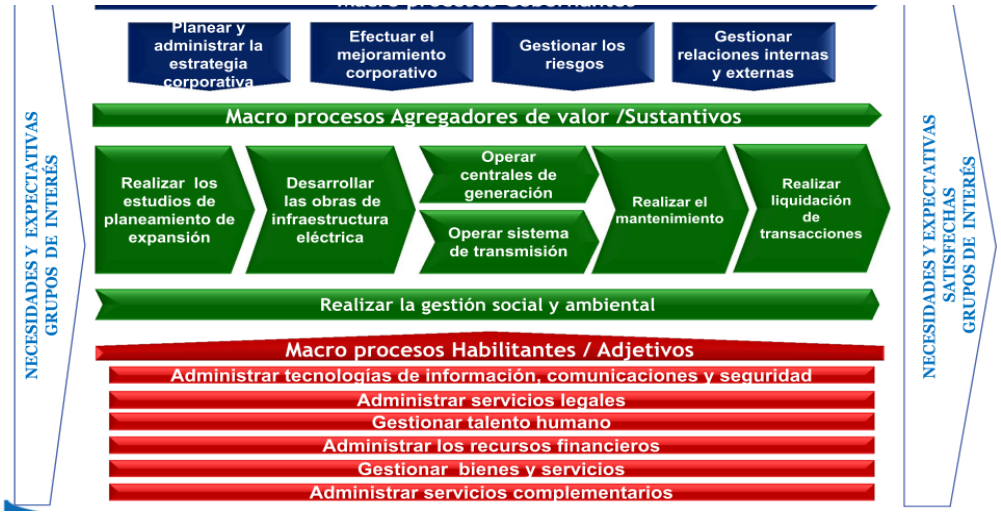
Respecto a la gestión de riesgos, para que la consecución de los objetivos estratégicos se alcance, se deben considerar los riesgos que estarían asociados a las actividades que se desarrollen dentro de la implementación de estrategias.

Los procesos corporativos deben tener como meta contribuir a la consecución de los objetivos estratégicos, por lo que la identificación de riesgos y gestión de éstos es fundamental.

1.3. Especificación de procesos empresariales

Para mayor comprensión del funcionamiento de la Empresa Pública Estratégica CORPORACIÓN ELÉCTRICA DEL ECUADOR CELEC EP, se presenta una visión general del sistema de gestión institucional, mediante la representación gráfica de la Cadena de Valor.

Ilustración 1. Cadena de Valor de CELEC EP



Fuente: Corporación Eléctrica del Ecuador CELEC EP

Elaborado por: Dirección de Gestión Estratégica

A continuación, una breve descripción de los procesos que conforman el sistema de gestión institucional de CELEC EP.

1.3.1. Catálogo de Procesos

1.3.1.1. Macroprocesos Gobernantes:

Se considerarán a aquellos que proporcionan directrices a los demás procesos y son realizados por el Directorio u organismo que haga sus veces y por la Gerencia General para poder cumplir con los objetivos y políticas institucionales.

1.3.1.2. Macroprocesos Agregadores de Valor:

Son los procesos esenciales de la Corporación, a través de los cuales se generan y administran los productos y servicios destinados a usuarios externos, garantizando el cumplimiento de la misión organizacional.

1.3.1.3. Macroprocesos Habilitantes:

Son aquellos que asesoran a los procesos gobernantes y agregadores de valor; son los responsables de brindar productos de asesoría y apoyo logístico para generar el portafolio de productos de la CELEC EP. Dan soporte a los procesos gobernantes y agregadores de valor, se encargan de proporcionar personal competente, reducir los riesgos del trabajo, preservar la calidad de los materiales, equipos y herramientas, mantener las condiciones de operatividad y funcionamiento coordinar y controlar la eficacia del desempeño administrativo v la optimización de los recursos.

2. CAPÍTULO II: MARCO TEÓRICO Y LEGAL

2.1. Marco Teórico

2.1.1. Definición de Riesgo

Un Riesgo es el efecto de la incertidumbre sobre los objetivos. (ISO, 31000: 2009)

El riesgo se puede definir como la combinación de la probabilidad de un suceso y sus consecuencias. En todos los tipos de empresa existe un potencial de sucesos y consecuencias que constituyen oportunidades para conseguir beneficios (lado positivo) o amenazas para el éxito (lado negativo). Se reconoce cada vez más que la gestión de riesgos trata tanto los aspectos positivos como los negativos de los riesgos; por lo tanto, los presentes estándares consideran el riesgo desde ambas perspectivas. En el campo de la seguridad, se suele admitir que las consecuencias son solo negativas, por lo que la gestión de riesgos de seguridad se centra en la prevención y en la mitigación del daño. (Baena-López, 2009)

2.1.2. Definición de Gestión de Riesgo

Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo. (ISO, 31000: 2009)

Son las actividades coordinadas para dirigir y controlar una empresa en relación con el riesgo e incluye, por norma general, la evaluación, el tratamiento, la aceptación y la comunicación de los riesgos. (Casares-San José, 2013)

2.1.3. Definición de Gestión de Riesgos empresariales.

Capacidad de una organización de entender, controlar y articular la naturaleza y nivel de los riesgos tomados en la búsqueda de una rentabilidad ajustada al riesgo. (ISO, 31000: 2009).

2.1.4. Marco de Gestión de Riesgos

Conjunto de componentes que proporcionan las bases y modalidades de organización para diseñar, implementar, controlar, la revisión y mejora continua de la gestión del riesgo en toda la organización. (ISO, 31000: 2009)

2.1.5. Proceso de Gestión de Riesgos

La aplicación sistemática de políticas de gestión, procedimientos y prácticas para las actividades de comunicación, consultoría, se establece el contexto, y la identificación, análisis, evaluación, tratamiento, seguimiento y la revisión de riesgo. (ISO, 31000: 2009)

2.1.6. Definición de riesgo de tecnología de la información

El concepto de riesgo de TI puede definirse como el efecto de una causa, multiplicado por la frecuencia probable de ocurrencia dentro del entorno de TI. Surge así entonces, la necesidad de que el control actúe sobre la causa del riesgo para minimizar sus efectos. Cuando se dice que los controles minimizan los riesgos, lo que en verdad hacen, es actuar sobre las causas de los riesgos, para minimizar sus efectos. (Piattini y Del Peso, 2004)

El riesgo de TI, es el riesgo de negocio asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de la TI, dentro de la empresa. Este riesgo consiste en los eventos relacionados con la TI, que pueden potencialmente impactar al negocio, cada evento puede ser visto como Riesgo y Oportunidad. (AEC, 2017)

2.2. Marco Legal

2.2.1. Normativa Ecuatoriana a considerar

2.2.1.1. Constitución de la República del Ecuador

La Constitución de la República del Ecuador, en los artículos 389 y 390, aborda el riesgo con la finalidad de que las empresas públicas y privadas cuenten con un sistema de gestión de riesgos, especificando lo siguiente:

Art. 389.- (…) El sistema nacional descentralizado de gestión de riesgo está compuesto por las unidades de gestión de riesgo de todas las instituciones públicas y privadas en los ámbitos local, regional y nacional. El Estado ejercerá la rectoría a través del organismo técnico establecido en la ley. Tendrá como funciones principales, entre otras:

Identificar los riesgos existentes y potenciales, internos y externos que afecten al territorio ecuatoriano.

Generar, democratizar el acceso y difundir información suficiente y oportuna para gestionar adecuadamente el riesgo.

Asegurar que todas las instituciones públicas y privadas incorporen obligatoriamente, y en forma transversal, la gestión de riesgo en su planificación y gestión.

Fortalecer en la ciudadanía y en las entidades públicas y privadas capacidades para identificar los riesgos inherentes a sus respectivos ámbitos de acción, informar sobre ellos, e incorporar acciones tendientes a reducirlos.

Articular las instituciones para que coordinen acciones a fin de prevenir y mitigar los riesgos, así como para enfrentarlos, recuperar y mejorar las condiciones anteriores a la ocurrencia de una emergencia o desastre.

Realizar y coordinar las acciones necesarias para reducir vulnerabilidades y prevenir, mitigar, atender y recuperar eventuales efectos negativos derivados de desastres o emergencias en el territorio nacional.

Garantizar financiamiento suficiente y oportuno para el funcionamiento del Sistema, y coordinar la cooperación internacional dirigida a la gestión de riesgo. (Asamblea Nacional Constituyente de Ecuador , 2008)

Art. 390.- Los riesgos se gestionarán bajo el principio de descentralización subsidiaria, que implicará la responsabilidad directa de las instituciones dentro de su ámbito geográfico. Cuando sus capacidades para la gestión del riesgo sean insuficientes, las instancias de mayor ámbito territorial y mayor capacidad técnica y financiera brindarán el apoyo necesario con respeto a su autoridad en el territorio y sin relevarlos de su responsabilidad. (Asamblea Nacional Constituyente de Ecuador , 2008)

2.2.1.2. Ley Orgánica de Empresas Públicas LOEP.

La Ley Orgánica de Empresas Públicas, en los numerales 2 y 4, en su artículo 11, establece lo siguiente:

Art. 11.- DEBERES Y ATRIBUCIONES DEL GERENTE GENERAL. - El Gerente General, como responsable de la administración y gestión de la empresa pública, tendrá los siguientes deberes y Atribuciones:

2. Cumplir y hacer cumplir la ley, reglamentos y demás normativa aplicable, incluidas las resoluciones emitidas por el Directorio;

4. Administrar la empresa pública, velar por su eficiencia empresarial e informar al Directorio trimestralmente o cuando sea solicitado por éste, sobre los resultados de la gestión de aplicación de las políticas y de los resultados de los planes, proyectos y presupuestos, en ejecución o ya ejecutados. (Asamblea Nacional, 2009)

Respecto a la LOEP y su relación con la gestión de riesgos, el Gerente General es el encargado de que se cumplan las leyes, reglamentos y demás normativa aplicable a la entidad; por lo tanto, la normativa relacionada con riesgos debe ser aplicada en la corporación y será el Gerente General el responsable de implementar metodologías para ello.

2.2.1.3. Ley Orgánica de la Contraloría General del Estado

Art. 9.- Concepto y elementos del Control Interno. - El control interno constituye un proceso aplicado por la máxima autoridad, la dirección y el personal de cada institución que proporciona seguridad razonable de que se protegen los recursos públicos y se alcancen los objetivos institucionales.

Constituyen elementos del control interno: el entorno de control, la organización, la idoneidad del personal, el cumplimiento de los objetivos institucionales, **los riesgos institucionales en el logro de tales objetivos y las medidas adoptadas para afrontarlos**, el sistema de información, el cumplimiento de las normas jurídicas y técnicas; y, la corrección oportuna de las deficiencias de control.

El control interno será responsabilidad de cada institución del Estado, y tendrá como finalidad primordial crear las condiciones para el ejercicio del control externo a cargo de la Contraloría General del Estado. (Contraloría General de Estado, 2002)

2.2.1.4. Normas de Control Interno – Contraloría General del Estado

Por otra parte, las Normas de Control interno, dictadas por la Contraloría General del Estado, en el artículo 300, describe el procedimiento a seguir dentro de la Evaluación del riesgo, de la siguiente manera:

300 Evaluación del riesgo

La máxima autoridad establecerá los mecanismos necesarios para identificar, analizar y tratar los riesgos a los que está expuesta la organización para el logro de sus objetivos.

El riesgo es la probabilidad de ocurrencia de un evento no deseado que podría perjudicar o afectar adversamente a la entidad o su entorno. La máxima autoridad, el nivel directivo y todo el personal de la entidad serán responsables de efectuar el proceso de administración de riesgos, que implica la metodología, estrategias, técnicas y procedimientos, a través de los cuales las unidades administrativas identificarán, analizarán y tratarán los potenciales eventos que pudieran afectar la ejecución de sus procesos y el logro de sus objetivos.

300-01 Identificación de riesgos

Los directivos de la entidad identificarán los riesgos que puedan afectar el logro de los objetivos institucionales debido a factores internos o externos, así como emprenderán las medidas pertinentes para afrontar exitosamente tales riesgos.

Los factores externos pueden ser económicos, políticos, tecnológicos, sociales y ambientales. Los internos incluyen la infraestructura, el personal, la tecnología y los procesos.

Es imprescindible identificar los riesgos relevantes que enfrenta una entidad en la búsqueda de sus objetivos.

La identificación de los riesgos es un proceso interactivo y generalmente integrado a la estrategia y planificación. En este proceso se realizará un mapa del riesgo con los factores internos y externos y con la especificación de los puntos claves de la institución, las interacciones con terceros, la identificación de objetivos generales y particulares y las amenazas que se puedan afrontar.

Algo fundamental para la evaluación de riesgos es la existencia de un proceso permanente para identificar el cambio de condiciones gubernamentales, económicas, industriales, regulatorias y operativas, para tomar las acciones que sean necesarias.

Los perfiles de riesgo y controles relacionados serán continuamente revisados para asegurar que el mapa del riesgo siga siendo válido, que las respuestas al riesgo son apropiadamente escogidas y proporcionadas, y que los controles para mitigarlos sigan siendo efectivos en la medida en que los riesgos cambien con el tiempo.

300-02 Plan de mitigación de riesgos

Los directivos de las entidades del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos, realizarán el plan de mitigación de riesgos desarrollando y documentando una estrategia clara, organizada e interactiva para identificar y valorar los riesgos que puedan impactar en la entidad impidiendo el logro de sus objetivos.

En el plan de mitigación de riesgos se desarrollará una estrategia de gestión, que incluya su proceso e implementación. Se definirán objetivos y metas, asignando responsabilidades para áreas específicas, identificando conocimientos técnicos, describiendo el proceso de evaluación de riesgos y las áreas a considerar, detallando indicadores de riesgos, delineando procedimientos para las estrategias del manejo, estableciendo lineamientos para el monitoreo y definiendo los reportes, documentos y las comunicaciones necesarias.

Los directivos de las entidades del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos, desarrollarán planes, métodos de respuesta y monitoreo de cambios, así como un programa que prevea los recursos necesarios para definir acciones en respuesta a los riesgos. Una adecuada planeación de la administración de los riesgos, reduce la eventualidad de la ocurrencia y del efecto negativo de éstos (impacto) y alerta a la entidad respecto de su adaptación frente a los cambios.

300-03 Valoración de los riesgos

La valoración del riesgo estará ligada a obtener la suficiente información acerca de las situaciones de riesgo para estimar su probabilidad de ocurrencia, este análisis le permitirá a las servidoras y servidores reflexionar sobre cómo los riesgos pueden afectar el logro de sus objetivos, realizando un estudio detallado de los temas puntuales sobre riesgos que se hayan decidido evaluar.

La administración debe valorar los riesgos a partir de dos perspectivas, probabilidad e impacto, siendo la probabilidad la posibilidad de ocurrencia, mientras que el impacto representa el efecto frente a su ocurrencia. Estos supuestos se determinan considerando técnicas de valoración y datos de eventos pasados observados, los cuales pueden proveer una base objetiva en comparación con los estimados.

La metodología para analizar riesgos puede variar, porque algunos son difíciles de cuantificar, mientras que otros se prestan para un diagnóstico numérico.

Se consideran factores de alto riesgo potencial los programas o actividades complejas, el manejo de dinero en efectivo, la alta rotación y crecimiento del personal, el establecimiento de nuevos servicios, sistemas de información rediseñados, crecimientos rápidos, nueva tecnología, entre otros. La valoración del riesgo se realiza usando el juicio profesional y la experiencia.

300-04 Respuesta al riesgo

Los directivos de la entidad identificarán las opciones de respuestas al riesgo, considerando la probabilidad y el impacto en relación con la tolerancia al riesgo y su relación costo/beneficio.

La consideración del manejo del riesgo y la selección e implementación de una respuesta son parte integral de la administración de los riesgos. Los modelos de respuestas al riesgo pueden ser: evitar, reducir, compartir y aceptar.

Evitar el riesgo implica, prevenir las actividades que los originan. La reducción incluye los métodos y técnicas específicas para tratar con ellos, identificándolos y proveyendo acciones para la reducción de su probabilidad e impacto. El compartirlo reduce la probabilidad y el impacto mediante la transferencia u otra manera de compartir una parte del riesgo. La aceptación no realiza acción alguna para afectar la probabilidad o el impacto.

Como parte de la administración de riesgos, los directivos considerarán para cada riesgo significativo las respuestas potenciales a base de un rango de respuestas. A partir de la selección de una respuesta, se volverá a medir el riesgo sobre su base residual, reconociendo que siempre existirá algún nivel de riesgo residual por causa de la incertidumbre inherente y las limitaciones propias de cada actividad. (Contraloría General del Estado, 2009)

2.2.1.5. NTE INEN-ISO 31000 Gestión del riesgo. Principios y directrices. Primera edición 2014 - 07

Esta Norma Técnica Ecuatoriana NTE INEN-ISO 31000 es una traducción idéntica de la Norma Internacional ISO 31000:2009. Risk Management. Principles and Guidelines. El comité responsable de esta Norma Técnica Ecuatoriana y de su traducción es el Comité Interno del INEN. (Instituto Ecuatoriano de Normalización, 2014)

2.2.2. Normativa Internacional a considerar

Dentro de la normativa internacional, se tiene algunas opciones para la gestión de riesgos. El modelo de gestión de riesgos que se propondrá se basa en el capítulo que aborda los riesgos de la norma ISO 9001- 2015 y la metodología MAGERIT bajo los principios que establece la ISO 31000; sin embargo, a continuación, se describirá normativa y herramientas relacionadas con el tema, que permitirán desarrollar un modelo que se ajuste de mejor manera a las necesidades de la corporación.

2.2.2.1. ISO 9001-2015

Es la base del Sistema de Gestión de la Calidad – SGC, es una norma internacional que se centra en todos los elementos de la gestión de la calidad con los que una empresa debe contar, a fin de contar con un sistema efectivo que le permita administrar y mejorar la calidad de sus productos o servicios.

Esta norma es una actualización de la versión 9001:2008, la evolución se da en tres aspectos:

- Enfoque en procesos, incorpora el ciclo Planificar – Hacer – Verificar – Actuar (PHVA) e integra el pensamiento basado en riesgos.
- Integración del pensamiento basado en riesgos, previniendo de lo malo y aprovechando lo bueno que pueda suscitarse, reconociendo además que no todos los procesos tienen el mismo impacto en el desarrollo de las actividades de la corporación. Este es el tema de análisis y aplicación en la presente investigación.
- Ciclo PHVA, cada proyecto, proceso y actividad deben ser gestionadas en la empresa con este método, a fin de que se asignen recursos necesarios para una adecuada

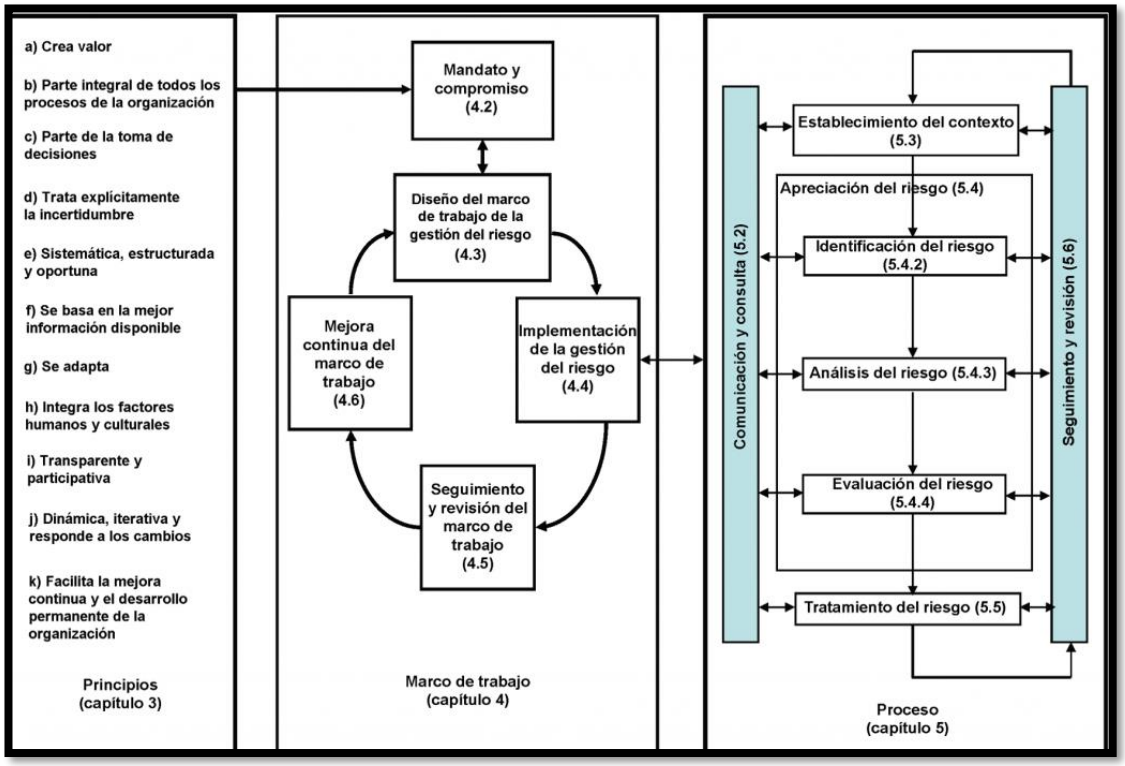
gestión y las oportunidades de mejora se determinen fácilmente. (ISO, Sistema de gestión de la calidad, 9001: 2015)

2.2.2.2. ISO 31000: 2009

Es una norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones de manera efectiva, independientemente de su tamaño y tipo.

El diseño e implementación de la gestión de riesgos depende de las necesidades de la organización, de los objetivos, del ámbito en el que se desarrolla, de su estructura, procesos y actividades, atendiendo tres pilares claves que se observan en la Figura 2.

Ilustración 2. Pilares Básicos de ISO 31000:2009



Fuente: Guía para la Gestión de riesgos: principios y directrices.

Primer pilar: Principios

La gestión del riesgo se centra en la creación y protección de valor. Debe formar parte integral de los procesos de la corporación, así como en la toma de decisiones, considerando la incertidumbre.

Segundo pilar: Marco de Trabajo

El propósito del segundo pilar es estructurar las actividades para la implementación y mejora continua del proceso de gestión de riesgos. El marco de trabajo o estructura de soporte (framework), debe ser actualizado continuamente.

Tercer pilar: Proceso de Gestión de Riesgos

Respecto al tercer pilar, éste, debería ser parte integral de la gestión y estar adaptado al proceso de negocio de la organización, e incluir los cinco componentes: establecimiento del contexto: evaluación de riesgo con la identificación, análisis y evaluación cualitativa y cuantitativa de los riesgos; el tratamiento del riesgo para la toma de decisiones; la comunicación y consulta; el monitoreo y revisión.

2.3. Similitudes y diferencias de las normativas ISO 9001: 2015 y 31000:2009 en aspectos relacionados con la Gestión del Riesgo.

2.3.1. Similitudes:

- El concepto de riesgo es común: Efecto de la incertidumbre en los objetivos.
- El riesgo es considerado no solo como amenaza, sino también como oportunidad
- Son aplicables a procesos de la empresa.
- Proporcionan insumos para plantear acciones preventivas frente a los riesgos.
- Frente a no conformidades que se presenten, es posible evaluarlas para proponer medidas que conduzcan a la mejora del proceso.

2.3.2. Diferencias:

- ISO 9001 es certificable, mientras que ISO 31000, no.

- ISO 9001, tiene como propósito la creación de un Sistema de Gestión de la Calidad, ISO 31000, es un estándar que recoge directrices y principios para la Gestión de Riesgos.
- ISO 9001:2015, aborda riesgos y oportunidades asociados con el contexto y los objetivos de la organización, mientras que ISO 31000, establece principios y directrices para la gestión de cualquier tipo de riesgos de una manera sistemática, trasparente y confiable, en cualquier ámbito y contexto. Los riesgos se identifican, se analizan y evalúan, además de que no solo contempla al riesgo como una amenaza, sino también como una oportunidad.

Una vez expuestas las similitudes y diferencias entre la dos normas ISO, se determina que aun cuando los propósitos y abordamiento del riesgo presentan diferencias, es posible que la Gestión de Riesgos bajo el esquema de ISO 9001:2015, se desarrolle bajo los principios y directrices de ISO 31000, ya que la norma 9001, no especifica una metodología para riesgos; y, debido a que ISO 31000 puede ser aplicada en cualquier ámbito y contexto, permitirá utilizarla y adaptarla para el presente trabajo.

2.4. Caso de aplicación: Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP

El modelo de gestión de riesgos de tecnologías de la información que se propondrá, se ajustará al sector de generación hidroeléctrica de la provincia del Azuay, específicamente a la Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP.

La utilización de tecnologías de la información en la empresa es alta, pues el uso de las mismas corresponde al 100% de uso a nivel de la empresa ya que todos los colaboradores de una u otra manera las utilizan para el desempeño de sus actividades laborales, y por la naturaleza de las actividades que se desarrollan, implica que la exposición al riesgo es mayor.

La corporación no cuenta con un área dedicada a la gestión de riesgos, por lo que éstos no se encuentran identificados claramente y; por lo tanto, no se tiene medidas de prevención ni de mitigación en caso de que se suscitasen incidentes de riesgo.

Con la finalidad de diseñar un modelo que se ajuste a las necesidades de la corporación, se considerará la normativa ecuatoriana, específicamente la Ley Orgánica de la Contraloría General del Estado y la Norma de Control Interno 300, “Evaluación del Riesgo”, que establecen la responsabilidad en el diseño, establecimiento, mantenimiento y evaluación de control interno a la máxima autoridad, la dirección y el personal de una organización, de manera que se proporcione seguridad razonable de que se protegen los recursos públicos y se alcancen los objetivos institucionales.

La Norma de Control Interno 300, establece a la máxima autoridad como responsable de establecer mecanismos para la identificación, análisis y tratamiento de los riesgos.

Considerando lo mencionado y el volumen de las operaciones de la Corporación Eléctrica del Ecuador CELEC EP, es importante que la Gerencia General como responsable de cumplir y hacer cumplir la ley, los reglamentos y la normativa, así como de velar por la eficiencia empresarial, como lo disponen los numerales 2 y 4 del artículo 11.- Deberes y atribuciones del gerente general, de la Ley Orgánica de Empresas Públicas, realice un análisis y evaluación del riesgo de tecnología de la información, al que puede estar expuesta la Corporación.

En base a lo expuesto, la normativa ecuatoriana, aplicable a la Corporación Eléctrica del Ecuador, no delimita qué metodología utilizar para Gestionar Riesgos; sin embargo, sí especifica que se los debe gestionar; por lo que, las norma internacional ISO 9001:2015 bajo principios y directrices de ISO 31000:2009, serán las utilizadas para el desarrollo del Modelo de Gestión de Riesgos de Tecnologías de la Información, objeto del presente trabajo.

2.5. Metodología de la Investigación

El tipo de investigación a utilizar es la investigación cualitativa, que consiste en la recopilación de información basada en la observación de comportamientos naturales, discursos, respuestas abiertas para la posterior interpretación de significados.

El método de investigación cualitativa no descubre, sino que construye el conocimiento, gracias al comportamiento entre las personas implicadas y toda su conducta observable. (SINNAPS, 2015)

2.5.1. Muestreo por Conveniencia

Se hará uso del muestreo por conveniencia, con el propósito de recabar información de personas que ocupan en la empresa una posición que va de acuerdo al fenómeno, objeto de investigación, ya que la riqueza de información que provean será útil para el trabajo que se realiza.

Los sujetos seleccionados para la realización de entrevistas, serán el jefe y dos especialistas involucrados en el desarrollo de actividades. Tres personas conformarán un equipo para cada proceso a fin de identificar riesgos asociados al mismo.

Al grupo seleccionado se le realizará entrevistas en función de una matriz que pretende levantar los riesgos asociados a los procesos de la empresa a fin de construir un modelo de gestión de riesgos de tecnologías de la información que se ajuste a la realidad de la corporación.

3. CAPITULO III: DIAGNÓSTICO DE LA EMPRESA Y ESTABLECIMIENTO DE ESQUEMA METODOLOGICO PARA DESARROLLO DE MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN

3.1. Diagnóstico de cumplimiento de Requisitos ISO 9001:2015

Para realizar un análisis de la situación actual de la empresa, se utilizará la Norma ISO 9001:2015 y los puntos que aborda la misma. El análisis se desarrolla a nivel de cumplimiento documental.

Con la finalidad de que se entienda la Tabla 4., se indica que la letra S, corresponde a SI, la letra N, corresponde a NO, y la letra P, a PARCIALMENTE.

Tabla 3. Análisis de Cumplimiento del Sistema de Gestión de la Calidad

SISTEMA DE GESTIÓN DE LA CALIDAD SGC				
DOCUMENTOS GENERALES				
SUJETO DE REVISIÓN	**S**	**N**	**P**	**OBSERVACIONES**
Los procesos están identificados y caracterizados así como la secuencia e interacción de los mismos			x	Existe un manual de procesos que no se aplica. Actualmente la empresa tiene un proyecto de Fortalecimiento de la Gestión por Procesos que se encuentra en etapa inicial.
Se aplican los procesos necesarios para el SGC en la organización			x	
Existe un manual de calidad		x		
Los procesos del mapa de procesos tiene procedimientos e instructivos documentados		x		El proyecto de Fortalecimiento de la Gestión por Procesos tiene como uno de sus productos, la elaboración de procedimientos e instructivos.
CONTEXTO DE LA ORGANIZACIÓN				
La empresa cuenta con una planeación estratégica actualizada	x			La planeación estratégica fue actualizada a finales del 2017.

Se tienen identificadas las partes interesadas y sus requisitos			x	Se considera como parte interesada al gobierno y no se enfoca en la sociedad
LIDERAZGO				
Existe una declaración documentada de la política de calidad		x		
Existe una declaración documentada de los objetivos de calidad		x		
Existe un organigrama y está actualizado con los cargos existentes			x	Actualmente el personal contratado supera a la estructura organizacional definida y no se ha aprobado una que se ajuste a las necesidades actuales. La nueva estructura ha sido presentada para aprobación del Directorio de la empresa y de Empresa Coordinadora de Empresas Públicas EMCO EP.
Existen manuales de funciones y descripción de los perfiles de cada cargo			x	No se cumple con lo establecido en los manuales.
Existen procedimientos documentados necesarios para la planificación, operación y control de los procesos			x	Dentro de las actividades a desarrollar, posterior a la aprobación de la nueva estructura, está la elaboración de un manual con los perfiles de cada cargo.
PLANIFICACIÓN				
Se cuenta con una matriz de riesgos o panorama de riesgos			x	Existe matriz solo a nivel de levantamiento de riesgos, pero no se gestionan.
Se tienen definidos objetivos de calidad por procesos		x		
SOPORTE				
La empresa ha elaborado un presupuesto para el sistema de gestión de la calidad		x		
Se tiene establecido un programa de mantenimiento para la infraestructura			x	No existe planificación en la que se pueda confiar la disponibilidad oportuna de las

				centrales, obras de los proyectos, oficinas, entre otros.
Se tiene un programa de capacitación definido con sus respectivos formatos		x		La capacitación no se ajusta a las necesidades. Uno de los objetivos en el departamento de TH es el fortalecimiento de las capacidades del personal.
Existen documentos que definan los procedimientos y directrices para la selección, vinculación y capacitación del personal			x	La elaboración de la narrativa de los procedimientos es parte del proyecto de Fortalecimiento de la Gestión por Procesos.
Existe una metodología para evaluar el desempeño y se tienen los respectivos formatos			x	El software utilizado puede ser modificado lo que lo convierte en un elemento no objetivo
Se tiene un documento para evaluar el clima organizacional			x	
Existe un documento donde se definen las directrices para la comunicación en la organización		x		
Existe un procedimiento para la elaboración, modificación y control de los documentos			x	La dotación de formatos para elaboración o modificación de documentos, se encuentra en proyecto.
Existe un procedimiento para la elaboración, modificación y control de los registros		x		
OPERACIÓN				
Se cuenta con procedimientos para la planificación del servicio		x		
Hay documentos que evidencien la interacción con el cliente			x	Para el caso de visitas a proyectos, centrales y demás sitios de la corporación, a través de la página web se puede acceder a un link para solicitar una visita al lugar deseado.
Se tiene información documentada para los proveedores externos			x	La comprobación de la veracidad de la información es casi nula.

Se cuenta con documentos que definan como se controla el servicio		x		
EVALUACIÓN DEL DESEMPEÑO				
Se cuenta con documentación para evaluar el desempeño de los procesos		x		En etapa de elaboración.
Se determinan los métodos de seguimiento, medición, análisis y evaluación, en su caso, para garantizar la validez de los resultados del SGC		x		
Se tiene establecido un procedimiento para las auditorías internas			x	El programa de auditoría es presentado al Gerente General, pero no se lleva a cabo completamente, además de que se solicita a la Gerencia que recomiende qué auditar en la empresa
Existen métodos para medir la satisfacción del cliente		x		
Existe un procedimiento establecido y documentado para la revisión por la dirección con sus respectivos formatos			x	En etapa de elaboración.
MEJORA				
Existe documentación para la toma de acciones correctivas y/o preventivas		x		
Existe documentación para elaborar planes de mejora		x		
Existe información documentada como prueba de la naturaleza de las no conformidades y de las acciones tomadas posteriormente			x	Se elaboran informes luego de actuar ante una situación de emergencia.

Fuente: Corporación Eléctrica del Ecuador

En función de la evaluación realizada en la Tabla 3, se observa que la gestión por procesos se encuentra en etapa inicial y que el factor determinante en este caso es la administración a lo largo de los años, pues no ha dedicado esfuerzos para contar con procesos documentados ni para gestionar los riesgos, lo que no ha permitido contar con un control adecuado.

En el siguiente capítulo, se vinculará la Tabla 3, con la identificación de los riesgos asociados a cada proceso.

3.2. Mecanismos de Gestión de Riesgos asumidos por la alta dirección.

En cuanto a la gestión de riesgos en la Corporación, no se han realizado esfuerzos por gestionarlos.

Mediante Oficio No. 000655 DR2-DPA-AE de fecha 25 de junio de 2015, el Delegado Provincial del Azuay de la Contraloría General del Estado, hace la entrega del informe de auditoría financiera por los ejercicios económicos terminados al 31 de diciembre de los años 2010 y 2011 a la Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP, donde manifiesta en una de sus recomendaciones que la Gerencia General, no ha implantado mecanismos para la evaluación del riesgo, lo que no garantiza seguridad razonable en la generación de información por parte de la Corporación.

Posterior a este informe, se procedió con la difusión del mismo, a fin de solicitar a los colaboradores de la empresa que realicen la identificación de los riesgos asociados a sus actividades.

Existe una identificación básica de riesgos en los diferentes procesos, pero no cuentan con medidas de tratamiento, prevención y mitigación, razón por la cual en la matriz a continuación no hay evidencia de establecimiento de controles; sin embargo, más adelante se analizarán los riesgos y controles que se determinarán en las entrevistas con los expertos de cada proceso de la corporación, que serán el punto de partida para el desarrollo del Modelo de Gestión de Riesgos de Tecnología de la Información.

Tabla 4. Evidencia de Establecimiento de Controles

SECCIÓN	RIESGO	CONTROL
Contexto	A nivel interno la corporación no cuenta con herramientas informáticas que le permita documentar ni hacer seguimiento del cumplimiento de los procesos. Al ser CELEC EP una empresa del sector público, debe regirse a la utilización de herramientas informáticas que se encuentran obsoletas y no contribuyen a la mejora de la empresa y por ende a su crecimiento.	No se han establecido controles

SECCIÓN	RIESGO	CONTROL
Liderazgo	La alta dirección no se encuentra comprometida con la utilización de herramientas informáticas para el desarrollo de actividades en la empresa. La cantidad de recursos económicos que se destinan para la adquisición de herramientas informáticas es insuficiente La Gerencia y Directorio de la corporación no consideran el peligro que constituye el no contar con medidas de protección para los ciberataques y hackers.	No existen controles establecidos
Planificación	Al no existir un sistema de gestión de riesgos, las herramientas informáticas utilizadas para de alguna manera gestionarlos, no son apropiadas, como, por ejemplo, el uso de EXCEL para recopilar lo riesgos identificados. Dentro de la planificación anual de la empresa y de su presupuesto, no se considera software ni consultorías para seguridad de la información, para gestión de riesgos, ni salvaguardar los activos de información.	No se han establecido controles
Soporte	La información no cuenta con medios que la documenten ni difundan adecuadamente. El servicio de Telecomunicaciones no está asegurado, pues existe total dependencia de la empresa estatal CNT para que provea la misma y para el caso de las centrales que se encuentran ubicadas en lugares de baja cobertura, se genera un problema al momento de establecer comunicación oportuna. El proveedor del software para seguimiento de operación de centrales, es asiático, lo que, por cuestiones de idioma, dificulta la solución de problemas que se presenten. La información que es de carácter público no cuenta con repositorio que permita a los empleados conocerla y considerarla para el desarrollo de sus actividades. La validación de los contratistas, la información que éstos proveen no cuenta con un sistema ni área dedicada a comprobar la veracidad de la misma.	No se han establecido controles

SECCIÓN	RIESGO	CONTROL
Operación	El desconocimiento de las aplicaciones y sistemas operativos por parte del personal, podría repercutir en la confiabilidad y disponibilidad de las centrales. La asignación de los niveles de autorizador para efectuar transferencias bancarias, debería contemplar a una sola persona y las contraseñas para hacerlo, no deberían compartirse. Para la solución de problemas en la operación de centrales, se recurre al soporte en línea por parte del proveedor asiático, razón por la cual el acceso a la información de la empresa no está restringido para terceros. Debido a la falta de repuestos para equipos informáticos, materiales para limpieza, accesorios y además a la falta de personal disponible y capacitado, pueden generar que no se realice los mantenimientos preventivos y correctivos y no se atiendan los casos presentados, lo cual podría llevar a que los servicios de Tics no estén disponibles o en óptimas condiciones para su correcto funcionamiento. Existe información que es de carácter confidencial y que no ha sido tratada adecuadamente, por lo que cualquier persona puede acceder a ésta.	No se han establecido controles
Evaluación del Desempeño	El sistema para realizar la evaluación del desempeño de 360 º, puede ser modificado, lo que no asegura que la evaluación sea confiable y objetiva.	No se han establecido controles
Mejora continua	Constituye un riesgo el no contar con programas y planes de mejora continua	No se han establecido controles.

Fuente: Corporación Eléctrica del Ecuador

Elaborado por: María Isabel Carrillo

Para la propuesta del Modelo de Gestión de Riesgos de Tecnologías de la Información que se abordará en el siguiente capítulo, se considerará los once principios que establece la ISO 31000 y que fueron definidos en el capítulo anterior.

3.3. Esquema metodológico para el desarrollo del modelo de gestión de riesgos de tecnología de la información

Para el desarrollo del esquema metodológico, se tomará en consideración el apartado 6, “Planificación” de la norma ISO 9001:2015, que incorpora el enfoque basado en Riesgos, que implica que las empresas deben incluir métodos o procedimientos para le evaluación, administración, eliminación y/o minimización de los riesgos, al momento de adaptar sus sistemas de gestión.

En el apartado 6, “Planificación”, específicamente en el punto 6.1 Acciones para abordar riesgos y oportunidades, se utilizará como herramienta de gestión de riesgos la norma internacional ISO 31000:2009, para lo cual a continuación se detalla la estructura a seguir que constituirá el modelo de gestión de riesgos de tecnologías de la información, que será aplicado en el siguiente capítulo.

3.3.1. Fases de desarrollo de la metodología

3.3.1.1. Fase 1: Determinación y descripción de procesos que se desarrollan en la corporación

En esta primera fase, se procederá con la determinación y descripción de cada uno de los procesos que se ejecutan en la empresa y sobre los cuales se realizará el levantamiento de los riesgos a través de entrevistas con los expertos.

Se determinarán además los responsables de la ejecución de los procesos.

3.3.1.2. Fase 2: Establecimiento del contexto

Consiste en la definición de los aspectos internos y externos que se deben considerar para la gestión de riesgos.

Dentro de los aspectos internos, están:

- La estructura organizativa
- Funciones y responsabilidades

- Gobierno Corporativo
- Políticas
- Objetivos
- Estrategias
- Normas, directrices, base legal que la rige.
- Cultura organizacional
- Sistemas de información.

Dentro de los aspectos externos, están:

- Factores sociales
- Factores Políticos
- Factores Tecnológicos
- Factores Económicos
- Factores Jurídicos

3.3.1.3. Fase 3: Identificación del Riesgo

En la fase de identificación del riesgo, se realizarán entrevistas con expertos en cada proceso, quienes proporcionarán información respecto de cuáles son los riesgos asociados a los procesos, dónde se originan los riesgos, sus causas y cómo éstos pueden impactar en los objetivos de la corporación.

Para realizar la identificación, se utilizará la Tabla 6. Matriz de identificación de riesgos, donde los campos deben ser completados según los siguientes criterios:

Proceso: Nombre del Proceso

Objetivo del Proceso: La finalidad o propósito de determinado proceso en la empresa, para qué se lo ejecuta, su producto.

Descripción del Riesgo: Breve descripción del riesgo

Punto crítico del proceso donde se identifica el riesgo: En dónde se origina el riesgo, revisando la caracterización y flujograma del proceso.

Causas: Qué desencadena un riesgo, la razón por la que se origina el riesgo.

Causa raíz: Descripción de la causa principal que desencadena, origina o genera un riesgo.

Consecuencias potenciales: Cómo puede repercutir un riesgo sobre los objetivos y procesos de la organización.

Tabla 5. Matriz de identificación de riesgos

Proceso	Objetivo del Proceso	Riesgo	Punto cítrico del proceso donde se identifica el riesgo	Causas	Consecuencias potenciales

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

3.3.1.4. Fase 4: Análisis de Riesgo

El análisis de los riesgos permitirá la comprensión de los mismos. Los factores a considerar para el análisis de riesgos son la probabilidad y el impacto.

La Probabilidad puede ser medida con criterios de frecuencia, si se ha materializado, y se la determinará a través del formato establecido en la Tabla 6. Determinación de la Probabilidad.

Tabla 6. Determinación de la Probabilidad

NIVEL	DENOMINACIÓN	FRECUENCIA
E-1	MUY BAJO	No se ha presentado en el último año.
D-2	BAJO	Al menos una vez en el último año.
C-3	MEDIO	Al menos una vez en los últimos 6 meses.
B-4	ALTO	Al menos una vez en los últimos 3 meses
A-5	MUY ALTO	Más de una vez en los últimos 3 meses.

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

El Impacto se mide según el grado en que las consecuencias o efecto pueden afectar a la corporación si se materializa el riesgo y se lo determinará mediante el formato de la Tabla 7. Determinación del Impacto.

Tabla 7. Determinación del Impacto.

NIVEL	DENOMINACIÓN	DESCRIPCIÓN
1	INSIGNIFICANTE	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la corporación.
2	LEVE	Si el hecho llegara a presentarse, tendría bajo impacto o efectos sobre la corporación.
3	MODERADO	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la corporación.
4	ALTO	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la corporación.
5	CATASTRÓFICO	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la corporación.

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

3.3.1.5. Fase 5. Evaluación del Riesgo

La evaluación de los riesgos, facilitará la toma de decisiones, en función de los resultados obtenidos de la calificación de la probabilidad y del impacto.

Los resultados obtenidos de la evaluación, nos darán una pauta para conocer qué riesgos necesitan tratamiento, y la prioridad para tratarlos.

La evaluación podría, además, indicar que los controles existentes deben mantenerse porque son los adecuados para tratar los riesgos.

Con la finalidad de tomar una decisión adecuada, se procederá con la evaluación de los riesgos, en base a formato definido en la Tabla 9. Matriz de Evaluación del Riesgo.

En la matriz de la Tabla 8., a continuación, se tiene la equiparación del nivel cualitativo del riesgo encontrado durante la fase de análisis de riesgos, frente a los criterios cualitativos del riesgo, previamente identificados.

Tabla 8. Matriz de Evaluación del Riesgo Cualitativo

		IMPACTO				
		INSIGNIFICANTE (1)	LEVE (2)	MODERADO (3)	ALTO (4)	CATASTRÓFICO (5)
PROBABILIDAD	MUY ALTO (5)	(5)	(10)	(15)	(20)	(25)
	ALTO (4)	(4)	(8)	(12)	(16)	(20)
	MEDIO (3)	(3)	(6)	(9)	(12)	(15)
	BAJO (2)	(2)	(4)	(6)	(8)	(10)
	MUY BAJO (1)	(1)	(2)	(3)	(4)	(5)

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

Tabla 9. Matriz de Análisis y Evaluación del Riesgo

RIESGO	OCURRENCIA	NIVEL DE LA OCURRENCIA	IMPACTO	NIVEL DEL IMPACTO	EVALUACIÓN DEL RIESGO	NIVEL DE RIESGO INHERENTE

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

En la Tabla 9, el nivel de riesgo inherente, depende del resultado obtenido en la evaluación del riesgo, bajo los siguientes criterios:

- Si el resultado de la evaluación del riesgo, está entre 0 y 1, el nivel de riesgo inherente es BAJO
- Si el resultado de la evaluación del riesgo, está entre 2 y 6, el nivel de riesgo inherente es MODERADO
- Si el resultado de la evaluación del riesgo, está entre 8 y 12, el nivel de riesgo inherente es ALTO
- Si el resultado de la evaluación del riesgo, está entre 15 y 25, el nivel de riesgo inherente es EXTREMO

3.3.1.6. Fase 6. Valoración del Riesgo

Dentro de la fase de Valoración del Riesgo, se procederá con la determinación de las siguientes variables:

- Controles existentes a nivel de los procesos
- Tipo de control que se aplica
- Periodicidad con la que se aplica el control
- Eficacia del Control
- Valoración del Control
- Grado de exposición
- Nivel de Riesgo Residual

Con el propósito de determinar las variables indicadas, se aplicará el siguiente formato:

Tabla 10. Factores para Valoración del Riesgo

Controles existentes	Tipo de Control	Valor asignado	Periodicidad del control	Valor asignado	Producto (Tipo x Periodicidad)	Eficacia del Control	Valoración del Control	Grado de exposición residual	Nivel de riesgo residual

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

Para comprensión de la Tabla 10., se describen los factores que la incluyen y cómo se determinan estos factores.

Controles existentes:

Los controles existentes, deben ser verificados en la caracterización de los procedimientos asociados a cada proceso (para el caso que existan procedimientos).

Tipo de control:

Dentro de los controles que existan en la empresa, se clasificarán de la siguiente manera y con la asignación de un valor, así:

Tabla 11. Tipo de Control

Tipo de Control	Valor asignado
Preventivo	4
Correctivo	3
Detectivo	2
Inexistente	1

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

- Preventivo: Control aplicado para evitar problemas antes de que aparezcan, monitorear operaciones y transacciones de entrada. Tiene como finalidad predecir problemas y hacer ajustes, prevenir ocurrencias de errores, omisiones.
- Correctivo: Tiene como finalidad reducir el impacto de una amenaza, identificar la causa de un problema, corregir errores suscitados.
- Detectivo: Controles que permiten la detección de errores, omisiones u actos que podrían perjudicar a la empresa.
- Inexistente: No existen controles.

Periodicidad de control

Cada cuanto tiempo se aplica un control, los cuales pueden ser:

Tabla 12. Periodicidad de control

Periodicidad de control	Valor asignado
Ocasional	1
Periódico	2
Permanente	3

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

- Ocasional: Controles claves que se aplican solo en forma ocasional en un proceso.
- Periódico: Controles claves aplicados en forma constante solo cuando ha transcurrido un periodo específico de tiempo.
- Permanente: Controles claves aplicados durante todo el proceso; es decir, en cada operación.

Producto

El producto se obtiene del resultado de multiplicar los valores asignados al Tipo de Control * Periodicidad de Control.

Eficacia del Control

Para determinar la eficacia de un control, se debe considerar el resultado del PRODUCTO.

- Si el producto presenta valores entre 1 y 3, se considera que no se han establecido controles; es decir, es inexistente.
- Si el producto presenta valores entre 4 y 6, se considera que la eficacia es baja.
- Si el producto presenta valores entre 7 y 9, se considera que la eficacia es media.
- Si el producto presenta valores entre 10 y 12, se considera que la eficacia es alta.

En la asignación de valores a la eficacia de control, corresponde:

Tabla 13. Eficacia de Control

Eficacia de control	Valoración del control
Inexistente	1
Baja	2
Media	3
Alta	4

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

Grado de exposición residual

Se refiere al grado en el que un proceso o actividad está expuesto al riesgo, aun después de haber implementado controles.

Para determinar el grado de exposición, se considerará el resultado obtenido en la Matriz de Evaluación del Riesgo (probabilidad * impacto), se multiplicará por la valoración del control.

Grado de exposición residual= Evaluación del Riesgo / Valoración del Control

Nivel de Riesgo Residual

El nivel de riesgo residual se califica en función del resultado obtenido en el cálculo del Grado de exposición residual.

Los parámetros a considerar para la calificación, son:

Tabla 14. Nivel de Riesgo Residual

Nivel	Valor
Bajo	De 1 a 4
Moderado	De 5 a 8
Alto	De 9 a 12
Extremo	De 15 a 25

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

3.3.1.7. Fase 7. Tratamiento del riesgo

Para el tratamiento del riesgo, se considerará la matriz de la Tabla 15.

Tabla 15. Tratamiento del riesgo

ESTRATEGIAS DE TRATAMIENTO	ACCIÓN DE TRATAMIENTO	TIEMPO DE IMPLEMENTACIÓN	RESPONSABLE	NOMBRE DEL INDICADOR	INDICADORES	METAS (% o # cumplimiento indicadores)	EVIDENCIA DE CUMPLIMIENTO	RESPUESTA ANTE EMERGENCIA

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

Estrategias de Tratamiento

Asumir: Esta medida nos conduce a aceptar el riesgo sin ocuparnos de buscar medidas para tratarlas, sino solo mantenerlo monitoreado, ya que no es posible la reducción de su probabilidad de ocurrencia, ni el impacto.

Evitar: Dentro de las opciones para evitar el riesgo, están: no proceder con el proyecto o actividad que incorpora el riesgo, o, escoger medios diferentes a los planificados para el desarrollo de un proyecto o actividad que logren el mismo resultado, pero que no incorporen el riesgo detectado. El problema que se puede suscitar al momento de evitar riesgos es que se pierda la oportunidad de un negocio y que, además, otros riesgos, no identificados, se vuelvan significativos.

Reducir: esta medida, tiene como objetivo la reducción de la probabilidad de ocurrencia de un riesgo, o reducir sus consecuencias, o lograr los dos objetivos a la vez. La probabilidad de ocurrencia de un riesgo se puede reducir a través de controles. Las consecuencias pueden reducirse asegurando que los controles se apliquen en el momento apropiado y de manera adecuada.

Transferir: El objetivo de esta medida es eliminar el riesgo transfiriéndolo de un lugar a otro, por ejemplo, la contratación de un seguro.

Tabla 16. Matriz medidas de tratamiento del riesgo

		IMPACTO				
		INSIGNIFICANTE (1)	**LEVE (2)**	**MODERADO (3)**	**ALTO (4)**	**CATASTRÓFICO (5)**
PROBABILIDAD	**MUY ALTO (A-5)**	B(5)	M(10)	A(15)	E(20)	E(25)
	ALTO (B-4)	B(4)	M(8)	A(12)	E(16)	E(20)
	MEDIO (C-3)	B(3)	M(6)	M(9)	A(12)	A(15)
	BAJO (D-2)	B(2)	B(4)	M(6)	M(8)	M(10)
	MUY BAJO (E-1)	B(1)	B(2)	B(3)	B(4)	B(5)

B: Zona de riesgo baja= Asumir el riesgo. De 1 a 5.

M: Zona de riesgo Moderado= Asumir el riesgo, reducir el riesgo. De 6 a 10.

A: Zona de riesgo Alta= Reducir el riesgo, evitar, compartir o transferir. De 11 a 15.

E: Zona de riesgo Extremo= Reducir el riesgo, evitar, compartir o transferir. De 16 a 25.

Fuente: Expertos CELEC EP y autora|

Elaborado por: María Isabel Carrillo

Acción de Tratamiento:

Descripción de las acciones a realizar para tratar los riesgos identificados y evaluados.

Tiempo de Implementación:

El tiempo que tomará implementar o ejecutar la acción de tratamiento.

Responsable:

Definición de la persona responsable de la ejecución de la acción de tratamiento.

Nombre del Indicador

Definir nombre del indicador que nos permitirá determinar resultados alcanzados.

Indicadores

Se debe definir indicadores que permitirán evaluar los resultados obtenidos, producto de la ejecución de la estrategia y acción de tratamiento del riesgo.

Metas

Porcentaje de acciones de tratamiento ejecutadas en un periodo de tiempo determinado.

Evidencia de cumplimiento

Establecer mecanismos a través de loa cuales se puede evidenciar el cumplimiento de las acciones de tratamiento del riesgo.

Respuesta ante emergencia

Establecer acciones a realizar si se suscitasen eventualidades.

3.3.1.8. Fase 8. Monitoreo y revisión

La fase de monitoreo y revisión es transversal a todas las fases del Sistema de Gestión de Riesgos.

Con el propósito de desarrollar esta fase, se considerará la matriz de la Tabla 17.

Tabla 17. Monitoreo y revisión

MECANISMOS DE VERIFICACIÓN	RESPONSABLES	PERIODICIDAD	RESULTADOS DE LA ACCIÓN (En base a los resultados de esta fase, el proceso deberá continuar nuevamente con la Fase 2 del sistema: Establecimiento del contexto)

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

Mecanismos de verificación: Definir mecanismos para verificar que los controles que se han aplicado son los adecuados, así como para obtener más información para mejorar la evaluación de los riesgos.

Responsables: Definir el responsable del monitoreo y revisión de las acciones de tratamiento.

Periodicidad: Cada cuánto tiempo se realiza el monitoreo y revisión.

Resultados de la acción: En base a los resultados de esta fase, el proceso deberá continuar nuevamente con la Fase 2. Establecimiento del contexto.

3.3.1.9. Fase 9. Comunicación y consulta.

La comunicación debe ser permanente durante todas las fases del sistema de Gestión de Riesgo. Es importante que se desarrolle de manera bidireccional, ya que la retroalimentación es básica, de manera que permita determinar si las decisiones tomadas han sido acertadas y cuáles son las medidas pendientes de realizar frente a los riesgos que aún no han sido identificados o que representan un riesgo potencial.

Para el desarrollo de esta fase, se considerará la matriz de la Tabla 18**.**

Tabla 18. Comunicación y consulta

IDENTIFICAR GRUPOS DE INTERÉS	PLANES DE COMUNICACIÓN Y CONSULTA	SISTEMAS DE INFORMACIÓN Y CONSULTA	RESPONSABLES	PLAZOS

Fuente: Expertos CELEC EP y autora

Elaborado por: María Isabel Carrillo

Identificar grupos de interés: Establecer comunicación con los grupos externos e internos, de interés para la empresa.

Planes de comunicación y consulta: Los planes que se han definido para mantener el flujo de comunicación en la empresa.

Sistemas de Información y consulta: Lo sistemas que se han establecido en la empresa para que el flujo de comunicación sea permanente y que todas las personas involucradas tengan acceso.

Responsables: Determinar los responsables de llevar la información y mantener la comunicación en la empresa como líderes, mediante los sistemas y planes de comunicación.

Plazos: Definición de plazos establecidos para que una determinada información sea comunicada.

En todo el transcurso de la fase de comunicación y consulta se debe evaluar el impacto de esta información y qué tan adecuados son los planes y canales de comunicación utilizados.

4. CAPÍTULO IV: APLICACIÓN DEL ESQUEMA METODOLÓGICO PARA EL DESARROLLO DEL MODELO DE GESTION DE RIESGOS DE TECNOLOGIA DE LA INFORMACIÓN

Para dar inicio a la aplicación del esquema metodológico, en la Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP, se describirán los procesos que conforman el Sistema de Gestión de Calidad de la empresa, que son sobre los cuáles se han levantado los riesgos.

4.1. Fase 1: Determinación y descripción de procesos que se desarrollan en la corporación

Mediante esta fase, se pretende identificar el conjunto de actividades interrelacionadas o que interactúan y deben categorizase como un proceso.

Para que estas actividades, sean definidas como procesos deben cumplir las siguientes características:

- Actividades existentes en la Unidad de Negocio
- Actividades para cubrir con la estrategia, objetivos y políticas.
- Actividades para cubrir mejores prácticas o sistemas de gestión.
- Actividades para cubrir requisitos normativos.
- Actividades para cumplir los Requisitos de las Partes Interesadas.

Los procesos se pueden agrupar por los siguientes tipos:

Procesos de Direccionamiento

- Gestionar los recursos financieros
- Planear y administrar la estrategia corporativa
- Desarrollar la estrategia corporativa
- Gestionar la comunicación

Procesos de Mejora

- Gestionar los procesos
- Efectuar el mejoramiento corporativo

- Desarrollar y administrar planes para el manejo documental
- Realizar auditorías internas
- Gestionar relaciones internas y externas

Procesos Financieros

- Administrar los recursos financieros
- Administrar el presupuesto y proyecciones
- Administrar los recursos financieros
- Gestionar la contabilidad

Procesos de Operación

- Operar centrales de generación

Procesos de Mantenimiento

- Mantenimiento de centrales de Generación
- Desarrollar el mantenimiento preventivo y predictivo

Procesos Jurídicos

- Administrar servicios legales
- Gestionar la normatividad externa
- Administrar servicios legales
- Realizar asesoría y patrocinio judicial y administrativo

Procesos de Servicios Complementarios

- Planear y administrar las instalaciones físicas
- Administrar servicios complementarios
- Administrar la seguridad física y del personal

Procesos de Adquisiciones

- Gestionar bienes y servicios
- Contratar bienes, servicios, obras y consultorías

Procesos de TIC

- Construir, adquirir e implementar las tecnologías de información, comunicaciones y seguridad
- Administrar tecnología de información, comunicaciones y seguridad
- Supervisar, evaluar y valorar las tecnologías de información, comunicaciones y seguridad.
- Administrar servicios internos de comunicación

Procesos de Talento Humano

- Gestionar el talento humano
- Gestionar la vinculación y desvinculación del personal.
- Planear y evaluar la gestión del talento humano
- Gestionar los programas de compensación y beneficios
- Gestionar las relaciones laborales

Procesos de Inventarios y Activos

- Gestionar bienes y servicios
- Administrar almacenes
- Gestionar activos fijos y bienes de control
- Gestionar los seguros requeridos por la corporación

Procesos de Seguridad y Salud Laboral

- Administrar la seguridad y salud en el trabajo

Procesos de Gestión Ambiental

- Realizar la gestión social y ambiental
- Administrar relaciones con los grupos de interés

Procesos de Expansión

- Diseñar centrales de generación
- Realizar los estudios de planeamiento de expansión
- Realizar estudios de proyectos de generación
- Desarrollar las obras de infraestructura eléctrica

4.2. Fase 2. Establecimiento del contexto

La Corporación Eléctrica del Ecuador CELEC EP, se creó como una Empresa Pública Estratégica, responsable de cumplir con los procesos de: generación, transmisión, distribución, comercialización, importación y exportación de energía eléctrica; ampliación del sistema eléctrico existente; planificación, diseño, instalación, operación y mantenimiento de sistemas, no incorporados al Sistema Nacional Interconectado, así como las demás responsabilidades establecidas en el Decreto Ejecutivo No. 220, de fecha 14 de enero de 2010

El Artículo 314 de la Constitución de la República del Ecuador, establece que el Estado es responsable de la provisión de servicio eléctrico y éste debe responder a los principios de obligatoriedad, generalidad, uniformidad, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad.

El Artículo 315 de la Constitución de la República del Ecuador, establece que el Estado constituirá empresas públicas para la gestión de sectores estratégicos, la prestación de servicios públicos, el aprovechamiento sustentable de recursos naturales o de bienes públicos y el desarrollo de otras actividades económicas.

Dicho precepto constitucional dispone que las Empresas Públicas funcionen como Sociedades de Derecho Público, con personalidad jurídica, autonomía financiera, económica, administrativa y de gestión, con altos parámetros de calidad y criterios empresariales, económicos, sociales y ambientales.

. Los aspectos relacionados con el Direccionamiento Estratégico, tales como: misión, visión, valores, principios, políticas, fortalezas, oportunidades, debilidades y amenazas, han sido definidos en el capítulo I.

Dentro del contexto de la Corporación, es fundamental considerar que, al ser una empresa pública, factores como el político y jurídico tienen una gran incidencia en las actividades, operaciones y decisiones que se ejecutan en la empresa.

Establecimiento de grupos de interés

Dentro de los grupos de interés se tiene:

- Colaboradores
- Sociedad en general
- Comunidades donde los proyectos se desarrollan (zonas de influencia)
- Empresas del sector eléctrico ecuatoriano
- Empresas del sector eléctrico internacional
- Entidades financieras nacionales e internacionales
- Empresas fiscalizadoras
- Empresas constructoras
- Demás entidades del sector público y privado.

Delimitación del Alcance:

El Modelo de Gestión de Riesgos se enfocará en los riesgos de tecnología de la información que se han identificado a nivel de los procesos de la Corporación.

Para las fases que se desarrollarán más adelante, han colaborado en la identificación de los riesgos, colaboradores de la empresa que se consideran expertos en los procesos, de manera que aporten con su conocimiento y experiencia, lo que facilitará la generación de medidas y acciones de tratamiento pata los riesgos identificados.

4.3. Fase 3. Identificación de Riesgos

Las entrevistas a los expertos permitieron la identificación de riesgos asociados a cada uno de los procesos que se desarrollan en CELEC EP Hidropaute.

Los riesgos identificados, según opiniones de los expertos repercuten sobre todo en aspectos relacionados con la confiabilidad y disponibilidad de las centrales, lo que afectaría por ende a la consecución del objetivo estratégico, **Mantener la disponibilidad, confiabilidad y resiliencia de los sistemas de generación/transporte de energía eléctrica y de telecomunicaciones de acuerdo a la normativa y estándares internacionales,** definido en el Capítulo I.

Por otra parte, la pérdida de información, así como la filtración de información de carácter confidencial, están relacionadas con fallas en los sistemas y vulnerabilidad de controles, respectivamente.

En el anexo 1. Matriz de Identificación de Riesgo de Tecnologías de la Información de CELEC EP, se detallan los riesgos identificados, los procesos a los cuales están asociados y demás elementos que conforman la referida matriz.

4.4. Fase 4. Análisis y Evaluación de los Riesgos Identificados.

En función de los criterios de los expertos, se ha asignado un valor tanto a la probabilidad como al impacto de los riesgos identificados.

Posterior a la asignación de estos valores, tal como se explicó en las Tablas 7 y 8, se procedió con la evaluación de los mismos, en función de lo definido en la Tabla 8.

El análisis y evaluación de los riesgos se realizó bajo el formato definido en la Tabla 9; y, en función de los resultados obtenidos se procedió con la valoración de los controles existentes, así como al desarrollo de controles necesarios y adecuados, a fin de gestionar los riesgos.

Para la realización de la Fase 4, se procedió con la matriz de Análisis y Evaluación de los Riesgos de Tecnologías de la Información de CELEC EP, que consta en el anexo 2.

4.5. Fase 5. Valoración de los Riesgos Identificados

Durante la fase de Valoración de los riesgos, los expertos manifestaron que cuentan con controles asignados para los riesgos que pudiesen suscitarse, pero que debido a que no existe un sistema de gestión de riesgos establecido, los controles se los realiza a discreción de los colaboradores encargados de monitorear los riesgos.

Generalmente se aplican esos controles en el momento en el que se materializa el riesgo o hay indicios de que se suscitará un riesgo en un futuro cercano.

Lo que se realizó en esta fase, fue organizar en una matriz de valoración de los riesgos, la información respecto de los controles que se considera a criterio de los expertos, se aplican en la empresa, aunque no de manera formal.

La aplicación de controles, debería realizarse de manera PREVENTIVA y PERMANENTE, con el fin de que su eficacia siempre alcance la escala ALTA y su nivel de riesgo residual sea BAJO.

Para el desarrollo de esta fase, se utilizó la Matriz de Valoración de los riesgos, que se visualiza en el anexo 3.

4.6. Fase 6. Tratamiento de los Riesgos Identificados

Una vez que se cuenta con la evaluación de los riesgos y la valoración de los controles, así como el establecimiento de controles necesarios, es importante que se tomen decisiones respecto a qué acciones realizar para tratar los riesgos identificados.

Las medidas tomadas para tratar los riesgos identificados, en su mayoría contemplan la reducción de los riesgos, a través de diferentes programas, proyectos, creación de metodologías.

Se debe considerar que los bienes que se encuentran bajo custodia de la corporación, representan valores significativos; y, el daño, inadecuada manipulación o falta de mantenimiento de aquellos bienes y activos que son utilizados para la generación de energía, repercutiría en la confiabilidad y disponibilidad de las centrales, además de consecuencias económicas desfavorables.

Una de las medidas de tratamiento para proteger los bienes de la corporación, sería la contratación de un seguro, que, aunque representa un valor alto por concepto de pago de prima de seguro, sería conveniente realizarlo, pues si se toma en cuenta el terremoto ocurrido en el Ecuador en abril del 2016, las pérdidas fueron significativas; por ello, la importancia de contar con una cobertura suficiente y adecuada.

Por otra parte, los tiempos de implementación de las acciones de tratamiento, así como tener definidos los responsables de ejecutar y supervisar estas mejoras, es fundamental, así como el establecimiento de indicadores y mecanismos que permitan evidenciar el cumplimiento de las acciones de tratamiento.

Las respuestas ante emergencias, también son un factor clave a considerar, ya que aun cuando se tiene un plan definido para tratar los riesgos, las eventualidades no pueden descartarse, por lo que actuar con oportunidad y calidad es lo que se pretende con la generación de respuestas ante emergencias.

La fase de tratamiento de los riesgos, para su desarrollo, utilizó una matriz que se visualiza en el anexo 4.

4.7. Fase 7. Monitoreo y revisión

El monitoreo y la revisión debe realizarse en todos los procesos y actividades que se realizan en la corporación.

Para el caso específico de la gestión de riesgos de tecnologías de la información, se ha establecido que los responsables, realicen el monitoreo de los riesgos en función de su importancia.

Cabe recalcar que el monitoreo no debe realizarse solo cuando un riesgo se ha materializado y tomar esto como un motivo para supervisar cómo se están gestionando los riesgos, pues mientras el monitoreo sea adecuado, es mayor la probabilidad de aplicar controles preventivos y detectar fallas a tiempo.

Como mecanismo de verificación, se ha definido reuniones con la Gerencia que permitan comunicar la situación de los procesos y por ende de los riesgos y sus medidas de tratamiento.

Las reuniones, además, robustecen el sistema de gestión de riesgos, pues un trabajo en equipo, permite generar mayor cantidad de ideas y soluciones a problemas.

En el anexo 5, se observa la matriz que contiene los insumos necesarios para la fase de monitoreo y revisión.

4.8. Fase 8. Comunicación y consulta

Para el desarrollo de la fase de comunicación y consulta, se proponen medidas enfocadas a que el personal de la corporación tenga conocimiento de la importancia de la gestión de riesgos y cuáles son los planes y acciones que existen a fin de que los incorporen en sus actividades diarias. Una de las medidas que se proponen para que los colaboradores de la

empresa tengan presente el riesgo en su mente, es el envío de cápsulas informativas, con mensajes cortos pero claros, que motiven a las personas a realizar sus actividades pensando siempre en el riesgo.

La comunicación debe realizarse de manera continua y no llevarse a cabo solo por un área determinada, pues el involucramiento de la alta Gerencia de CELEC EP, denota la importancia de la comprensión y responsabilidad sobre los riesgos.

Como medida adicional, la implementación de un buzón de sugerencias con acciones para gestión de riesgos, ayudará a la corporación a conocer la percepción de sus empleados respecto a las actividades y procesos en los cuales ellos consideran que el riesgo juega un papel importante, así como cuál es el tratamiento que darían a un evento que se suscite.

La comunicación es un aspecto que debe tratarse con mucho cuidado en la corporación, pues al ser una empresa pública, la información que se genera al interior en algunas ocasiones es de carácter confidencial y la divulgación de esta, abarcaría consecuencias que alarmarían a la sociedad en general, tal es el caso, del retraso en los proyectos hidroeléctricos.

Administrar la información de carácter confidencial no se traduce en ocultar información, sino en saber cómo difundirla de manera que los datos que sean conocidos por la sociedad, sean oficiales y no especulaciones.

Establecer contacto con los organismos del sector eléctrico y que este contacto sea de manera permanente. Comunicar oportunamente información que involucre a más empresas del sector eléctrico y cuando su actuar sea necesario para solventar problemas o apoyar iniciativas y proyectos de la corporación.

Se debe implementar en la corporación, una plataforma virtual a través de la cual los colaboradores tengan la posibilidad de conocer lo que sucede en la empresa, con los proyectos, los recursos destinados, las decisiones tomadas.

5. CONCLUSIÓN

Los riesgos se encuentran presentes en todas las actividades que realizamos, independientemente si se trata del ámbito laboral o personal.

La conciencia de la presencia de los riesgos a nivel corporativo, es un elemento que influye en la consecución de los objetivos.

A nivel internacional, el riesgo es un factor considerado al momento de diseñar un plan, iniciar un proyecto, comunicar información, empezar un negocio, plantear estrategias, por lo que desarrollan junto con sus ideas de negocio, un plan para tratar eventos que se susciten y que podrían repercutir de manera negativa en los objetivos, o, si representasen una oportunidad, también desarrollan un plan para aprovecharla.

Producto de la aplicación del modelo propuesto para gestión de riesgo de tecnología de la información y de todas las fases que lo comprende, se determinó que hay un factor que influye significativamente en la implementación de la gestión de riesgos en CELEC EP, este factor es el nivel de involucramiento y apoyo de la alta Gerencia.

Durante las entrevistas con los expertos, el criterio de que la alta gerencia no considera el riesgo como un elemento importante a tomar en cuenta, fue unánime, pues los riesgos se tratan en el momento en el que se materializan y, además, cada persona es la encargada de aplicar medidas de prevención y tratamiento de riesgos según su apreciación.

La utilización de tecnologías de la información en la ejecución de actividades diarias en la empresa es masiva, prácticamente no existen actividades en el que las tecnologías de la información no estén involucradas.

La identificación de los riesgos de tecnologías de la información, asociados a los procesos que tiene la empresa, permitió conocer que, dentro del grupo de expertos, existen personas que cuentan con conocimiento y que, aunque no existe un sistema formal de riesgos implementado, estas personas han establecido controles, lo que ha disminuido el impacto de la materialización de riesgos.

Una vez que se realizó la evaluación de los riesgos, se determina que los controles para el acceso a la información, son ineficaces, por lo que la restricción en el acceso, así como la creación de usuarios con sus respectivas contraseñas, sería una medida de control a aplicar así como también la compra de licencias de software utilizado en la empresa y la respectiva capacitación al personal para manejo de estos sistemas, a fin de que la empresa, sea capaz de solventar sus problemas, sin tener que recurrir a los proveedores frecuentemente, y éstos, no cuenten con acceso a la información y los sistema de la empresa permanentemente.

Dentro de los riesgos, las fallas que se generen en los sistemas de ventilación, afectaría directamente a la integridad y disponibilidad de los equipos que se encuentran en las

centrales. Las medidas a aplicar para prevenir la ocurrencia de este riesgo, es una adecuada planificación de los mantenimientos a los equipos.

La decisión de utilizar los principios y directrices de la ISO 31000, dentro del apartado que aborda los riesgos y oportunidades en la ISO 9001:2015, es porque la ISO 31000, es aplicable a cualquier riesgo, empresa, contexto; y, aunque el modelo propuesto tiene como objetivo gestionar riesgos de tecnología de la información, podría ser utilizado para gestionar otros riesgos en la corporación.

Se debe considerar, además, que mediante la ISO 9001:2015, dentro de su capítulo de riesgos, se abordan también las oportunidades, que, aunque no se determinó alguna en la fase de entrevistas, los factores político y económico, dada una situación particular, podrían convertirse en oportunidades.

CELEC EP, como ya se mencionó anteriormente, es una empresa pública y la gestión de riesgos, debería ser primordial, pues utiliza recursos públicos y además está al servicio de la sociedad. La incorporación de mecanismos, metodologías y sistemas que permitan gestionar los riesgos, así como la capacitación al personal en estas herramientas, proporciona un escenario de confianza, donde la posibilidad de alcanzar objetivos es mayor.

6. REFERENCIAS BIBLIOGRÁFICAS

27005, I. (31 de ENERO de 2014). SGSI. Obtenido de http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

AEC, A. E. (27 de Noviembre de 2017). AEC. Obtenido de https://www.aec.es/web/guest/centro-conocimiento/risk-it

Asamblea Nacional. (16 de Octubre de 2009). Asamblea Nacional. Obtenido de http://www.asambleanacional.gob.ec/es/leyes-aprobadas?leyes-aprobadas=All&title=Ley%20Org%C3%A1nica%20de&fecha=&page=3

Asamblea Nacional Constituyente de Ecuador . (20 de Octubre de 2008). Constitución de la República del Ecuador. Ecuador.

Baena-López, G. (2009). I+E Investigación Estratégica. Bogotá, Colombia: GABL Internacional Marketin, 2009.

Casares-San José, I. (2013). Proceso de Gestión de riesgos y seguros en las empresas. Madrid, España: Molinuevo, Gráficos, S.L.

CELEC. (1 de Septiembre de 2017). CELEC EP HIDROPAUTE. Obtenido de CELEC EP HIDROPAUTE: https://www.celec.gob.ec/hidropaute/ley-de-transparencia/11-espanol/perfil-corporativo/127-paute-integral.html

Chicano-Tejada, E. (2015). Auditoría de seguridad informática. Málaga: IC Editorial.

Contraloría General de Estado. (12 de Junio de 2002). Obtenido de http://www.contraloria.gob.ec/Normatividad/BaseLegal

Contraloría General del Estado. (2009). Normas de Control Interno. Ecuador.

Coronel, A. (2015). EOI. Obtenido de http://www.eoi.es/wiki/index.php/Gesti%C3%B3n_de_proyectos

ESTUPIÑÁN, R. (2006). Administración del Riesgo E.R.M y la Auditoría Interna. Bogotá.

EXCELLENCE, I. (Agosto de 2015). ww.pmg-ssi.com. Obtenido de http://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/

Instituto Ecuatoriano de Normalización. (Julio de 2014). Quito.

ISACA. (2012). COBIT 5 para la seguridad de la información.

ISO. (2015). Requisitos para los Sistemas de Gestión de la Calidad.

ISO. (31000: 2009). Recuperado el 29 de Noviembre de 2017, de https://www.iso.org/standard/43170.html

ISO. (9001: 2015). Sistema de gestión de la calidad.

ISOTools. (2017). Obtenido de https://www.isotools.org/about-us/

justicia, R. (27 de Noviembre de 2014). Centro de Seguridad Contra Incidentes Tecnológicos para 2015. El Telégrafo.

Marta Fernández. (octubre de 2016). www.ca.aenor.es. Obtenido de http://www.ca.aenor.es/documentos/certificacion/folletos/RevistaAENOR_ISO37001.pdf

Ministerio de Haciendas y Administraciones Públicas. (2006). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España.

NTC, I. 2. (2013). Gestión de la seguridad de la información.

NTC, I. 3. (2009). Gestión de riesgos - principios y directrices.

Piattini, M., & Del Peso, E. (2004). Auditoría Informática, un enfoque práctico. México: RA-MA 2004.

Rault, R., Schalkwijk, L., Acissi, Agé, M., Crocfer, N., Crocfer, R., . . . Lasson, S. (2015). Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa . Barcelona: ENI.

Rodríguez, F. (2012). Los empresarios no valoran la magnitud del riesgo informático. Líderes.

Serra, C. (2011). ISACA. Obtenido de ISACA: https://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf

SINNAPS. (2015). Obtenido de https://www.sinnaps.com/blog-gestion-proyectos/metodologia-cualitativa

Standarizacion, I. O. (2009).

ANEXOS

Anexo 1. Identificación del riesgo

#	Proceso	Objetivo del Proceso	Riesgo	Punto cítrico del proceso donde se identifica el riesgo	Causas	Consecuencias potenciales
1	Administrar contabilidad general	Brindar soporte a los usuarios de tecnologías de información y facilitar el crecimiento y la mejora continua del área de tecnología.	Colapso en las bases de datos	Gestión del Registro Contable	Fallas de Infraestructura Tecnológica	Información incompleta. Tiempo de reprocesos y riesgo de errores
2	Administrar la operación y la mejora continua de las tecnologías de información, comunicaciones y seguridad	Brindar soporte a los usuarios de tecnologías de información y facilitar el crecimiento y la mejora continua del área de tecnología.	Controles de seguridad ineficaces, personal no autorizado puede acceder a información confidencial, ocasionando perdida de disponibilidad de los sistemas, confidencialidad e integridad de la información	Administrar la Operación de Tics	Fallos de sistemas de ventilación	Afección a la integridad y disponibilidad de equipos. Daños en los discos duros
3	Administrar la operación y la mejora continua de las tecnologías de información, comunicaciones y seguridad	Brindar soporte a los usuarios de tecnologías de información y facilitar el crecimiento y la mejora continua del área de tecnología.	Controles ineficaces .en los accesos a información, esta puede ser mal utilizada, ocasionando reclamos y malestar del personal.	Administrar la Operación de Tic´s	Controles de seguridad para acceso a la información ineficaces	Perdida de disponibilidad de los sistemas, confidencialidad e integridad de la información

#	Proceso	Objetivo del Proceso	Riesgo	Punto cítrico del proceso donde se identifica el riesgo	Causas	Consecuencias potenciales
4	Administrar la operación y la mejora continua de las tecnologías de información, comunicaciones y seguridad	Brindar soporte a los usuarios de tecnologías de información y facilitar el crecimiento y la mejora continua del área de tecnología.	Diseños no adecuados, pueden afectar a la mantenibilidad (Central Mazar), lo que afectaría a la confiabilidad y disponibilidad de las centrales	Administrar la Operación de Tic´s	Falta de sistemas redundantes para derivar servicios críticos ante fallos en los sistemas primarios	Pérdida de disponibilidad, confidencialidad e integridad d la información.
5	Diseñar y entregar servicios de tecnologías de información, comunicaciones y seguridad	Controlar y administrar los registros contables y financieros, así como desarrollar e implementar lineamientos que soporten el proceso de elaboración y consolidación de los estados financieros de la Corporación.	Fallas de los sistemas de ventilación, puede existir sobrecalentamiento de equipos, que ocasionarían afección a la integridad y disponibilidad de los mismos	Administrar la Operación de Tic´s	Necesidades de software de parte de los usuarios no satisfechas por la organización	Existencia de software sin licencia. Problemas legales debido a software no autorizado
6	Administrar la operación y la mejora continua de las tecnologías de información, comunicaciones y seguridad	Controlar y administrar los registros contables y financieros, así como desarrollar e implementar lineamientos que soporten el proceso de elaboración y consolidación de los estados financieros de la Corporación.	Fallas en la Infraestructura tecnológica, podría presentarse pérdidas de información, ocasionando informes incompletos, reprocesos y errores	Administrar la Operación de Tic´s	Falta de seguridad en el acceso al data center.	Robo de información. Daño a la infraestructura tecnológica

#	Proceso	Objetivo del Proceso	Riesgo	Punto cítrico del proceso donde se identifica el riesgo	Causas	Consecuencias potenciales
7	Desarrollar el mantenimiento preventivo y predictivo	Controlar y administrar los registros contables y financieros, así como desarrollar e implementar lineamientos que soporten el proceso de elaboración y consolidación de los estados financieros de la Corporación.	Fallas en la Infraestructura tecnológica, podría presentarse pérdidas de información, ocasionando informes incompletos, reprocesos y errores	Ejecución del Mantenimiento	Existen especificaciones de calidad de los materiales que no pueden ser medidas o comprobadas directamente por parte de Hidropaute sobre los productos comprados. Productos o Servicios altamente especializados que tiene limitada oferta	.- Afecta a la confiabilidad y disponibilidad
8	Realizar estudios de proyectos de generación y transmisión	Definir y entregar los servicios hacía la operación de tecnologías de la información.	Fallos de los sistemas de aire de precisión, puede existir sobrecalentamiento de equipos, que ocasionarían afección a la integridad y disponibilidad de los mismos	Ejecución de Proyectos de Expansión	Nivel de incertidumbre relacionada con los estudios técnicos.	Afecciones en la calidad, tiempo y costo
9	Administrar contabilidad general	Desarrollar y mantener actualizados los estudios de proyectos de expansión de generación, transmisión y distribución necesarios para garantizar el abastecimiento de la demanda en condiciones de seguridad, confiabilidad y calidad del servicio de energía eléctrica.	Falta de seguridad en el data center, existiría accesos no autorizado a la infraestructura tecnológica, pudiendo ocasionar robo de información y/o daños a la infraestructura.	Gestión del Registro Contable	Fallas de Infraestructura Tecnológica	Información incompleta. Tiempo de reprocesos y riesgo de errores

#	Proceso	Objetivo del Proceso	Riesgo	Punto cítrico del proceso donde se identifica el riesgo	Causas	Consecuencias potenciales
10	Gestionar las relaciones laborales	Gestionar la relación con el talento humano, atendiendo oportunamente sus requerimientos y las situaciones de cumplimiento normativo, asegurando que este relacionamiento se lleve a cabo dentro del marco legal vigente.	Falta de sistemas redundantes que permitan derivar servicios críticos ante fallos en los sistemas primarios, ocasionaría la pérdida de servicios tecnológicos, impidiendo el desarrollo normal de las actividades de la empresa.	Gestión de Nómina, Reclutamiento y Selección de Personal.	Controles de acceso a la información ineficaces	1.-Reclamos 2.- Malestar interno 3.-Afectación a la Imagen de la Organización
11	Administrar almacenes	Gestionar los almacenes y ejecutar las operaciones logísticas sobre los bienes almacenados en las bodegas y depósitos de la Corporación.	Falta o deficiencia de materiales y repuestos críticos adquiridos, pueden causar fallas en las unidades de generación.	Bodega	Falta de actualización de infraestructura tecnológica	información contable imprecisa y decisiones no confiables
12	Administrar la operación y la mejora continua de las tecnologías de información, comunicaciones y seguridad	Programar y ejecutar las acciones de mantenimiento, a fin de asegurar las condiciones operativas de la infraestructura de generación, transmisión y distribución de energía eléctrica.	Insuficiencias en los estudios del proyecto puede generarse inconvenientes en la ejecución de la obra	Administrar la Operación de Tic´s	Fallos de sistemas de ventilación	Afección a la integridad y disponibilidad de equipos. Daños en los discos duros

#	Proceso	Objetivo del Proceso	Riesgo	Punto cítrico del proceso donde se identifica el riesgo	Causas	Consecuencias potenciales
13	Desarrollar el mantenimiento preventivo y predictivo	Programar y ejecutar las acciones de mantenimiento, a fin de asegurar las condiciones operativas de la infraestructura de generación, transmisión y distribución de energía eléctrica.	Necesidades no satisfechas de software, el personal instala en los equipos software no autorizados, ocasionando incumplimientos de la normativa legal.	Ejecución del Mantenimiento	Errores de Diseño de Centrales de Generación	Afecta a la confiabilidad y disponibilidad
14	Administrar contabilidad general	Brindar soporte a los usuarios de tecnologías de información y facilitar el crecimiento y la mejora continua del área de tecnología.	Vulnerabilidad de los controles y filtración de información confidencial, ocasionaría ingreso no autorizado al sistema, generando alteración de información	Gestión del Registro Contable	El sistema IFS podría tener ciertas vulnerabilidades. Inexistencia de alertas o políticas de salvaguarda de la información	Desvío de fondos, Fraude en la información. Filtración de información confidencial

Anexo 2. Análisis y Evaluación del Riesgo

#	RIESGO	PROBABILIDAD OCURRENCIA	NIVEL DE LA OCURRENCIA	IMPACTO	NIVEL DEL IMPACTO	EVALUACIÓN DEL RIESGO	NIVEL DE RIESGO INHERENTE
3	Controles ineficaces .en los accesos a información, esta puede ser mal utilizada, ocasionando reclamos y malestar del personal.	MUY ALTO	5	CATASTRÓFICO	5	25	EXTREMO
5	Fallas de los sistemas de ventilación, puede existir sobrecalentamiento de equipos, que ocasionarían afección a la integridad y disponibilidad de los mismos	MUY ALTO	5	CATASTRÓFICO	5	25	EXTREMO
14	Vulnerabilidad de los controles y filtración de información confidencial, ocasionaría ingreso no autorizado al sistema, generando alteración de información	MUY ALTO	5	CATASTRÓFICO	5	25	EXTREMO
7	Fallas en la Infraestructura tecnológica, podría presentarse pérdidas de información, ocasionando informes incompletos, reprocesos y errores	MEDIO	3	ALTO	4	12	ALTO
8	Fallos de los sistemas de aire de precisión, puede existir sobrecalentamiento de equipos, que ocasionarían afección a la integridad y disponibilidad de los mismos	ALTO	4	MODERADO	3	12	ALTO

#	RIESGO	PROBABILIDAD OCURRENCIA	NIVEL DE LA OCURRENCIA	IMPACTO	NIVEL DEL IMPACTO	EVALUACIÓN DEL RIESGO	NIVEL DE RIESGO INHERENTE
13	Necesidades no satisfechas de software, el personal instala en los equipos software no autorizados, ocasionando incumplimientos de la normativa legal.	MEDIO	3	ALTO	4	12	ALTO
1	Colapso en las bases de datos	BAJO	2	CATASTRÓFICO	5	10	ALTO
2	Controles de seguridad ineficaces, personal no autorizado puede acceder a información confidencial, ocasionando perdida de disponibilidad de los sistemas, confidencialidad e integridad de la información	BAJO	2	CATASTRÓFICO	5	10	ALTO
10	Falta de sistemas redundantes que permitan derivar servicios críticos ante fallos en los sistemas primarios, ocasionaría la pérdida de servicios tecnológicos, impidiendo el desarrollo normal de las actividades de la empresa.	BAJO	2	MODERADO	3	6	MODERADO
11	Falta o deficiencia de materiales y repuestos críticos adquiridos, pueden causar fallas en las unidades de generación.	BAJO	2	MODERADO	3	6	MODERADO
4	Diseños no adecuados, pueden afectar a la mantenibilidad (Central Mazar), lo que afectaría a la confiabilidad y disponibilidad de las centrales	BAJO	2	MODERADO	3	6	MODERADO

#	RIESGO	PROBABILIDAD OCURRENCIA	NIVEL DE LA OCURRENCIA	IMPACTO	NIVEL DEL IMPACTO	EVALUACIÓN DEL RIESGO	NIVEL DE RIESGO INHERENTE
9	Falta de seguridad en el data center, existiría accesos no autorizado a la infraestructura tecnológica, pudiendo ocasionar robo de información y/o daños a la infraestructura.	MUY BAJO	1	ALTO	4	4	MODERADO
12	Insuficiencias en los estudios del proyecto puede generarse inconvenientes en la ejecución de la obra	MUY BAJO	1	ALTO	4	4	MODERADO

Anexo 3. Valoración y Evaluación de los riesgos

#	Riesgo	Controles existentes	Tipo de Control	Valor asignado	Periodicidad del control	Valor asignado	Producto (Tipo x Periodicidad)	Eficacia del Control	Valoración del Control	Evaluación del Riesgo	Grado de exposición residual	Nivel de riesgo residual
1	Diseños no adecuados, pueden afectar a la mantenibilidad (Central Mazar), lo que afectaría a la confiabilidad y disponibilidad de las centrales	.-Rediseños .adecuaciones y mejoras -planes de mantenimiento -ingeniería de mantenimiento	PREVENTIVO	4	OCASIONAL	1	4	BAJA	2	6	3	BAJO
2	Vulnerabilidad de los controles y filtración de información confidencial, ocasionaría ingreso no autorizado al sistema, generando alteración de información	Los accesos al sistema están restringidos al personal autorizado (claves asignadas).	PREVENTIVO	4	PERIÓDICO	2	8	MEDIA	3	10	3	BAJO
3	Fallas en la Infraestructura tecnológica, podría presentarse pérdidas de información, ocasionando informes incompletos, reprocesos y errores	Respaldos de la información en el departamento de sistemas.	PREVENTIVO	4	OCASIONAL	1	4	BAJA	2	10	5	MODERADO

#	Riesgo	Controles existentes	Tipo de Control	Valor asignado	Periodicidad del control	Valor asignado	Producto (Tipo x Periodicidad)	Eficacia del Control	Valoración del Control	Evaluación del Riesgo	Grado de exposición residual	Nivel de riesgo residual
4	Fallos de los sistemas de aire de precisión, puede existir sobrecalentamiento de equipos, que ocasionarían afección a la integridad y disponibilidad de los mismos	Se ha implementado sistemas de aire de precisión	PREVENTIVO	4	PERMANENTE	3	12	ALTA	4	25	6	MODERADO
5	Controles de seguridad ineficaces, personal no autorizado puede acceder a información confidencial, ocasionando perdida de disponibilidad de los sistemas, confidencialidad e integridad de la información	Instalación de aplicativos de seguridad como firewall, rsfirewall, anti spam, etc.	PREVENTIVO	4	PERIÓDICO	2	8	MEDIA	4	25	6	MODERADO
6	Falta de sistemas redundantes que permitan derivar servicios críticos ante fallos en los sistemas primarios, ocasionaría la pérdida de servicios tecnológicos, impidiendo el desarrollo normal de las actividades de la empresa.	Redundancia y alta disponibilidad de equipos	PREVENTIVO	4	PERMANENTE	3	12	ALTA	4	12	3	BAJO
7	Necesidades no satisfechas de software, el personal instala en los equipos software no autorizados, ocasionando incumplimientos de la normativa legal.	Existen políticas de buen uso de la tecnología. Sanciones en caso de detectarse	PREVENTIVO	4	PERMANENTE	3	12	ALTA	4	12	3	BAJO

#	Riesgo	Controles existentes	Tipo de Control	Valor asignado	Periodicidad del control	Valor asignado	Producto (Tipo x Periodicidad)	Eficacia del Control	Valoración del Control	Evaluación del Riesgo	Grado de exposición residual	Nivel de riesgo residual
8	Falta de seguridad en el data center, existiría accesos no autorizado a la infraestructura tecnológica, pudiendo ocasionar robo de información y/o daños a la infraestructura.	Seguridad física de acceso. Monitoreo por cámaras	PREVENTIVO	4	PERMANENTE	3	12	ALTA	4	4	1	BAJO
9	Falta o deficiencia de materiales y repuestos críticos adquiridos, pueden causar fallas en las unidades de generación.	Plan anual de contrataciones. Adquisición en base a especificaciones técnicas basadas en normas Pruebas de recepción, de ser factible.	PREVENTIVO	4	PERMANENTE	3	12	ALTA	4	6	2	BAJO
10	Controles ineficaces .en los accesos a información, esta puede ser mal utilizada, ocasionando reclamos y malestar del personal.	Se labora con software que dispone de restricciones de acceso y calves personales. La información confidencial esta correctamente archivada y controlada Se firmó el acuerdo de confidencialidad según lo dispuesto en la norma técnica de seguridad de la información. Se socializa y gestiona el código de ética y conducta	PREVENTIVO	4	PERMANENTE	3	12	ALTA	4	6	2	BAJO

#	Riesgo	Controles existentes	Tipo de Control	Valor asignado	Periodicidad del control	Valor asignado	Producto (Tipo x Periodicidad)	Eficacia del Control	Valoración del Control	Evaluación del Riesgo	Grado de exposición residual	Nivel de riesgo residual
11	Colapso en las bases de datos	Uso de respaldo. Trabajo de recuperación de datos	PREVENTIVO	4	PERMANENTE	3	12	ALTA	4	4	1	BAJO
12	Insuficiencias en los estudios del proyecto puede generarse inconvenientes en la ejecución de la obra	Enfrentar técnicamente la eventualidad	CORRECTIVO	3	PERIÓDICO	2	6	BAJA	2	12	6	MODERADO
13	Fallas de los sistemas de ventilación, puede existir sobrecalentamiento de equipos, que ocasionarían afección a la integridad y disponibilidad de los mismos	Se ha implementado sistemas de aire de precisión	PREVENTIVO	4	PERMANENTE	3	12	ALTA	4	25	6	MODERADO

Anexo 4. Tratamiento de los riesgos

#	RIESGO	ESTRATEGIAS DE TRATAMIENTO	ACCIÓN DE TRATAMIENTO	TIEMPO DE IMPLEMENTACIÓN	RESPONSABLE	NOMBRE DEL INDICADOR	INDICADORES	METAS	EVIDENCIA DE CUMPLIMIENTO	RESPUESTA ANTE EMERGENCIA
1	Diseños no adecuados, pueden afectar a la mantenibilidad (Central Mazar), lo que afectaría a la confiabilidad y disponibilidad de las centrales	REDUCIR	Implementación de la metodología para la inclusión de mejoras. Elaboración del plan de mejoras.	1 año	Subgerente de Generación	Metodología de mejora implementada Plan de mejora definido.	Actividades Realizadas / Actividades Planificadas	100%	Informes del Área	Planificar y ejecutar adecuaciones y mejoras requeridas al equipo afectado
2	Vulnerabilidad de los controles y filtración de información confidencial, ocasionaría ingreso no autorizado al sistema, generando alteración de información	REDUCIR	Mejorar los sistemas de seguridad de la información ingresada.	1 año	Subgerente Financiero / Subgerente de Gestión Organizacional	Vulnerabilidades al mes	Sumatoria de vulnerabilidades al mes	0	Informes del Área	Activar investigaciones internas para determinar responsabilidades

#	RIESGO	ESTRATEGIAS DE TRATAMIENTO	ACCIÓN DE TRATAMIENTO	TIEMPO DE IMPLEMENTACIÓN	RESPONSABLE	NOMBRE DEL INDICADOR	INDICADORES	METAS	EVIDENCIA DE CUMPLIMIENTO	RESPUESTA ANTE EMERGENCIA
3	Fallas en la Infraestructura tecnológica, podría presentarse pérdidas de información, ocasionando informes incompletos, reprocesos y errores	REDUCIR	Maximizar la cantidad de información respaldada	1 año	Subgerente Financiero	Porcentaje de Información Respaldada	Megas de Información Respaldada / Total de Información en Servidores	80 %	Informes del Área	Actividades de Recuperación de Información
4	Fallos de los sistemas de aire de precisión, puede existir sobrecalentamiento de equipos, que ocasionarían afección a la integridad y disponibilidad de los mismos	TRANSFERIR	Contratar un seguro. Monitorear la eficacia del sistema de aire de precisión	1 año	Analista de Infraestructura y Help Desk - Cuenca Analista de Soluciones de Producción - Guarumales	Daños por Sobrecalentamiento de Equipos	Número de Casos Reportados	0	Informes del Área	Respaldo de información antes de sacar de línea el equipo afectado
5	Controles de seguridad ineficaces, personal no autorizado puede acceder a información confidencial, ocasionando perdida de disponibilidad de los sistemas, confidencialidad e integridad de la información	REDUCIR	Campañas de seguridad de la información	6 meses	Jefe de TIC´s	# de campañas de seguridad	# de campañas de seguridad de la información	2 campañas	Informes del Área	Analizar causa, repetir a responsables de ser necesario, informar a las autoridades y fuerza pública
6	Falta de sistemas redundantes que permitan derivar servicios críticos ante fallos en los sistemas primarios, ocasionaría la pérdida de servicios tecnológicos, impidiendo el desarrollo normal de las actividades de la empresa.	ASUMIR	Mantener Redundancia y alta disponibilidad de equipos	2 años	Jefe de TIC´s	Disponibilidad de Servicios TIC's	Porcentaje de disponibilidad de los servicios TIC	100 %	Informes del Área	Iniciar labores de Levantamiento de Sistemas o recuperación de servicios

#	RIESGO	ESTRATEGIAS DE TRATAMIENTO	ACCIÓN DE TRATAMIENTO	TIEMPO DE IMPLEMENTACIÓN	RESPONSABLE	NOMBRE DEL INDICADOR	INDICADORES	METAS	EVIDENCIA DE CUMPLIMIENTO	RESPUESTA ANTE EMERGENCIA
7	Necesidades no satisfechas de software, el personal instala en los equipos software no autorizados, ocasionando incumplimientos de la normativa legal.	ASUMIR	Existen políticas de buen uso de la tecnología. Sanciones en caso de detectarse. Se eliminó la administración de los usuarios en los equipos, siendo TIC los únicos que autorizan instalaciones	6 meses	Jefe de TIC´s	Instalaciones no autorizadas de software	Número de software no autorizados instalados	0	Informes del Área	Sancionar de acuerdo a política de uso de TIC´S
8	Falta de seguridad en el data center, existiría accesos no autorizado a la infraestructura tecnológica, pudiendo ocasionar robo de información y/o daños a la infraestructura.	ASUMIR	Mantener monitoreo por cámara de vigilancia	2 años	Jefe de TIC´s	Incumplimientos a la Política de Uso de Tecnología	Incumplimientos Presentados / Total Usuarios	0	Informes del Área	Sancionar de acuerdo a política de uso de TIC´S
9	Falta o deficiencia de materiales y repuestos críticos adquiridos, pueden causar fallas en las unidades de generación.	REDUCIR	Mantener Controles Existentes	N/A	N/A	N/A	N/A	N/A	N/A	Iniciar reemplazo inmediato del material defectuoso Revisión de Especificaciones, análisis de causa y lanzamiento de un nuevo proceso
10	Controles ineficaces .en los accesos a información, esta puede ser mal utilizada, ocasionando reclamos y malestar del personal.	EVITAR	Ninguno - riesgo cerrado	N/A	N/A	N/A	N/A	N/A	N/A	N/A

#	RIESGO	ESTRATEGIAS DE TRATAMIENTO	ACCIÓN DE TRATAMIENTO	TIEMPO DE IMPLEMENTACIÓN	RESPONSABLE	NOMBRE DEL INDICADOR	INDICADORES	METAS	EVIDENCIA DE CUMPLIMIENTO	RESPUESTA ANTE EMERGENCIA
11	Colapso en las bases de datos	REDUCIR	Maximizar la cantidad de información respaldada	2 años	Subgerente Administrativo	Porcentaje de Información Respaldada	Megas de Información Respaldada / Total de Información en Servidores	80 %	Informes del Área	Reportar a Tics vía servidesk
12	Insuficiencias en los estudios del proyecto puede generarse inconvenientes en la ejecución de la obra	REDUCIR	Plan de Acción Específica para cada Eventualidad	1 año	Subgerente de Expansión	Avance Físico del Proyecto de Expansión	Avance Físico Real / Avance Físico Planificado	95%	Informes del Área	Conformar equipo técnico experimentado para enfrentar la eventualidad
13	Fallas de los sistemas de ventilación, puede existir sobrecalentamiento de equipos, que ocasionarían afección a la integridad y disponibilidad de los mismos	TRANSFERIR	Contratación de un seguro. Monitorear la eficacia del sistema de aire de precisión	1 año	Jefe de TIC´s	Daños por Sobrecalentamiento de Equipos	Número de Casos Reportados	0	Informes del Área	Respaldo de información antes de sacar de línea el equipo afectado

Anexo 5. Monitoreo y Revisión

#	RIESGO	MECANISMOS DE VERIFICACIÓN	RESPONSABLES	PERIODICIDAD	RESULTADOS DE LA ACCIÓN (En base a los resultados de esta fase, el proceso deberá continuar nuevamente con la Fase 2 del sistema: Establecimiento del contexto)
1	Diseños no adecuados, pueden afectar a la mantenibilidad (Central Mazar), lo que afectaría a la confiabilidad y disponibilidad de las centrales	Rendición de Cuentas Mensual de Subgerentes a la Gerencia de Unidad de Negocio	Subgerente de Generación	Semestral	Por Verificar
2	Vulnerabilidad de los controles y filtración de información confidencial, ocasionaría ingreso no autorizado al sistema, generando alteración de información	Reunión de trabajo entre subgerentes involucrados.	Subgerente Financiero	Mensual	Por Verificar
3	Fallas en la Infraestructura tecnológica, podría presentarse pérdidas de información, ocasionando informes incompletos, reprocesos y errores	Reunión de trabajo entre subgerentes involucrados.	Subgerente Financiero	Semestral	Por Verificar

#	RIESGO	MECANISMOS DE VERIFICACIÓN	RESPONSABLES	PERIODICIDAD	RESULTADOS DE LA ACCIÓN (En base a los resultados de esta fase, el proceso deberá continuar nuevamente con la Fase 2 del sistema: Establecimiento del contexto)
4	Fallos de los sistemas de aire de precisión, puede existir sobrecalentamiento de equipos, que ocasionarían afección a la integridad y disponibilidad de los mismos	Reunión de trabajo entre subgerentes involucrados - Informe mensual de gestión de las áreas involucradas	Jefe de TIC´s	Mensual	No ha existido fallo
5	Controles de seguridad ineficaces, personal no autorizado puede acceder a información confidencial, ocasionando perdida de disponibilidad de los sistemas, confidencialidad e integridad de la información	Rendición de Cuentas Mensual de Subgerentes a la Gerencia de Unidad de Negocio	Jefe de Tic´s	Semestral	Por Verificar
6	Falta de sistemas redundantes que permitan derivar servicios críticos ante fallos en los sistemas primarios, ocasionaría la pérdida de servicios tecnológicos, impidiendo el desarrollo normal de las actividades de la empresa.	Rendición de Cuentas Mensual de Subgerentes a la Gerencia de Unidad de Negocio	Jefe de Tic´s	Semestral	Por Verificar

#	RIESGO	MECANISMOS DE VERIFICACIÓN	RESPONSABLES	PERIODICIDAD	RESULTADOS DE LA ACCIÓN (En base a los resultados de esta fase, el proceso deberá continuar nuevamente con la Fase 2 del sistema: Establecimiento del contexto)
7	Necesidades no satisfechas de software, el personal instala en los equipos software no autorizados, ocasionando incumplimientos de la normativa legal.	Rendición de Cuentas Mensual de Subgerentes a la Gerencia de Unidad de Negocio	Jefe de Tic´s	Semestral	Por Verificar
8	Falta de seguridad en el data center, existiría accesos no autorizado a la infraestructura tecnológica, pudiendo ocasionar robo de información y/o daños a la infraestructura.	Rendición de Cuentas Mensual de Subgerentes a la Gerencia de Unidad de Negocio	Jefe de Tic´s	Semestral	Por Verificar
9	Falta o deficiencia de materiales y repuestos críticos adquiridos, pueden causar fallas en las unidades de generación.	Rendición de Cuentas Mensual de Subgerentes a la Gerencia de Unidad de Negocio	Subgerente de Generación	Semestral	Por Verificar

#	RIESGO	MECANISMOS DE VERIFICACIÓN	RESPONSABLES	PERIODICIDAD	RESULTADOS DE LA ACCIÓN (En base a los resultados de esta fase, el proceso deberá continuar nuevamente con la Fase 2 del sistema: Establecimiento del contexto)
10	Controles ineficaces .en los accesos a información, esta puede ser mal utilizada, ocasionando reclamos y malestar del personal.	Se considera riesgo cerrado			
11	Colapso en las bases de datos	Rendición de Cuentas Mensual de Subgerentes a la Gerencia de Unidad de Negocio	Subgerente Administrativo	Semestral	Por Verificar
12	Insuficiencias en los estudios del proyecto puede generarse inconvenientes en la ejecución de la obra	Rendición de Cuentas Mensual de Subgerentes a la Gerencia de Unidad de Negocio	Subgerente de Expansión	Semestral	Por Verificar

#	RIESGO	MECANISMOS DE VERIFICACIÓN	RESPONSABLES	PERIODICIDAD	RESULTADOS DE LA ACCIÓN (En base a los resultados de esta fase, el proceso deberá continuar nuevamente con la Fase 2 del sistema: Establecimiento del contexto)
13	Fallas de los sistemas de ventilación, puede existir sobrecalentamiento de equipos, que ocasionarían afección a la integridad y disponibilidad de los mismos	Rendición de Cuentas Mensual de Subgerentes a la Gerencia de Unidad de Negocio	Jefe de Tic´s	Semestral	Por Verificar