UNIVERSIDAD NACIONAL PEDRO HENRÍQUEZ UREÑA
VICERRECTORÍA DE POSTGRADO Y EDUCACIÓN CONTINUADA
Escuela de Postgrado

ELABORACIÓN PROYECTO PLAN DE CONTINUIDAD DE NEGOCIO BASADOS EN LA NORMA ISO 22301:2019, ORGANISMO COORDINADOR DEL SISTEMA ELÉCTRICO NACIONAL INTERCONECTADO DE LA REPÚBLICA DOMINICANA DEL AÑO 2021.

SUSTENTANTES

FERNANDO AUGUSTO BERAS THOMAS
HEINAR ADALBERTO NOVAS PIÑA

Para la obtención del grado de Magíster
En Gerencia de Proyectos

ASESORES
Dr. Enrique Cambier M.
Ing. Rafael Ruiz

Santo Domingo, D.N., República Dominicana
Julio 2021

Tabla de Contenido

Lista de tablas

Lista de Figuras

UNPHU
Universidad Nacional
Pedro Henríquez Ureña

Vicerrectoría de Postgrado
y Educación Continuada

Carta Autorización Presentación de Tesis

YO, **Dr. Enrique Ernesto Cambier M.**, profesor(a) de la Escuela de Postgrado de la Universidad Pedro Henríquez Ureña, por medio de la presente hago constar que la tesis titulada: **Elaboración proyecto plan de continuidad de negocio basados en la norma ISO 22301:2019, Organismo Coordinador del Sistema Eléctrico Nacional Interconectado de la República Dominicana del año 2021.** elaborada por: **Fernando Augusto Beras Thomas (fb19-0529), Heinar Adalberto Novas Piña (hn19-0107)**, bajo mi asesoría, reúne todas las condiciones exigibles para ser presentada y defendida públicamente, considerando la relevancia del tema como el procedimiento metodológico utilizado: revisión teórica adecuada, contextualización, definición de objetivos y estructuración de los datos pertinentes a la naturaleza de la información recogida, así como las conclusiones aportadas.

En consecuencia, de ello, en calidad de asesor y garante del trabajo realizado, siguiendo las normativas del Reglamento de Tesis de Postgrado, manifiesto mi acuerdo para que sea autorizada su presentación.

Declaración que se emite en Santo Domingo, República Dominicana, a los 16 días del mes de julio del 2021.

Dr. Enrique Ernesto Cambier M.

UNPHU
Universidad Nacional
Pedro Henríquez Ureña

Vicerrectoría de Postgrado
y Educación Continuada

Carta Autorización Presentación de Tesis

YO, **Rafael Ruiz.**, profesor(a) de la Escuela de Postgrado de la Universidad Pedro Henríquez Ureña, por medio de la presente hago constar que la tesis titulada: **Elaboración proyecto plan de continuidad de negocio basados en la norma ISO 22301:2019, Organismo Coordinador del Sistema Eléctrico Nacional Interconectado de la República Dominicana del año 2021.** elaborada por: **Fernando Augusto Beras Thomas (fb19-0529), Heinar Adalberto Novas Piña (hn19-0107)**, bajo mi asesoría, reúne todas las condiciones exigibles para ser presentada y defendida públicamente, considerando la relevancia del tema como el procedimiento metodológico utilizado: revisión teórica adecuada, contextualización, definición de objetivos y estructuración de los datos pertinentes a la naturaleza de la información recogida, así como las conclusiones aportadas.

En consecuencia, de ello, en calidad de asesor y garante del trabajo realizado, siguiendo las normativas del Reglamento de Tesis de Postgrado, manifiesto mi acuerdo para que sea autorizada su presentación.

Declaración que se emite en Santo Domingo, República Dominicana, a los 21 días del mes de julio del 2021.

Ing. Rafael Ruiz

Declaración De Autor De Obra Intelectual Original

Fernando Augusto Beras Thomas, cédula de identidad y registro electoral **001-1892264-0** y **Heinar Adalberto Novas Piña,** cédula de identidad y registro electoral **223-0062649-0** Declaramos: Ser los autores de la tesis que lleva por Título elaboración proyecto plan de continuidad de negocio basados en la norma ISO 22301:2019, organismo coordinador del sistema eléctrico nacional interconectado de la república dominicana del año 2021**,** asesorada por el Dr. Enrique Cambier y el Ing. Rafael Ruiz quien presentó a la Escuela de Graduados, para que sea defendida y evaluada en sesión pública.

Que la tesis es una obra original. Además, puede ser libremente consultable.

Que me consta que una vez la tesis haya sido defendida y aprobada, su divulgación se realizará bajo licencia de la Universidad Nacional Pedro Henríquez Ureña.

Que el contenido de la tesis y su publicación no infringe derechos de propiedad intelectual, industrial, secreto comercial o cualquier otro derecho de terceros, por lo que exonero a la Universidad Nacional Pedro Henríquez Ureña, de cualquier obligación o responsabilidad ante cualquier acción legal que se pueda suscitar derivada de la obra o de su publicación.

Estos datos no vulneran derechos de terceros y por lo tanto asumo cualquier responsabilidad que se pueda derivar de las mismas y de su publicación, como constancia, firmamos el presente documento.

Santo Domingo DN, República Dominicana,

El día 15 del mes de julio del año 2021.

Agradecimientos

Gracias a los compañeros de estudio de la maestría, fueron un gran soporte para la misma, en especial al Ing. Rafael Correa. A Heinar Novas mi compañero de tesis quien nos hemos apoyado mutuamente para poder culminar nuestra investigación.

Por último y no menos importante a nuestros asesores el Dr. Enrique Cambier y el profesor Rafael Ruiz, quienes nos guiaron durante este trayecto para la culminación exitosa de nuestra tesis. Y a Universidad Pedro Henríquez Ureña, por suministrar los recursos necesarios para poder tomar las clases aun en pandemia.

Fernando Beras

Gracias a los asesores Dr. Enrique Cambier M. e Ing. Rafael Ruiz, por asumir el reto y tener la disposición de colaborar en este proyecto.

Gracias a mi compañero de este hermoso proyecto Fernando Beras, por acompañarme y dedicar parte de su tiempo en la elaboración de este proyecto.

Al cuerpo docente y compañero de estudio de la maestría en Gerencia de Proyecto del periodo 2019-2020, por contribuir su granito de arena.

Al Organismo Coordinador, por facilitar todas las informaciones requerida y apoyo en la culminación de este proyecto.

Heinar Novas

Dedicatoria

Dedico mi trabajo de grado a mis padres por su apoyo incondicional en mi crecimiento académico. A mi novia, por siempre estar ahí y apoyarme en la realización de esta tesis.

Y para mis compañeros de tesis quienes formaron parte de mi crecimiento educativo durante 2 años y nos apoyamos mutuamente.

Fernando Beras

A mis padres, abuela paterna, esposa e hijos, por tener la paciencia y entender del tiempo ausente en algunos momentos para poder avanzar y finalizar este proyecto.

A todas las personas que de una u otra manera han tenido miedo de dar el primer paso para arrancar este viaje, anímate y no tenga miedo.

Heinar Novas

Resumen

En la actualidad, las empresas en todo el mundo han experimentado diferentes eventos que le generaron pérdidas financieras y no financiera, por tal razón se han visto en la necesidad contratar un tercero para identificar y definir diferentes estrategias que le ayude con la continuidad de negocio. La finalidad de esta investigación es la elaboración de un Plan de Continuidad de Negocio para el Organismo Coordinador del Sistema Eléctrico Nacional Interconectado de la República Dominicana, basándose en la Norma ISO 22301: 2019, para lo cual es necesario identificar los procesos, determinar el nivel de impacto en caso de interrupción, identificar los riesgos que puedan generar las interrupciones en la organización y plasmar estrategias para definir los procesos que debe poseer el plan de continuidad de negocio. Los procesos que toca el plan de continuidad del negocio deben estar basados en los puntos neurálgicos del organismo coordinador del sistema eléctrico, como son el espacio de trabajo, los sistemas de tecnología utilizados, los recursos utilizados y los procesos del negocio. La metodología empleada fue la metodología holística que genera una visión integral de la diversidad del conocimiento, permitiendo evidenciar la vigencia de las ideas. Finalmente, el establecimiento de planes de continuidad permite contar con procedimientos que se detallan y trabajan de manera continúa recuperando la operatividad de los procesos críticos de la organización en un tiempo apropiado, que no genere pérdidas financieras para la empresa, evitar sanciones regulatorias, defender los objetivos estratégicos de la institución y sobre todo problemas en cuanto a su reputación.

Palabras clave: Norma, Gestión, Prevención de Riesgo, Planificación de Proyecto.

Abstract

Currently, companies around the world have experienced different events that generated financial and non-financial losses, for this reason they have found it necessary to hire a third party to identify and define different strategies to help them with business continuity. The purpose of this research is the development of a Business Continuity Plan for the Organismo Coordinador del Sistema Eléctrico Nacional Interconectado de la República Dominicana, based on the ISO 22301: 2019 Standard, for which it is necessary to identify the processes, determine the level of impact in case of interruption, identify the risks that the interruptions may generate in the organization and shape strategies to define the processes that the business continuity plan must have. The processes that the business continuity plan touches must be based on the neuralgic points of the Organismo Coordinador del Sistema Eléctrico, such as the workspace, the technology systems used, the resources used and the business processes. The methodology used was the holistic methodology that generates a comprehensive vision of the diversity of knowledge, allowing evidence of the validity of ideas. Finally, the establishment of continuity plans allows to have procedures that are detailed and work continuously, recovering the operation of the critical processes of the organization in an appropriate time, which does not generate financial losses for the company, avoid regulatory sanctions, defend the strategic objectives of the institution and especially problems regarding its reputation.

Keywords: Norm, Management, Risk Prevention, Project Planning.

Parte 1. Marco Introductorio

Introducción

Desde los inicios de 2000, la continuidad del negocio se ha vuelto la base de las organizaciones, debido a los diferentes eventos ocurridos en las últimas dos décadas. Tales eventos han dejado un remanente en la historia, por ejemplo, en el 2010 la compañía Toyota lanzo vehículos al mercado que tenían defectos de fábrica, el mismo ocasiono que 4 personas murieran en un accidente de tránsito. No existió una comunicación de Toyota a sus consumidores, incluso trataron de tapar la situación. Esto ocasiono una crisis de reputación dejándoles en perdida más de 2000 millones de euros.

Otro ejemplo más reciente, en los inicios del 2020 el mundo completo se vio afectado por la pandemia de origen chino Covid-19. Las empresas se vieron afectadas ya que el recurso humano es vulnerable al virus, ocasionando interrupción en las operaciones, ya sea por la misma enfermedad o por las medidas de cierre de los gobiernos. "Estas organizaciones dependen de sus recursos y si alguno de ellos se ve afectado, esto significaría una interrupción de las operaciones. Por lo tanto, debe existir una cultura de resiliencia en la cual se preocupen por dichos recursos" (Minolli, 2005). "Para las organizaciones siempre han existido recursos que ayudan al cumplimiento de sus objetivos, como lo son sus empleados, procesos, la información, proveedores, telecomunicaciones, tecnología, entre otros" (Chiavenato, 2001).

Las interrupciones de los procesos pueden causar un sin número de impactos a la empresa, desde un impacto financiero, impacto reputacional, hasta multas y sanciones. Lamentablemente estos eventos se presentan de imprevisto. Actualmente el Organismo Coordinador del Sistema Eléctrico Nacional Interconectado de la República Dominicana carece de un Plan de Continuidad de Negocio, los cual es muy común en las empresas de República Dominicana.

Como respuesta a esto existe la Norma ISO 22301:2019 que es el Sistema de Gestión de Continuidad de Negocio, el mismo da las pautas para la creación de un Plan de Continuidad de Negocio. El Plan de Continuidad de Negocio ayuda a asegurar la continuidad de las operaciones mediante procedimientos alternos. Considerando las condiciones propias de la organización y la posibilidad brindada por la Norma mencionada.

Capítulo 1: Presentación del problema

1.1 Planteamiento del problema.

El Organismo Coordinador del Sistema Eléctrico fue creado el 29 de octubre de 1998 mediante la Resolución No. 235 de la Secretaría de Estado de Industria y Comercio. Desde entonces el Organismo Coordinador del Sistema Eléctrico carece de un plan de continuidad de negocio, situación por la cual los impactos, tanto estratégicos como regulatorios, operativos, reputacionales, sociales y de recursos humanos han sufrido interrupciones que generan problemas en el quehacer misional de la empresa.

En octubre del 2019 hubo un corte de energía eléctrica debido a inconvenientes en el tendido eléctrico, al encender la planta eléctrica de contingencia que suministraría la energía para proseguir con las operaciones, esta se encontraba inservible. Debido al largo tiempo de resolución, se procedió a apagar un sin número de equipos tecnológicos, así interrumpiendo las operaciones y causando retrasos.

En el año 2020, se produjo un inconveniente con la página web, la cual es utilizada por los asociados para subir las informaciones pertinentes. Este problema fue causado por un fallo con el suplidor del servicio web y necesitó de bastantes horas para su solución. Esto evidentemente causó descontentos de parte de los asociados y de diferentes quejas. Esta página web es muy sensible debido a que si no está disponible para los asociados esto le podría causar pérdida millonaria por tardanzas en sus declaraciones de los servicios. Es por esto surge la necesidad de establecer un plan de continuidad de negocio en el Organismo Coordinador.

1.2 Delimitación del problema.

El Organismo Coordinador del Sistema Eléctrico tiene como visión ser reconocida en el sector eléctrico latinoamericano como una institución de excelencia operacional, por lo que necesita incorporar mejores prácticas para garantizar la continuidad de las operaciones,

preservar la integridad del personal, las instalaciones, los equipos y la información que maneja la organización.

Si bien el cumplimiento de la misión organizacional se encuentra ampliamente relacionada con la calidad, es preciso que la organización cuente con un plan de continuidad de negocio a partir de 2021, que le permita no solo prestar el servicio de calidad sino también garantizar la realización de las operaciones organizacionales día a día, lo que implica necesariamente la puesta en marcha de un plan de continuidad.

Ante la falta de desarrollo de un plan de continuidad específicamente para la organización es necesario plantear la presente investigación tiene la intención de realizar el diseño de este basándose en la Norma ISO 22301 del 2019, buscando el fortalecimiento de los lineamientos y procedimientos para garantizar la prestación de los servicios a los Agentes del Mercado Eléctrico Mayorista, así como también impulsar el restablecimiento de dichos servicios considerando posibles contingencias.

1.3 Preguntas de Investigación.

¿Cómo se puede mejorar la continuidad de las operaciones del Organismo Coordinador del Sistema Eléctrico Nacional Interconectado de la Republica Dominicana?

¿Qué tan desarrollado se encuentra la continuidad de negocio en el Organismo Coordinador del Sistema Eléctrico Nacional Interconectado de la Republica Dominicana?

¿Qué valor agrega un plan de continuidad de negocio al Organismo Coordinador del Sistema Eléctrico Nacional Interconectado de la Republica Dominicana?

1.4 Objetivos de la Investigación.

1.4.1 Objetivo General

Elaborar un Plan de Continuidad de Negocio para el Organismo Coordinador del Sistema Eléctrico Nacional Interconectado de la República Dominicana, basándose en la Norma ISO 22301:2019.

1.4.2 Objetivo Específicos

Identificar los impactos que puedan generar interrupción sobre los procesos y servicios del Organismo Coordinador del Sistema Eléctrico Nacional.

Identificar los riesgos de continuidad del Organismo Coordinador del Sistema Eléctrico Nacional.

Definir los procesos que debe poseer el plan de continuidad del negocio.

Parte 2. Marco Teórico

Capítulo 2: Norma ISO

2.1 Organización Internacional de Normalización (ISO).

La norma ISO (Organización Internacional de Normalización) son documentos que ayudan a las organizaciones a alcanzar la calidad deseada de sus productos y/o servicios y al mismo tiempo ayudan a cumplir los objetivos de la organización. También permite reducir costos, aumentar la productividad y reducción de errores en los procesos.

Se creó en el año 1946 con la presencia de 64 representantes delegados provenientes de 25 países. Esta reunión tuvo cita en Londres, Inglaterra en la sede del Instituto de Ingenieros Civiles. Estas personas decidieron adentrarse en el proyecto de creación de una organización cuya finalidad sería facilitar una unificación en normas de

industrialización y una mejora en la coordinación internacional de empresas (Riera & et al., 2018).

La organización Internacional de Normalización fue creada en 1947 y es una empresa sin fines de lucro, con el objetivo de promover entre las empresas del mundo el desarrollo y aplicación de las normas estandarizadas que ofrece y sean respetadas a nivel internacional. Todo es posible gracias a las herramientas que ofrece la organización, que facilitan la estandarización y garantizan la calidad de los productos, bienes o servicios brindados por la organización. "En el momento actual la organización se encuentra constituida por 180 comités técnicos y las actividades técnicas se encuentran descentralizadas en unos 2700 comités, subcomité, y grupos de trabajo" (Cordero López & Nuñez Rodenas, 2020).

2.2. Norma ISO 22301:2019

La norma ISO 22301:2019 especifica los requisitos para conformar el sistema de gestión de continuidad del negocio, otorgando a las organizaciones las herramientas necesarias para que el negocio se encuentre bajos los procesos estandarizados que la ISO 22301 ofrece. Al cumplir con los requisitos, la empresa se protege ante incidentes disruptivos, así como reducir la probabilidad de ocurrencia y estar preparado contra ellos y recuperarse de ellos cuando se presentan. "Esta norma internacional sobre la gestión de la continuidad del negocio especifica los requisitos para la planificación, el establecimiento, la implantación, la operación, la supervisión, la revisión, el mantenimiento y la mejora continua de un sistema de gestión documentado" (Sotres, 2012).

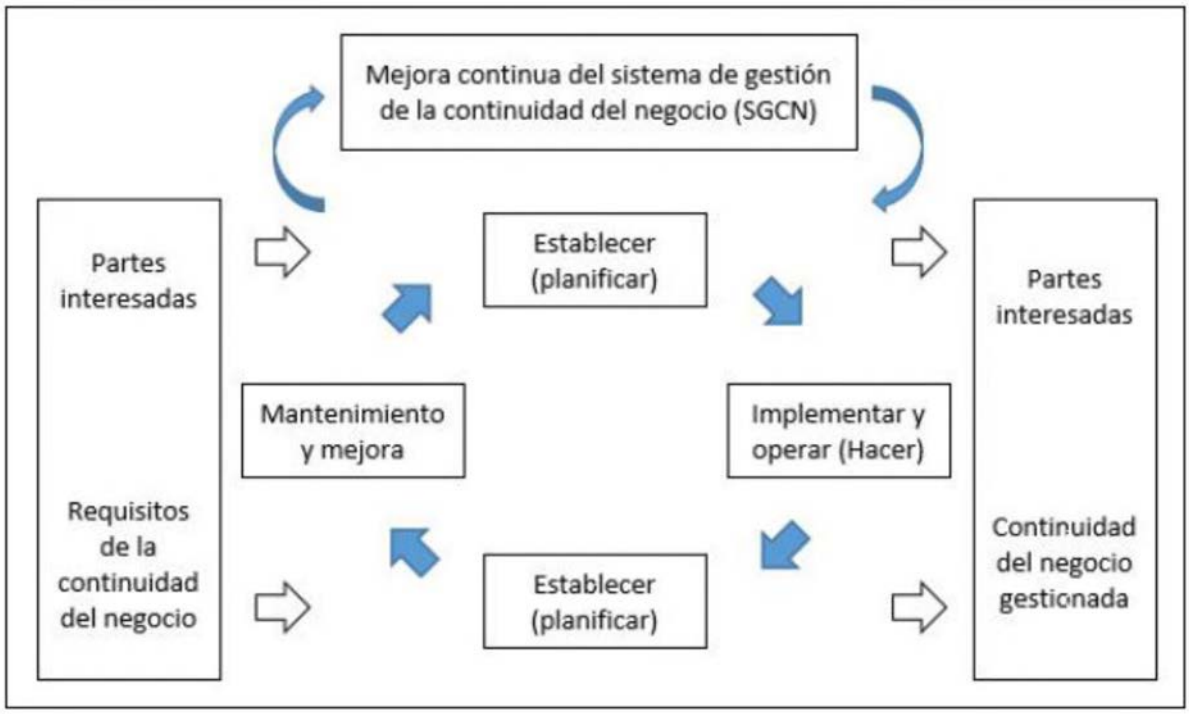
El Sistema de Gestión de Continuidad del Negocio utiliza un modelo muy reconocido en las normas internacionales, planificar-hacer-verificar-actuar. Esta metodología abarca por completo lo que es el modo de operar de la continuidad del negocio en una empresa. Esta metodología se puede implementar para todas las partes que conforma el SGCN. "La norma ISO 22301 aplica el modelo "Planificar-Hacer-Verificar-Actuar" conocido por sus siglas en

inglés PDCA (Plan-Do-Check-Act) para planificar, establecer, implantar, operar, supervisar, revisar, mantener, y mejorar de manera continua la eficacia del SGCN de una organización" (Sotres, 2012). Vale la pena mencionar que estos pasos iniciales, se ven complementados de manera consistente en la norma, que permiten proceder a la implementación del plan de continuidad, estos se ven analizados en la siguiente figura:

Figura 1,

Modelo PDCA.

Fuente: ISO 22301:2019



2.3 Alcance

Los requisitos especificados en esta norma son genéricos y son aplicables a todas las organizaciones, independientemente del tipo, tamaño y naturaleza. El grado de aplicación de estos requisitos depende la complejidad del entorno operativo de la organización. El alcance de la norma "específica los requisitos para implementar, mantener y mejorar un sistema de

gestión para proteger, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de eventos disruptivos cuando surjan" (INTECO, 2021).

2.4 Mejorías esperadas con la aplicación de la Norma ISO 22301

La implementación de la norma ISO 22301 ha traído beneficios para las organizaciones, lo que les permite prepararse para enfrentar situaciones previsibles e impredecibles, ayudando así a reducir los riesgos antes, durante y después de los accidentes. Adicionalmente esta norma enseña a las organizaciones a priorizar sus procesos y actividades, es decir, en caso de interrupciones generales las empresas sabrán que procesos o sistemas tecnológicos deben recuperar primero, esto depende de la criticidad e impacto que ocasionen los mismos. Por lo tanto, ayudara a la reducción de las pérdidas financieras como no financieras de la organización.

Se ha demostrado que la implementación de la norma 22301 en su versión anterior lograba generar una mejora de casi el 60% en la previsibilidad ante procesos disruptivos, desde este punto de vista se encuentra que la implementación de la norma facilita el cumplimiento regulatorio. Al tener una estructura o base de la continuidad del negocio, permite a las organizaciones tomas decisiones precisas sobre el contexto al que se enfrenta.

> Esta norma permite la identificación de recursos claves, como: el personal, sistemas tecnológicos y suplidores. Y no menos importante, poco a poco se va llevando la cultura de la continuidad del negocio a cada individuo de la organización, lo que provoca que cada uno de ellos se sienta identificado y progresivamente la continuidad del negocio sea parte del día a día (Sarabia (2015).

Capítulo 3: Continuidad del Negocio.

3.1. Historia de la Continuidad del Negocio

La continuidad del negocio empezó a tener notoriedad a los inicios del 1970, debido a que las empresas empezaron a depender de sistemas computarizados para realizar los procesos. Los sistemas computarizados tenían vulnerabilidades, que es caso de salir de servicio, esto interrumpía los procesos de la organización. Con esto se creó los primeros centros de cómputos alternos, esto ayudaba a las empresas a continuar las operaciones aun el centro de cómputo propia se encentre interrumpido.

> Cuando se analiza la continuidad del negocio es preciso hacer alusión al término recuperación ante desastres (disaster recovery) el cual es desarrollado inicialmente en los años 70´s, a partir de que los administradores de centros de cómputo comenzaron a reconocer la dependencia de sus organizaciones con sus sistemas computarizados. En aquella época, la mayoría de los sistemas eran procesos en lote que corrían en grandes computadoras centrales o mainframes, los cuales en ocasiones podían estar caídos por varios días antes de que se produzcan daños significativos a la organización, (Bussiness Continuity (2012).

La continuidad del negocio es la forma que tienen las empresas de mantener funcionando los procesos esenciales tras una interrupción. Cumplir con esto asegura a la empresa una menor perdida financieras y reputacional ante estos eventos de disrupción, aumenta la resiliencia de la empresa al recuperarse con mayor facilidad y rapidez. La continuidad del negocio otorga a las empresas medios alternos para realizar los procesos.

> Para el caso la continuidad de negocio se reconoce como un precepto consistente al interior de la Norma ISO 22301, bajo la explicación de otros conceptos. La norma en cuestión alude que esta se reconoce como la capacidad que tiene la organización para

continuar con la entrega de productos o la prestación de servicios a niveles aceptables, luego de la existencia de un evento perjudicial. (ISO 22301, 2012).

Adicionalmente se encuentra que el sistema de gestión de continuidad del negocio es una parte del sistema general de gestión que establece, implementa, opera, monitorea, revisa, mantiene y mejora la continuidad del negocio. El sistema de gestión incluye adicionalmente una estructura organizacional, diferentes actividades de planificación, responsabilidades, procedimientos, procesos y recursos.

> En efecto el sistema de continuidad del negocio se estructura fácticamente y con la posibilidad de aplicación en un plan de continuidad de negocio, en el cual existen procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a nivel predefinido de operación debido a la interrupción. Normalmente, ello incluye recursos, servicios y actividades necesarias para garantizar la continuidad de las funciones críticas del negocio (ISO 22301, 2019).

3.2. Análisis de riesgo

Cabe considerar que dentro de un negocio o empresa debe realizarse la identificación del riesgo la cual se inicia determinando las causas, con base en los factores internos y/o externos analizados para la organización y que pueden afectar el logro de los objetivos. La identificación de los riesgos a los que se expone una empresa del sector de la construcción permite analizarlos y tomar acciones para la recuperación luego de ocurrido un evento inesperado que pueda interrumpir la prestación de los servicios.

> Se reconoce que la evaluación y control de los riesgos tiene como adición la identificación de las amenazas que pueden presentarse tanto internas como externas, incluyendo las concentraciones de riesgos, que pueden causar la interrupción o pérdida de las actividades críticas de la organización, así como la probabilidad o frecuencia de que ocurra una amenaza (Ángel Torres y Velasco Galeano) (2014).

Al inicio de estos procesos se encuentra presente el análisis del impacto, que tiene como intención identificar y priorizar los componentes de un sistema de información correlacionándolos con la actividad misional de la empresa, en donde el negocio se soporta, ocupando esta información para caracterizar el impacto en los procesos, en el caso de que el sistema no estuviera disponible.

> El análisis de riesgos se reconoce como relevante precisamente porque los entornos globalizados representan riesgos mucho más complejos debido a la cantidad de paradigmas existentes en las operaciones, de ahí que este proceso permita mitigar en buena medida la posibilidad de materializar las amenazas que impacten el negocio, implementando mecanismos como procesos de gestión de continuidad del negocio (Gonzáles (2015).

Los elementos para el modelamiento de los sistemas de continuidad de negocio es precisamente la correcta elaboración de un análisis de impacto, precisamente porque es en este en donde se determinan los procesos críticos para el negocio y las dependencias que son necesarias para continuar brindando los servicios que son aceptables a un buen nivel.

3.3. Plan de Continuidad del Negocio

El plan de continuidad del negocio es el documento base para la gestión de la continuidad del negocio, dentro se recopilan las acciones que debe tomar la organización para recuperar las operaciones lo más rápido posible y reducir los impactos que podría generar el incidente de interrupción. "Procedimientos documentados que guía a las organizaciones a responder, recuperar, resumir, y restaurar a un nivel pre determinado las operaciones después de un incidente" (ISO 22301, 2019).

Para crear el plan de continuidad del negocio hay que tener claro el propósito, alcance y usuario, es decir, cual es el objetivo del mismo, ver qué área se verán afectadas y el personal que debe conocer de este plan. Si la empresa cuenta con un sistema de gestión continuidad del

negocio robusto, el plan debe incluir los documentos a la cual está vinculado, como las políticas de continuidad del negocio, el análisis de impacto del negocio, análisis de riesgo y estrategias de continuidad.

El plan debe contar con roles y responsabilidades, determinando las personas encargadas de gestionar los incidentes, dependiendo el tipo de incidente. Dentro debe contar con los contactos claves en caso de una eventualidad y tener los activadores claros para saber cuándo un incidente puede causar una interrupción en las operaciones, al igual de cuándo debe volver a la normalidad cuando acabe el incidente.

El plan de continuidad debe contar con la contingencia de espacios de trabajo alternos en caso que las instalaciones se vean comprometidas. Se tener una estrategia para recuperación de las operaciones de la empresa, así como las estrategias para recuperar los activos y sistemas tecnológicos.

Capítulo 4: Gestión del Proyecto

4.1. Acta Constitutiva

El Acta de Constitución viene a definir el alcance, los objetivos y participantes del proyecto y al mismo tiempo dar una visión preliminar de los roles y responsabilidades, de los objetivos, de los interesados y define la autoridad del Gerente de Proyecto. Este documento es la base crucial del proyecto y es expedido y firmado por el Patrocinador.

Tabla 1,

Acta Constitutiva

Fuente: Elaboración propia

ACTA CONSTITUTIVA	
Título del Proyecto:	
Elaboración Proyecto Plan de Continuidad de Negocio Basado en la Norma ISO 22301:2019, Organismo Coordinador Del Sistema Eléctrico Interconectado de la República Dominicana del Año 2021	
Inicio: 15 de diciembre 2020	**Fin:** 31 de mayo 2021
Director: Ing. Fernando Beras	
Patrocinador: Manuel López San Pablo	
Nivel de autoridad de patrocinador: Aprobar cambios en cronogramas y presupuestos.	
Caso de negocio: El proyecto se está realizando debido a que se identificó una oportunidad de mejora en la continuidad de las operaciones, debido a que no existe un plan de continuidad de negocio que mitigue las posibles interrupciones. El plan de continuidad esta alineado al cumplimiento de los objetivos estratégico del Organismo Coordinador.	
Inversión: RD$ 2.4 MM +- 5%	
Recursos: Recursos humanos asignados de acuerdo con las decisiones del director del proyecto. El idioma oficial será el español.	
Alcance y Objetivos:	
Alcance:	
Se desea elaborar un Plan de Continuidad de Negocio tomando en cuenta el levantamiento de información, el cual abarcara los procesos críticos del Organismo Coordinador.	
Objetivo General:	
Elaborar un Plan de Continuidad de Negocio para el Organismo Coordinador basándose en la Norma ISO 22301:2019	
Objetivos Específicos:	
Identificar los impactos que pueden interrupción entre los procesos y servicios del Organismo Coordinador.	
Identificar los riesgos de continuidad de negocio del Organismo Coordinador.	
Definir los procesos que debe poseer el Plan de Continuidad de Negocio para mejorar la capacidad de la organización en la presentación del servicio ante una interrupción.	
Definición de Condiciones, Restricciones y Supuestos del Proyecto:	
Restricciones:	
El presupuesto es de RD$2.4 MM.	
Pandemia COVID-19.	
Plan de Continuidad de Negocio debe realizarse en el marco de la ISO 22301:2019.	
El proyecto debe culminar a mas tardar el 31 de mayo 2021.	
Supuestos:	
El Plan de Continuidad de Negocio será entregado ante de la fecha limite de culminación.	
El personal del Organismo Coordinador estarán dispuesta a colaborar.	
El Organismo Coordinador suministrará todas las informaciones necesarias.	
Requisitos:	
El plan de continuidad del negocio debe ser entregado a tiempo pautado.	
El plan de continuidad del negocio debe incluir los procedimientos que se deben realizar ante una interrupción.	
El plan de continuidad del negocio debe ser creado bajo el estandar de la norma ISO 22301:2019	
Riesgos de alto nivel:	
Retrasos en la entrega del análisis y formulación ocasionando desplazamiento en los tiempo del proyecto	
Incumplimiento en el alcance, tiempo y calidad del proyecto, causando sanciones por la empresa que contrata.	
Interesados claves:	
Patrocinador: Manuel López San Pablo	
Project Manager: Ing. Fernando Beras	
Consejo de Coordinación del Organismo Coordinador	

4.2. Plan de Gestión de Alcance

4.2.1 Enunciado del Alcance

El proyecto de la elaboración de un plan de continuidad del negocio será creado para el Organismo Coordinador del Sistema Eléctrico, el mismo será conformado en base a los procesos críticos de la empresa, los demás procesos no se tomarán en cuenta para el proyecto. El plan de continuidad del negocio se podrá utilizar exclusivamente por el Organismo Coordinador del Sistema Eléctrico.

Tabla 2,

Enunciado del Alcance

Fuente: Elaboración propia

ENUNCIADO DEL ALCANCE	
Nombre del Proyecto	Elaboración Proyecto Plan de Continuidad de Negocio Basado en la Norma ISO 22301:2019, Organismo Coordinador Del Sistema Eléctrico Interconectado de la República Dominicana del Año 2021.
Preparado por:	Ing. Heinar Novas
Descripción del alcance	
Se desea elaborar un Plan de Continuidad de Negocio tomando en cuenta el levantamiento de información, el cual abarcará los procesos críticos del Organismo Coordinador.	
Objetivo del proyecto	
Elaborar un Plan de Continuidad de Negocio para el Organismo Coordinador basándose en la Norma ISO 22301:2019	
Criterios de aceptación	
Conceptos	**Criterio**
Técnicos	Todas las especificaciones técnicas deben quedar establecidas con claridad desde el inicio y deben ser aprobadas por el patrocinador.
Calidad	Se debe lograr al menos un 95% de la satisfacción del patrocinado.
Administración	Todos los entregables deberán contar con la aprobación del Gerente del Proyecto, y del patrocinador.
Comerciales	Se deberá cumplir estrictamente con lo establecido en cada uno de los contratos.
Entregables del proyecto	
• Entrega de Análisis de Impacto de Negocio (BIA)	
• Entrega de Riesgos de Continuidad	
• Entrega de Estrategias de Continuidad de Negocio	
• Entrega de Plan de Continuidad de Negocio	
Exclusiones del proyecto	
• No incluye la implementación del Sistema de Continuidad de Negocio.	
Restricciones del proyecto	
• El presupuesto es de RD$2.4 MM.	
• Pandemia COVID-19.	
• Plan de Continuidad de Negocio debe realizarse en el marco de la ISO 22301:2019.	
• El proyecto debe culminar a mas tardar el 31 de mayo 2021.	
Supuestos del proyecto	
• El Plan de Continuidad de Negocio será entregado ante de la fecha limite de culminación.	
• El personal del Organismo Coordinador estarán dispuesta a colaborar.	
• El personal del Organismo Coordinador estarán dispuesta a colaborar.	

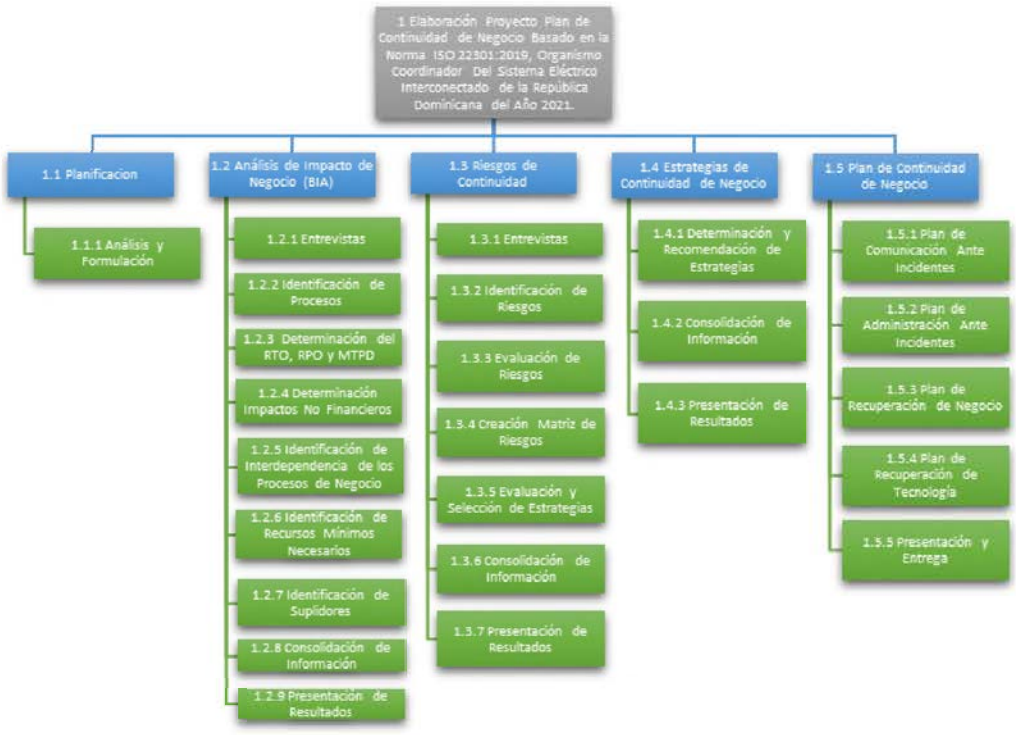
4.2.1 Estructura de Desglose de Trabajo

La Estructura de Desglose de Trabajo fue realizada con el objetivo de asegurar que todas las actividades que se consideren estrictamente necesarias para la realización de nuestro proyecto se encuentren al alcance, de esta manera podemos asegurar que no se desperdicien recursos ni esfuerzos que podremos utilizar para futuros proyectos. También ayudará a realizar la revisión del avance proyecto, ya que se puede monitorear que actividades son completadas.

Figura 2,

Estructura de Desglose de Trabajo

Fuente: Elaboración propia



4.2.1 Diccionario Estructura de Desglose de Trabajo

El diccionario de la estructura de desglose del trabajo es una herramienta que permite visualizar de manera detallada todo el contenido de cada uno de los entregables del proyecto, en ese sentido, ayuda a respaldar cada entregable que se encuentra en nuestra Estructura de Desglose de Trabajo. (Anexo 15)

4.3. Plan de Gestión del Tiempo

Con el propósito de administrar y controlar los procesos necesarios para completar el proyecto en el tiempo y plazos acordados con el patrocinador y el grupo de interesados, a continuación, se presenta el cronograma de actividades para dicho proyecto. El mismo fue realizado el Microsoft Project.

Figura 3,

Cronograma

Fuente: Elaboración propia

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors
1		**1 Elaboracion Plan de Continuidad de Negocio Basado en la Norma 22301:2019, Organismo Coordinador del Sistema Electrico Interconectado de la Republica Dominicana del ano 2021**	**112 days**	**Tue 12/15/20**	**Thu 5/27/21**	
2		**1.1 Planificacion**	**5 days**	**Tue 12/15/20**	**Mon 12/21/2**	
3		1.1.1 Analisis y Formulacion	5 days	Tue 12/15/20	Mon 12/21/2	
4		**1.2 Analisis de Impacto del Negocio**	**48 days**	**Tue 12/22/20**	**Thu 3/4/21**	3
5		1.2.1 Entrevistas	5 days	Tue 12/22/20	Tue 12/29/2(	
6		1.2.2 Identificacion de Procesos	8 days	Wed 12/30/20	Tue 1/12/21	5
7		1.2.3 Determinacion de RTO, RPO y MTPD	5 days	Wed 1/13/21	Tue 1/19/21	6
8		1.2.4 Determinacion Impacto no financieros	7 days	Wed 1/20/21	Mon 2/1/21	7
9		1.2.5 Identificacion de Interdependencia de los Procesos de Negocio	4 days	Tue 2/2/21	Fri 2/5/21	8
10		1.2.6 Identifiacion de Recursos Minimos Necesarios	7 days	Mon 2/8/21	Tue 2/16/21	9
11		1.2.7 Identificacion de Suplidores	5 days	Wed 2/17/21	Tue 2/23/21	10
12		1.2.8 Consolidacion de Informacion	5 days	Wed 2/24/21	Tue 3/2/21	11
13		1.2.9 Presentacion Resultados	2 days	Wed 3/3/21	Thu 3/4/21	12
14		**1.3 Riesgos de Continuidad**	**28 days**	**Fri 3/5/21**	**Wed 4/14/21**	4
15		1.3.1 Entrevistas	5 days	Fri 3/5/21	Thu 3/11/21	
16		1.3.2 Identificacion de Riesgos	8 days	Fri 3/12/21	Tue 3/23/21	15
17		1.3.3 Evaluacion de Riesgos de Continuidad	4 days	Wed 3/24/21	Mon 3/29/21	16
18		1.3.4 Creacion de Matriz de Riesgo	4 days	Tue 3/30/21	Mon 4/5/21	17

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	December 2020 2 7 12
19		1.3.5 Evaluacion y Seleccion de Estrategias	3 days	Tue 4/6/21	Thu 4/8/21	18	
20		1.3.6 Consolidacion de Informacion	2 days	Fri 4/9/21	Mon 4/12/21	19	
21		1.3.7 Presentacion Resultados	2 days	Tue 4/13/21	Wed 4/14/21	20	
22		**1.4 Estrategias de Continuidad**	**9 days**	**Thu 4/15/21**	**Tue 4/27/21**	**14**	
23		1.4.1 Determinacion y Recomendacion de Estrategias	5 days	Thu 4/15/21	Wed 4/21/21		
24		1.4.2 Consolidacion de Informacion	2 days	Thu 4/22/21	Fri 4/23/21	23	
25		1.4.3 Presentacion Resultados	2 days	Mon 4/26/21	Tue 4/27/21	24	
26		**1.5 Plan de Continuidad del Negocio**	**22 days**	**Wed 4/28/21**	**Thu 5/27/21**	**22**	
27		1.5.1 Plan de Comunicacion ante Incidentes	4 days	Wed 4/28/21	Mon 5/3/21		
28		1.5.2 Plan de Administracion ante Incidentes	4 days	Tue 5/4/21	Fri 5/7/21	27	
29		1.5.3 Plan de Recuperacion de Negocio	5 days	Mon 5/10/21	Fri 5/14/21	28	
30		1.5.4 Plan de Recuperacion de Tecnologia	8 days	Mon 5/17/21	Wed 5/26/21	29	
31		1.5.5 Presentacion y Entrega	1 day	Thu 5/27/21	Thu 5/27/21	30	

4.4. Plan de Calidad

El equipo de tesis cuenta con dos integrantes profesionalmente especializados que dirigen los procesos internos permitiendo una mejora continua en cada etapa del proyecto. Nos enfocamos en brindar la satisfacción de los clientes en base al compromiso de los integrantes del grupo de tesis, experiencia en la gestión de proyectos y altos conocimientos en las mejores prácticas y estandarización para crear un plan de continuidad del negocio.

El objetivo del equipo de tesis está orientado a desarrollar y gestionar los procesos de forma eficiente y eficaz con el propósito de generar satisfacción a nuestros clientes y cumplir con las normas que rigen los procedimientos. El equipo de tesis se enfoca en cumplir al 100% de los requisitos y especificaciones de los interesados, garantizar la entrega del proyecto al tiempo establecido según el cronograma, cumplir al 100% las normas ISO 22301:2019 para asegurar la calidad de los entregables. A continuación, los estándares de calidad utilizados para el proyecto:

Tabla 3,

Estándares de Calidad

Fuente: Elaboración propia

Estándar Y Norma	Organización que regula	Aplica a:
ISO 22301	Gestión de la Continuidad del Negocio (ISO)	Establece sistemas de gestión de la continuidad del negocio.
ISO 31000	Gestión de Riesgos (ISO)	Dedicada a la gestión de riesgos.

Como parte del aseguramiento de la Calidad, utilizamos la herramienta de la Matriz de la programación de la Calidad, la cual es la base para llevar a cabo las actividades específicas para el aseguramiento con relación a las expectativas del patrocinador y los demás Interesados.

Tabla 4,

Matriz de la Programación de la Calidad

Fuente: Elaboración propia

Entregable / Proceso	Requisitos	Actividad a realizar	Responsable
Planificación	La planificación no deberá pasar de 5 días.	Mediante el cronograma se llevará el seguimiento y el control del tiempo	Gerente de Proyecto
Análisis de Impacto del Negocio	El documento debe estar listo y presentado en no más de 48 días.	Mediante el cronograma se llevará el seguimiento y el control del tiempo	Analista de Proyecto
Riesgos de Continuidad	El documento debe estar listo y presentado en no más de 28 días.	Mediante el cronograma se llevará el seguimiento y el control del tiempo	Analista de Proyecto
Estrategias de Continuidad	El documento debe estar listo y presentado en no más de 9 días.	Mediante el cronograma se llevará el seguimiento y el control del tiempo	Analista de Proyecto
Plan de Continuidad del Negocio	El documento debe estar listo y presentado en no más de 22 días.	Mediante el cronograma se llevará el seguimiento y el control del tiempo	Gerente de Proyecto

4.5. Plan de Comunicaciones

En el plan de comunicaciones establece como fue llevada a cabo la gestión de la comunicación durante el proyecto, con el objetivo de mantener una comunicación coordinada en las diferentes fases del proyecto y con los interesados del proyecto, de igual forma manteniendo informados a los interesados. Para llevar a cabo este el plan de comunicaciones, se identificaron los interesados del proyecto para así saber el tipo de información adecuada que será compartida y porque medio es la mejor opción de compartirla.

Dentro de las herramientas a utilizar para la comunicación en el proyecto de la elaboración de un plan de continuidad del negocio, utilizamos correos electrónicos, reuniones virtuales, llamadas telefónicas, mensajería instantánea y presentaciones.

Las entrevistas fueron realizadas por vía de reuniones virtuales y llamadas por telefónicas, la cual se utilizó una comunicación interactiva. Para la presentación de resultados en cada una de las etapas del proyecto se utilizaron las reuniones virtuales y las presentaciones power point. En el anexo 13 y 14 se visualizan la matriz de interesados y la matriz de comunicación respectivamente.

4.5.1 Metodologías Empleadas en las Comunicaciones

A lo largo del proyecto se efectuaron diversas entrevistas a los dueños de los procesos, las mismas fueron realizadas por medio de conferencias vía el software google meet, con estas se buscaba recopilar información, generar datos y controlar que tipo de información se iba a utilizar. Con el registro de interesados fue utilizado para identificar los entrevistados. De igual forma se utilizó el correo electrónico para dar seguimientos en la gestión del proyecto, llamadas telefónicos para confirmar datos. Se utilizó una comunicación interactiva.

4.6. Plan de Recursos

Este plan tiene como propósito gestionar y administrar los recursos necesarios para completar el proyecto en el tiempo y plazos acordados con el patrocinador desde el inicio hasta final del proyecto. También, asignar las responsabilidades de todos los recursos involucrado en todos los entregables del proyecto.

Tabla 5,

Matriz de Recursos (Capital Humano)

Fuente: Elaboración propia

#	Nombre	Cargo
1	Fernando Beras	Gerente de Proyecto
2	Heinar Novas	Analista de Proyecto

Tabla 6,

Matriz de Recursos (Equipos)

Fuente: Elaboración propia

#	Nombre	Cargo
1	Laptop	Lenovo
2	Laptop	Macbook Pro

La Matriz RACI de este proyecto relaciona e identifica las diferentes responsabilidades de los actuantes con relación a los entregables del proyecto bajo las siguientes nomenclaturas, significados y reglas. "R" – Responsable, "A" – Aprobador, "C" – Consultado, "I" – Informado.

Las reglas a tener y cumplir en cuenta en esta matriz es que al menos debe haber un responsable dentro de la matriz RACI, sólo hay un aprobador por tarea y No hay límites de responsables, informados y consultados según se necesite.

Tabla 7,

Matriz RACI

Fuente: Elaboración propia

Matriz RACI					
	Roles/Responsabilidades				
Entregables	Patrocinador	Director Proyecto	Analista Proyecto	Gerente Operaciones	Gerente Comercial
Planificacion	A/C/I	A/R	R	C	C
Análisis de Impacto de Negocio (BIA)	A/C/I	A/R	R	C	C
Riesgos de Continuidad	A/C/I	A/R	R	C	C
Estrategias de Continuidad de Negocio	A/C/I	A/R	R	C	C
Plan de Continuidad de Negocio	A/C/I	A/R	R	C	C

Leyenda	
Rol / Responsabilidad	Descripción
R	**Responsable:** Este rol es el que realiza (ejecuta) el trabajo asociado con la actividad.
A	**Aprobador:** Es el encargado de aprobar (firmar), el trabajo realizado, a partir de esa aprobación, este se vuelve responsable por la actividad.
C	**Consultado:** Posee alguna información o capacidad que se necesita para mantener el trabajo. Se le informa y consulta información, de manera bidireccional con el responsable y/o aprobador.
I	**Informado:** Rol que debe ser informado sobre el progreso y los resultados del trabajo. En este caso la comunicación es unidireccional (se le da información pero no se recibe información).

4.7. Plan de Gestión de Riesgos

El Plan de Gestión de Riesgo es uno de los elementos iniciales al momento de planificar un proyecto, nos ayuda a prever las situaciones futuras que puedan presentarse, este es el producto del área del conocimiento de la Gestión de Riesgo, según la Guía del PMI. Primero que todo se realiza una identificación de los riesgos del proyecto, evaluando los posibles eventos que puedan perjudicar el cumplimiento de los objetivos del proyecto.

Luego de obtener los riesgos se debe determinar el impacto inherente en el proyecto. El impacto inherente se determina identificando la probabilidad de ocurrencia del riesgo, multiplicado por el nivel de impacto que pueda ocasionar dicho riesgo. Por último, se deben colocar controles que ayuden a mitigar el riesgo para así obtener un riesgo residual, es decir, eliminar o disminuir la probabilidad de ocurrencia del riesgo.

Tabla 8,

Probabilidad de Ocurrencia

Fuente: Elaboración propia

Probabilidad de Ocurrencia		
Cualitativo	**Cuantitativo**	**Descripción**
Muy Alto	4	Evento frecuente. Se reproduce muchas veces. Interfieren de modo claro en el ritmo de las actividades, de modo que se tornan evidentes aún para los que no conocen el proceso.
Alto	3	Evento común o usual, normalmente encarado de modo natural debido a su habitualidad. Son eventos de amplio conocimiento de los involucrados en el proceso.
Medio	2	Evento ocasional, casual o eventual; a veces inesperado, pero con historia. Normalmente de conocimiento de los gestores de procesos y de los operadores más experimentados.
Bajo	1	Evento raro o extraordinario para los estándares conocidos de gestión y operación del proceso. Los históricos de esos eventos no siempre están disponibles, aunque puedan asumir dimensión estratégica para la manutención del proceso y/o negocio.

Tabla 9,

Nivel de Impacto

Fuente: Elaboración propia

Nivel de Impacto		
Cualitativo	**Cuantitativo**	**Descripción**
Muy Alto	4	Detiene la ejecución del proyecto.
Alto	3	Retrasa la ejecución del proyecto y no se puede responder de manera fácil y rápida al evento.
Medio	2	Retrasa la ejecución del proyecto y se puede responder de manera fácil y rápida al evento.
Bajo	1	No afecta la ejecución del proyecto. Se puede responder de manera fácil y rápida al evento.

Tabla 10,

Matriz de Riesgo

Fuente: Elaboración propia

EDT	Actividad	Riesgo	Descripción del Riesgo	Prob.	Impacto	Nivel de Riesgo Inherente	Control	Tipo de Control	Prob.	Impacto	Nivel de Riesgo Residual
1.1.1	Análisis y Formulación	Retrasos en el proyecto	Retrasos en la entrega del análisis y formulación ocasionando desplazamiento en los tiempo del proyecto	3	4	Alto	El equipo de proyecto cuenta con el plan de tiempo del proyecto con el cual se le da seguimiento al cronograma de trabajo.	Preventivo	2	1	Bajo
1.2.1/1.3.1	Entrevistas	No existe colaboración	Los entrevistados no se muestren colaborativos a la hora de entrevistarlos	2	4	Moderado	Desde el inicio el Gerente de Proyecto comunica al Gerente General que necesitara el apoyo de cada uno de los colaboradores para poder proceder con las entrevistas.	Preventivo	1	1	Bajo
		Falta de tiempo	Los colaboradores de la empresa no cuenten con tiempo suficiente para poder participar en las entrevistas	2	4	Moderado	Desde el inicio el Gerente de Proyecto planifica con los colaboradores que van a participar y agendan las entrevistas en el Outlook.	Preventivo	2	1	Bajo
1.2.2	Identificación de Procesos	Incongruencias en los resultados	Identificar procesos que no sean criticos para el plan de continuidad	2	3	Bajo	El analista de proyecto posee los conocimientos esenciales para la identificación oportuna de riesgos criticos	Preventivo	1	1	Bajo
1.3.2	Identificación de Riesgos	Falta de estrategias	Falla en la identificación de riesgos ocasionando que algunas estrategias no sean identificadas	2	4	Moderado	El equipo de proyecto cuenta con el conocimiento en la gestión de riesgos de la ISO 31000	Preventivo	2	1	Bajo
1.3.5	Evaluación y selección de estrategias	Falta de estrategias	No identificación oportuna de las estrategias	2	4	Moderado	El equipo de proyecto cuenta con los conocimientos necesarios por parte de la norma ISO 22301 de continuidad del negocio.	Preventivo	2	1	Bajo
1.5.5	Presentación y Entrega	Incumplimiento en el alcance, tiempo y calidad del proyecto	Incumplimiento en el alcance, tiempo y calidad del proyecto, causando sanciones por la empresa que contrata.	3	4	Alto	Desde un inicio el equipo de proyecto realiza una planificación de tiempo, alcance y calidad que va a requerir el proyecto	Preventivo	2	1	Bajo

Parte 3. Marco Metodológico

Capítulo 5: Metodología de la investigación

5.1. Base Metodológica.

La presente investigación cuenta con una base holística, la cual de acuerdo con los diferentes constructos teóricos que interrelacionados, presentan un punto de vista sistémico de los fenómenos mediante la especificación de relaciones entre variables, con el propósito de explicar y predecir fenómenos. "En este sentido se comprende que la investigación tiene en cuenta una teoría constituida por un conjunto de variables interrelacionadas que explican y predicen situaciones, que se encuentran vigentes, o deberían refutarse total o parcialmente" Kerlinger (1997).

Los supuestos presentados dentro de la investigación holística, es construido en base a un modelo que permite organizar y sistematizar la información y el conocimiento relacionado con la metodología de la investigación. La investigación es interdisciplinar, ya que se integran diferentes disciplinas de la investigación.

5.2. Perspectiva metodológica.

La presente investigación se reconoce como cuantitativa, precisamente porque se basa en datos objetivos mediante entrevistas con respuestas concretas que permiten generar una propuesta completa referente a la continuidad del negocio en cuestión. "Eventualmente se reconoce que el paradigma cuantitativo se reconoce como positivista y busca la medición objetiva, demostración de causalidad y generalización de los resultados de la investigación" (Fernández & Díaz, 2002). En la misma medida desde la recogida de información la investigación se reconoce como estructurada y sistemática, considerando la aplicación de la norma ISO 22301 este tipo de construcción es supremamente necesaria, considerando el orden que se debe conservar. La investigación se debe considerar de igual forma cualitativa,

ya que algunas partes se basan en la observación del entorno, algunas respuestas de las entrevistas son abiertas y se utilizan datos anteriores para sacar información.

5.3. Tipo de investigación.

Eventualmente y dados los condicionantes anteriormente mencionados se evidencia que la investigación asume una tipología holística, la cual "se define como la comprensión crítica reflexiva del entorno que permite una visión amplia del mundo y de la vida, desde una perspectiva integradora con énfasis en la trascendencia" (Mendoza & et al, 2019). Desde esta percepción la holística permitirá al presente proyecto de investigación generar una mirada englobante de la diversidad del conocimiento, permitiendo evidenciar la vigencia de las ideas.

5.4. Diseño de la investigación.

La investigación se reconoce como no experimental manteniendo las condiciones de la investigación cuantitativa y cualitativa desde su sistematicidad. Este no pretende manipular de manera consistente las variables del estudio, y se basa en la observación de fenómenos como tal y como se presentan en el contexto, y analizarlos con posterioridad, en este proceso no existe ningún estímulo, los sujetos son analizados en su torno natural. Se utilizó la metodología APA 7ma edición para el desarrollo de la investigación.

> El diseño no experimental es el que se realiza sin manipular en forma deliberada ninguna variable. El investigador no sustituye intencionalmente las variables independientes. Se observan los hechos tal y como se presentan en su contexto real y en un tiempo determinado o no, para luego analizarlos. Por lo tanto, en este diseño no se construye una situación específica sino que se observa las que existen (Martins & Palella, 2010).

5.5. Objetivos de la investigación.

El objetivo esencial de la investigación holística es elaborar un Plan de Continuidad de Negocio para el Organismo Coordinador del Sistema Eléctrico Nacional Interconectado de la República Dominicana, basándose en la Norma ISO 22301: 2019 en el transcurso del año 2021. La parte cuantitativa se basa en datos objetivos mediante entrevistas con respuestas concretas que permiten generar una propuesta completa referente a la continuidad del negocio; mientras que la parte cualitativa determinará algunas partes que se basan en la observación del entorno actual de la empresa, algunas respuestas de las entrevistas son abiertas de acuerdo a la experiencia de los gerentes entrevistados y se utilizan datos históricos para sacar información.

5.6 Fases del proceso de la investigación.

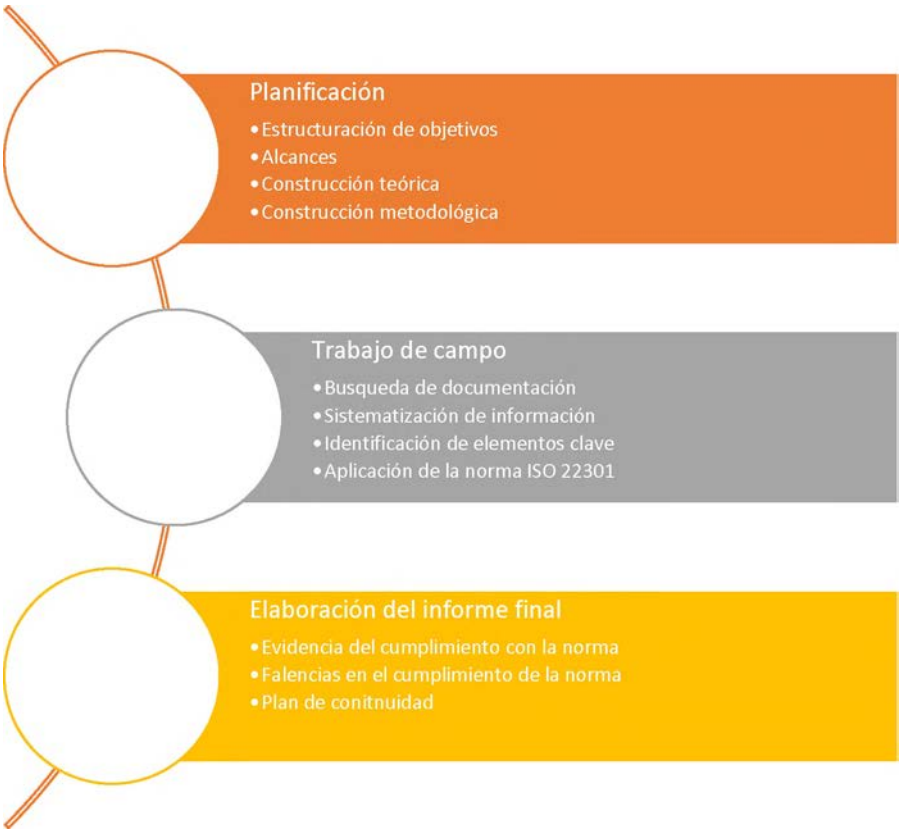
El presente proyecto conlleva una metodología de investigación marcada en fases. La fase de planificación, donde se establecen tantos los objetivos de investigación como el alcance que provee el trabajo y también el tiempo destinado que se ocupara para esta investigación, adicionalmente se propone realizar la planeación propia de la recolección de información y demás indicadores procedentes.

La fase de trabajo de campo, donde se buscará generar procesos como la aplicación de la norma ISO 22301 del año 2019, considerando la totalidad de sus requisitos, definiendo las condiciones organizacionales que se encuentran presentes en cada uno de los ítems evaluados y la fase de elaboración informe final, el cual luego de la realización del trabajo de campo es necesario sintetizar la totalidad de la información considerando la generación de un documento que dé pie a la estructuración de este plan.

Figura 4,

Visión holística del proceso de creación de plan de continuidad empresarial

Fuente: Elaboración propia.



5.7. Procedimiento determinación de variables.

El presente documento de investigación, relaciona las variables que tienen la posibilidad de medirse y se encuentran ajustadas al proceso, estas se definen como las variables dependientes, estas se deben tener en cuenta en el desarrollo de la presente investigación y se encuentra la capacidad por parte de la organización para continuar brindando sus proyectos y/o servicios, identificando junto a ello los productos, servicios y procesos críticos, con el fin de establecer procedimientos de recuperación críticos y así con ello conocer el nivel de cumplimiento de la norma ISO 22301. Así mismo considerar el riesgo que pueden afectar la continuidad de las operaciones.

Las variables independientes a tener en cuenta van desde el análisis de impacto, los planes de continuidad del negocio, auditorías internas y la gestión de riesgo acompañado del Sistema de gestión de continuidad del negocio basado en la norma ISO 22301.

5.8. Población y determinación de la muestra.

La población corresponde, para el caso como la totalidad de documentos y elementos que en el entorno interno y externo puedan afectar la continuación del negocio al interior de la organización, para el caso el muestreo de los documentos se realiza a conveniencia considerando aquellos que puedan ser útiles para el proyecto de investigación.

5.9 Fuentes de recolección de información.

Considerando el objetivo que se encuentra estructurado en la presente investigación, es necesario ocupar diferentes fuentes de información. Las fuentes primarias, consisten en la localización de información propicia al interior de la organización, sin llegar a realizar ningún tipo de observación o experimentación. Para el caso la observación resulta considerarse uno de los elementos para socavar la información, posterior a la observación es necesario considerar el análisis de los diferentes procesos que constituyen el fenómeno concebido como la continuidad del negocio. Adicionalmente se reconoce que otra de las fuentes primarias de información son los documentos oficiales de la organización y el Check list propio de la Norma ISO 22301.

Continuando es necesario tener en cuenta las fuentes de información secundarias, estas son aquellas que parten de datos pre elaborados que pueden ser obtenidos de la web o la biblioteca, se incluyen para el caso los estudios, tesis, tesinas y demás documentos que pueda tener información referente a la temática analizada y permitan entonces la construcción de los diferentes elementos teóricos para sustentar el proyecto de investigación. Para el caso se

ocuparán documentos de referencia que permitan verificar la aplicación de la norma ISO 22301 aplicando la posibilidad de generar continuidad en el negocio.

Parte 4. Resultados y Análisis, Conclusiones y Recomendaciones

Capítulo 6: Resultados y Análisis

6.1. Diagnostico situacional de la organización.

Para realizar un plan de continuidad del negocio, es necesario obtener el estado actual de la empresa, en este caso al Organismo Coordinador del Sistema Eléctrico Nacional, es decir, ver el estado de la empresa en el momento antes de empezar el proyecto. Esto ayudara a tener una visión 360 de cómo está posicionada la empresa en el momento en términos de continuidad del negocio.

6.1.1. Análisis de la empresa

El presente estudio se encuentra concentrado en el Organismo Coordinador del Sistema Eléctrico Nacional Interconectado (OC) el cual fue creado el 29 de octubre de 1998, mediante la Resolución No 235 de la Secretaria de Estado de Industria y Comercio para coordinar la operación de las instalaciones de las empresas de generación, transmisión y distribución de electricidad que pertenecen al Sistema Eléctrico Nacional Interconectado (SENI) de la República Dominicana.

Posteriormente, la Ley General de Electricidad N°125-01, promulgada el 26 de julio de 2001, establece que las empresas eléctricas de generación, transmisión, distribución y comercialización, así como los auto productores y cogeneradores que venden sus excedentes a través del SENI, deben coordinar la operación de sus instalaciones para prestar el mejor servicio al mínimo costo, y que para ello deben constituir e integrar un organismo que coordine la operación de los sistemas de generación, transmisión, distribución y comercialización en el SENI, denominado Organismo Coordinador (OC). El tipo de la estructura organizacional es funcional, debido a que cada uno realiza sus funciones. (Anexo 1)

Adicionalmente el Consejo de Coordinación que se reconoce como la autoridad máxima del OC-SENI tiene la responsabilidad de velar por el cumplimiento de las disposiciones y funciones que establecen la normativa que regula al sector eléctrico. El Consejo de Coordinación se encuentra conformado por un representante de la Superintendencia de Electricidad (SIE) que lo preside, un representante del Bloque de Generación, un representante del Bloque de Generación hidroeléctrica, un representante del Bloque de transmisión, un representante del Bloque de Distribución.

En lo referente a la misión y visión establecidas por la empresa, se destaca que, en cuanto a la primera, dicha empresa afirma que esperan planificar y coordinar la operación del sistema eléctrico nacional interconectado para lograr generar un abastecimiento de energía seguro, a mínimo costo y determinar las transacciones económicas, conforme a la normativa, con una organización interdependiente y uso efectivo de los recursos y en lo referente a la visión, esta espera ser reconocida en el sector eléctrico latinoamericano como una institución de excelencia operacional.

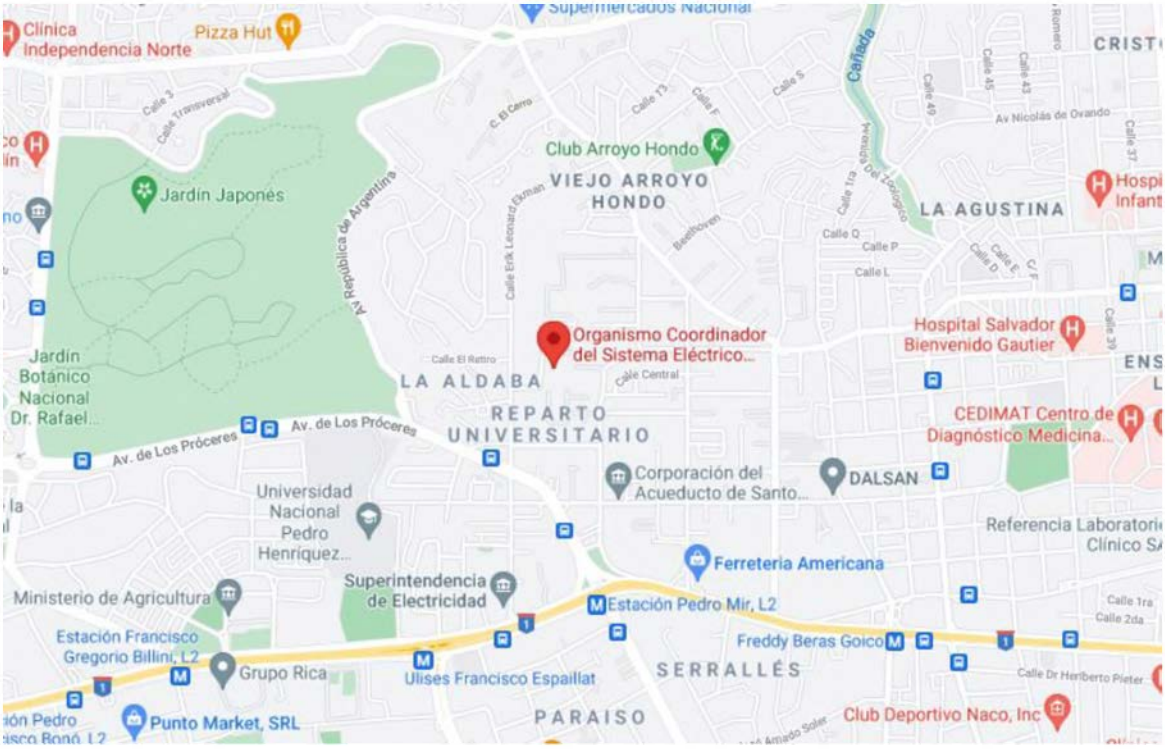
6.1.2. Ubicación e infraestructura

En el siguiente mapa tomado de google maps, se puede observar la ubicación exacta donde se encuentra ubicado del Organismo Coordinador del Sistema Eléctrico Nacional. Para ser más exactos, la edificación principal se encuentra en la Calle 3 número 3, Arroyo Hondo primero, Santo Domingo, Distrito Nacional, República Dominicana.

Figura 5,

Ubicación Organismo Coordinador, 2021

Fuente: Google Maps



6.1.3. Análisis GAP del sistema de gestión de la continuidad del negocio de la organización

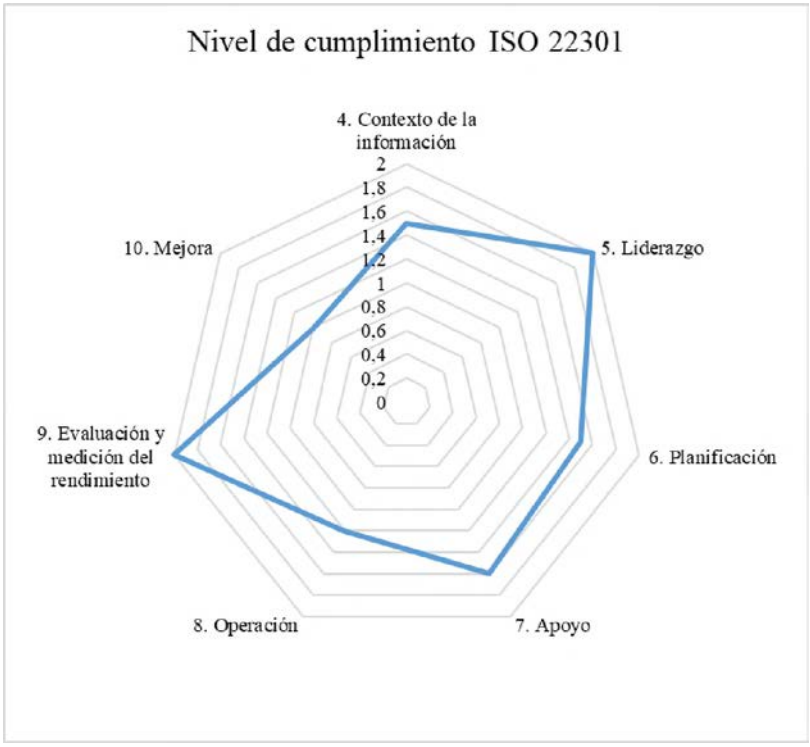
En esta etapa se debe indicar el nivel de cumplimiento que tiene la organización respecto a la Norma ISO 22301, ello también acorde con la Ley general de Electricidad 125-01, para comprender la diferencia entre el estado actual de la organización y el estado que intenta alcanzar. (Anexo 2)

Para identificar el cumplimiento de los aspectos anteriormente analizados se tuvieron en cuenta los informes presentados por la organización para el año 2020, encontrados en la página web oficial, eventualmente en la figura siguiente se puede apreciar el nivel de cumplimiento que tiene la organización con respecto a cada uno de los ítems ISO 22301. No obstante, se encuentra que el mejor nivel de desarrollo se encuentra en la evaluación y medición de rendimiento al igual que en liderazgo. Mientras que el peor nivel se encuentra en el sector de la mejora.

Figura 6,

Nivel de cumplimiento de la ISO 22301

Fuente: Elaboración propia.



6.2. Análisis del impacto al negocio BIA (Bussiness Impact Analysis)

En esta etapa de análisis de impacto de negocio tiene como intención básica identificar los problemas y/o servicios críticos para la organización, y sobre ellos determinar el tiempo límite que puede estar inoperativos, es decir que son aquellos que no pueden brindar los servicios al cliente; con el objetivo de establecer planes que permitan recuperar las operaciones en el momento en el que ocurran eventos adversos.

6.2.1. Identificación de los procesos críticos.

La identificación de los servicios críticos se realiza conforme con la continuidad de las operaciones, y en general del negocio, la cual resulta ser una responsabilidad de todos y cada uno de los funcionarios del Organismo Coordinador, sin embargo, se debe tener en cuenta que la administración de la continuidad requiere de la presencia de un líder que motive y desarrolle las condiciones necesarias para lograrlo.

La continuidad es expresada bajo la responsabilidad y adopción de cada área organizacional individualmente tiende al fracaso, a menos que exista una alta madurez en continuidad capaz de afianzar y fortalecer la disciplina de los individuos que la componen. Por esto, dentro de las organizaciones con un nivel bajo de cultura de continuidad, se hace necesario tener un líder que vele por alinear, fortalecer y mantener el sistema de continuidad del negocio. El organigrama del Organismo Coordinador estará anexo a esta investigación.

En este levantamiento de procesos fue seleccionado el nivel gerencial de la organización, ya que tiene conocimientos de los procesos críticos del negocio. Además, se recomendó tener el acompañamiento de su equipo de trabajo o colaboradores del área. Con la ayuda de todo el equipo catalogaron lo procesos en críticos y no críticos (Anexo 3 y Anexo 4).

Los procesos no críticos de las diferentes gerencias no se tomaron en cuenta dado que los mismos no representan impacto directo a los servicios brindados por la organización. Luego de identificar los puestos de trabajo, procesos y productos ofrecidos, se debe realizar

un diagnóstico de la organización para identificar las necesidades de cara a continuidad. Aquí se evidencia con qué recursos contamos y que debemos atacar primero a la hora de realizar el levantamiento del BIA.

El análisis de impacto del negocio o Business Impact Analysis (BIA) es el paso siguiente para la elaboración de un plan de continuidad del negocio, el cual tiene como objetivo identificar los procesos críticos para la operación de la organización, así como los productos, servicios que ofrece, cantidad de empleados, edificaciones, recursos e infraestructura tecnológica y poder evaluar cada elemento de la organización, así como participar en la continuidad de las operaciones y cómo pueden verse impactados.

Debido a que el BIA es un análisis donde se toman datos de los entrevistados y de la organización en un momento en el tiempo y dichos datos pueden variar a medida que pasa el tiempo, por ende, la realización y entrega del análisis de impacto del negocio debe realizarse de manera acelerada para evitar resultados no acordes al tiempo presente.

Antes de iniciar las entrevistas primero se estableció una reunión inicial para dar inicio a lo que es el proyecto. La reunión contó con la participación del nivel gerencial de cada departamento. Con esto se pudo asegurar el compromiso y apoyo de cada uno de ellos. Como la metodología utilizada es la norma internacional 22301:2019, a continuación, los conceptos básicos del BIA

El impacto es el efecto o consecuencia por una interrupción de las operaciones de la entidad. El impacto se puede observar o medir mediante aspectos económicos, imagen de las personas o empresas, sanciones legales, disminución de capacidad de respuesta y competitividad, entre otros. El Tiempo Máximo de Tolerancia es el Tiempo que le llevará a los impactos adversos, en convertirse en inaceptables y pueden resultar al no suministrar productos o servicios o no ejecutarse una actividad. La Información crítica para el proceso es el punto en el cual la información o los datos de un proceso o aplicación deben ser recobrados

tras una interrupción. Se utiliza frecuentemente para ayudar a definir estrategias de respaldo de información.

A fin de establecer los impactos no monetarios se establecieron seis categorías de impactos (Estratégico, Regulatorio, Operativo, Reputacional, Social y Recursos Humanos). Dentro de cada una de estas categorías se definieron los criterios para clasificar el nivel de impacto, a través del consenso de los equipos de trabajo de la organización. (Anexo 5)

Se presentan también los criterios establecidos para el establecimiento de los impactos no financieros, debe mencionarse que los impactos se agruparon por "Nivel" de acuerdo con la rapidez de la interrupción para cada nivel de impacto. Posteriormente, cada proceso fue clasificado colocando el "Nivel" más alto para cada uno de los seis criterios de clasificación no financiera y así obtener su clasificación definitiva por impacto.

Tabla 11,

Nivel de impacto

Fuente: Elaboración propia.

Nivel de Impacto					
Nivel	Catastrofico	Critico	Grave	Moderado	Leve
Tipo de Impacto: Operativo					
1	Menos de 3 horas	Menos de 2 horas	Menos de 1/2 hora		
2	De 3 horas a 3 dias	De 2 horas a 1 dia	De 1/2 hora a 4 horas		
3	De 3 dias a 1 mes	De 1 dia a 1 semana	De 4 horas a 2 dias		
4	De 1 mes a 2 meses	De 1 semana a 3 semanas	De 2 dias a 1 semana		
5			Mas de 1 semana	Todos	Todos
Tipo de Impacto: Reputacional					
1	Menos de 2 horas	Menos de 4 horas	Menos de 1 hora		
2	De 3 horas a 1 dia	De 4 horas a 2 dias	De 1 hora a 3 horas		
3	De 1 dia a 3 dias	De 2 dias a 4 dias	De 4 horas a 3 dias		
4	De 3 dias a 1 semana	De 4 dias a 2 semana	De 1 semana a 3 semanas		
5	Mas de 1 semana	2 semanas en adelante	mas de 3 semanas	Todos	Todos
Tipo de Impacto: Recursos Humanos					
1	Menos de 2 horas	Hasta 3 horas	Hasta 1/2 hora		
2	De 2 horas a 2 dias	De 4 horas a 4 dias	De 1/2 hora a 4 horas		
3	De 2 dias a 5 dias	De 5 dias a 1 semana	De 4 horas a 2 dias		
4	De 5 dias a 2 semanas	De 1 semana a 3 semanas	De 2 dias a 1 semana		
5	Mas de 2 semanas	Mas de 3 semanas	Mas de 1 semana	Todos	Todos
Tipo de Impacto: Social					
1	Menos de 2 horas	Hasta 3 horas	Hasta 1/2 hora		
2	De 2 horas a 2 dias	De 4 horas a 4 dias	De 1/2 hora a 4 horas		
3	De 2 dias a 5 dias	De 5 dias a 1 semana	De 4 horas a 2 dias		
4	De 5 dias a 2 semanas	De 1 semana a 3 semanas	De 2 dias a 1 semana		
5	Mas de 2 semanas	Mas de 3 semanas	Mas de 1 semana	Todos	Todos
Tipo de Impacto: Estrategico					
1	Menos de 2 horas	Hasta 3 horas	Hasta 1/2 hora		
2	De 2 horas a 2 dias	De 4 horas a 4 dias	De 1/2 hora a 4 horas		
3	De 2 dias a 5 dias	De 5 dias a 1 semana	De 4 horas a 2 dias		
4	De 5 dias a 2 semanas	De 1 semana a 3 semanas	De 2 dias a 1 semana		
5	Mas de 2 semanas	Mas de 3 semanas	Mas de 1 semana	Todos	Todos
Tipo de Impacto: Regulatorio					
1	Menos de 2 horas	Hasta 3 horas	Hasta 1/2 hora		
2	De 2 horas a 2 dias	De 4 horas a 4 dias	De 1/2 hora a 4 horas		
3	De 2 dias a 5 dias	De 5 dias a 1 semana	De 4 horas a 2 dias		
4	De 5 dias a 2 semanas	De 1 semana a 3 semanas	De 2 dias a 1 semana		
5	Mas de 2 semanas	Mas de 3 semanas	Mas de 1 semana	Todos	Todos

Posteriormente, luego de asignados los "Niveles" a cada proceso, se estableció el criterio de selección de los procesos más críticos para todos aquellos procesos que alcancen la capa más crítica "Nivel-1" en cualquier tipo de impacto. En cada uno de los impactos indicamos su categoría, asignándoles una letra desde leve a catastrófico, con rangos desde la letra A, a la letra E, respectivamente:

Tabla 12,

Categoría de impacto

Fuente: Elaboración propia.

Catastrófico	E
Crítico	D
Grave	C
Moderado	B
Leve	A

6.2.2. Determinación de RTO, RPO, MTPD

El análisis de los impactos financieros se centra en el hecho de que ocurrió un evento que interrumpió las operaciones normales de los procesos críticos para la entidad, esto enmarcado en un período de tiempo. Como se menciona en nuestra metodología, el entrevistado se basó en el peor escenario, momento en el cual el proceso no se debería detener. Los impactos que se pueden identificar como impactos financieros ante una interrupción para el OC son los ingresos, si bien el OC es un organismo sin fines de lucro, los ingresos pudieran verse afectados por no brindar los servicios con calidad en sistema eléctrico nacional interconectado según la ley general de electricidad 125-01. Las demandas, el OC podría ser objeto de demandas por parte de los agentes debido a errores en la ejecución de la programación de la operación o errores en el cálculo de transacciones económicas.

El tiempo de recuperación son los tiempos identificados en el OC de acuerdo con el escenario del peor caso o el tiempo más crítico para alguno de los procesos de la institución; este tiempo puede afectar la operación o la consecución de los objetivos. Al final, los encuestados respondieron dos tipos de tiempos de recuperación:

El primero hace referencia al Máximo Tiempo de Tolerancia de los procesos de negocio después de una interrupción y es conocido como MTO. Mientras que el segundo hace referencia a la posible pérdida de información en un período de tiempo (RPO), esta información podría ser reconstruida con fuentes internas o externas.

Figura 7,

MTDP

Fuente: Elaboración propia

De acuerdo con la figura inmediatamente anterior, se evidencia el listado de procesos con un tiempo de recuperación inferior a 8 horas de interrupción. Tomando en cuenta que en el peor de los escenarios el que toma en cuenta según los entrevistados en el cual podría impactar la operación y la institución.

El RPO busca identificar cuánta información se podría perder en un evento de interrupción o desastre, sin generar impactos a los procesos o servicios de la compañía, y que los procesos de negocios podrían reconstruir o volver a obtener información de su operación normal porque se tienen las fuentes originales para esto. Se identificó solo un proceso cuya máxima tolerancia (cantidad de tiempo) que estaría dispuesto a perder información es de menos de una hora. Los tiempos identificados por los responsables de los procesos/servicios en el OC son los siguientes:

Figura 8,

RPO

Fuente: Elaboración propia

6.2.3. Impacto No Financiero

Tabla 13,

Resultado Impacto No Financiero

Fuente: Elaboración propia

Proceso	Tipo de Impacto					
	Ope.	Rep.	RR.HH	Social	Estr.	Reg.
1.1.1 Supervisión y coordinación en tiempo real y verificación del cumplimiento de los programas	1E	3E	3E	3C	2D	N/A
1.2.1 Programación diaria	3E	5E	5C	5C	5E	N/A
1.2.2 Verificación de costos variables	3E	5E	5C	5C	4E	3E
1.2.3 Programación semanal	5B	5B	5B	5B	5B	N/A
2.1.1 Revisión de la entrega de medidas	3C	4C	5B	5B	5C	N/A
2.1.2 Habilitación de SMC (Sistema de medición comercial)	4C	5C	5A	5A	5B	N/A
2.2.1 Cálculos de transacciones económicas	3D	4C	5B	5B	4C	2D
2.2.2 Cálculo de Costos marginales	5B	5B	5B	5B	5B	N/A

6.2.4 Mapeo de Interdependencia de los Procesos de Negocio

Dentro del estudio que se ha realizado del estado actual de continuidad de negocio en el OC, se confirmó que los procesos críticos se soportan sobre aplicaciones o servicios de TI para realizar sus actividades y ha permitido medir el nivel de prioridad de cada aplicación o servicio de TI.

Al realizar los diferentes tipos de levantamiento se determinó que los sistemas tecnológicos tienen mucha relevancia y alto impacto debido a que los mismo soportan las operaciones críticas y no críticas que se llevan día a día en la organización.

Por esto a continuación identificaron los sistemas y aplicaciones que soportan cada proceso de la organización, organizándose por tiempo máximo de recuperación en los que fueron catalogados dichos procesos:

Figura 9,

Tiempo de recuperación de sistemas

Fuente: Elaboración propia

Tiempos de Recuperación	Sistemas
Tiempo de Recuperación: 0 a 60 minutos	• SCADA • REGIO • Internet
Tiempo de Recuperación: 8 horas	• MODOM • DIGSILENT • Sistema de Verificación de Costos Variables
Tiempo de Recuperación: 1 día	• Prime Read • PSS/E • PFT • Máquina virtual para correr PSS/E con Windows 98 • Microsoft Office

6.2.5. Recursos Mínimos Necesarios

La identificación de los recursos mínimos necesarios para los procesos es indispensable para el BIA. Los recursos mínimos se refieren a las personas, sistemas, instalaciones físicas, etc., que van a ser necesarios para continuar las operaciones aun haya una interrupción crítica. Estos recursos mínimos levantados son parte integral de lo que es el plan de continuidad del negocio. (Anexo 6)

6.2.6. Suplidores

Las dependencias externas o suplidores forman parte del ecosistema de una organización, ya que son las que suplen cualquier tipo de servicio o producto a la empresa. Especialmente en la continuidad del negocio se debe dar un trato especial a los suplidores ya que la organización no cuenta con el control sobre la continuidad del negocio de dicho

suplidor. Una interrupción de un suplidor podría generar una interrupción de nuestros procesos más críticos.

Además de identificar cada proveedor, es buena práctica determinar si cada suplidora cuenta con planes de continuidad del negocio y si este ha sido probado. También es recomendable identificar si en el contrato entre las partes existe una cláusula donde exija dicho plan de continuidad del negocio. A continuación, presentamos el resultado de los principales proveedores de los procesos del OC y su preparación en contingencia:

Tabla 14,

Proveedores

Fuente: Elaboración propia.

Nombre del proveedor	**Servicio**
Wind Telecom	Fibra enlace SCADA e internet
Claro Dominicana	Internet y telefonía
Altice	Internet y telefonía
Viva Dominicana	Internet

6.2.7. Evaluación de Riesgo

La evaluación de riesgo es parte integral para el diseño y elaboración del plan de continuidad del negocio. La evaluación de riesgo de continuidad nos ayuda a determinar las debilidades o puntos de mejora de la organización, sabiendo se obtiene una visión clara de cuales con las prioridades de la organización en materia de las estrategias que se van a implementar dentro del plan de continuidad del negocio.

Un riesgo es la probabilidad de que un evento ocurra y que ocasione pérdidas o daños afectando desfavorablemente el logro de los objetivos. En el caso de la continuidad del negocio, la evaluación de riesgo ayuda a buscar la probabilidad e impacto de los eventos de interrupción que puedan ocurrir que afecten la organización.

La gestión de riesgos de continuidad aplica para cualquier sector industrial o productivo y puede ser la diferencia entre un servicio ininterrumpido que permita cumplir con los objetivos establecidos o el cierre definitivo del negocio. El levantamiento de riesgos de continuidad fue realizado para aquellos procesos definidos como críticos dentro de la entidad, criterio que fue confirmado por el personal del proyecto. Dentro del alcance del análisis de riesgos de continuidad se analizaron los procesos que pueden afectar la continuidad del negocio, los procesos analizados en la evaluación del riesgo están distribuidos en los departamentos de Operación en Tiempo Real, Programación de la Operación, Transacciones y Mediciones. (Anexo 16)

La actividad de evaluación y análisis de riesgos busca determinar la probabilidad de que se presenten amenazas o vulnerabilidades que puedan impactar la operación cotidiana de los procesos involucrados en la gestión del negocio. La información recopilada se obtuvo mediante entrevistas, solicitud de información, análisis internos y externos y análisis situacional de aspectos que puedan afectar las operaciones del negocio. Los riesgos que se presentarán fueron identificados como factores que afectan la continuidad en las cuatro dimensiones, que son, procesos del negocio, personas, infraestructura tecnológica e infraestructura física.

Figura 10,

Dimensiones para evaluación de riesgo

Fuente: KPMG Advisory Service

Dentro de la dimensión de procesos de negocios tenemos los aspectos que se tomaron en cuenta, como la gestión de los procesos, donde se documenta e identifica los procesos críticos, se definen de indicadores de gestión, se determinan los acuerdos de niveles de servicio (SLA) con los involucrados. En los procesos de negocio se deben identificar y documentar los recursos mínimos de las operaciones y los cargos críticos.

De igual forma se tomó en cuenta la definición y ejecución de pruebas de planes alternos de trabajo, se generan los procedimientos de recuperación y contingencia, identificar y analizar las vulnerabilidades o amenazas de los procesos críticos. Ver la existencia de la alta dependencia de proveedores externos, así como, que mecanismos ellos tienen de contingencia de los servicios ofrecidos y la existencia de un plan de comunicación de crisis.

Otro aspecto dentro de la dimensión de la gestión de procesos es el soporte de tecnología de información, aquí se toman en cuenta el nivel de oportunidad del soporte tecnológico a los procesos de negocio, la coordinación de las interrupciones programadas que

debe tener el departamento de tecnología, tener un nivel de atención aceptable a los incidentes de tecnología de información y contar con la recuperabilidad, integridad y disponibilidad de los sistemas de información de acuerdo a los objetivos estratégicos de la empresa.

Se toma en cuenta la dimensión de las personas o recursos humanos como factor que puede afectar la continuidad de la OC, uno de los aspectos es la gestión del conocimiento. Estos son ejemplos de los factores que deben tomarse en cuenta para evitar interrupciones futuras, el entrenamiento y capacitación del personal, entrenamiento cruzado, conocimientos de actualizaciones y mejoras en los procedimientos existentes, políticas de información sensible en medios magnéticos, electrónica o impresa, índices de rotación de personal, políticas de retención de personal.

La seguridad laboral forma parte dentro de la dimensión de las personas, esto incluye la capacitación sobre elementos de protección, la salud hospitalaria (manejo de epidemias, virus), los procedimientos definidos para el ingreso de personal nuevo (habilidades, experiencia, medidas de seguridad) y los planes de comunicación en crisis.

La dimensión de tecnología de información forma parte de los factores de interrupción, dentro de los aspectos se encuentra la confiabilidad, la cual se debe manejar el control, gestión y mantenimiento de los servidores, bases de datos, redes, almacenamiento, aplicaciones y sistemas de información. Los procesos deben estar definidos e implementados para el soporte ante incidentes.

El aspecto de la disponibilidad plantea que los procedimientos deben estar definidos e implementados para el mantenimiento preventivo y correctivo, contar con planes o procedimientos de contingencia y sitios alternos de procesamiento. Contar con inventario (stock) de componentes o partes críticas y capacidad de enlaces de transmisión y redundancia. El aspecto de la recuperabilidad ante incidentes de sistemas tecnológicos, es obtenido mediante la realización de pruebas de recuperación y retorno de los sistemas tecnológicos,

procesos de restauración de cintas de respaldos, respaldos de datos, al igual que requerirles a los proveedores de planes de contingencia en caso de que tengan alguna interrupción que afecte a la OC.

En la dimensión de infraestructura física los factores a tomar en cuenta para evitar interrupción o disminuir el tiempo de la misma, son la preparación ante emergencias, estas son acciones a tomar para prevenir la materialización de los riesgos que pongan en peligro la integridad de las personas y activos. Ante los incendios se deben definir planes de atención y evacuación ante incendios.

El aspecto energético debe contar con controles predictivos o preventivos y mecanismos correctivos de fallas relacionadas con aire acondicionado, suministro de energía y potencia eléctrica requerida por equipos electrónicos o mecánicos. Y por último la seguridad y accesos, donde se debe tomar en cuenta el control de accesos en áreas críticas restringidas, así como la entrada de visitantes, control de recursos dentro de las edificaciones.

Los aspectos de cada una de las dimensiones mencionadas se evalúan la presencia o carencia de características de excelencia y bajo el juicio y experiencia del equipo de proyecto del Organismo Coordinador Del Sistema Eléctrico Nacional Interconectado De La República Dominicana. Esta evaluación comparada contra estándares y prácticas líderes permite identificar mecanismos y/u oportunidades de mejoras. En adición a esto, los resultados del presente informe han sido validados por el personal responsable en la institución de cada uno de los procesos definidos en el alcance anteriormente planteado.

Para cada uno de los riesgos se evalúa la probabilidad, el impacto y el control que permita mitigar o reducir el nivel de riesgo inherente. Para la evaluación de riesgo debemos conocer las amenazas que existe para el organismo coordinador. Ejemplos: ausencia del plan de continuidad, insuficiente gestión de monitoreo, aplicativos mal diseñados, falla en la seguridad de la información, inundación, incendio, robo de datos, sabotaje, entre otros.

Identificando proactivamente las vulnerabilidades podemos controles y reducir el impacto a los que estamos expuestos. En el anexo definiciones será ampliado más detallado los conceptos vistos en esta investigación.

La definición de cada una de las clasificaciones de riesgo inherente siguientes fue posible al esfuerzo realizado por el equipo del Organismo Coordinador Del Sistema Eléctrico Nacional Interconectado De La República Dominicana esto permitió valorar los riesgos residuales de continuidad. La clasificación de probabilidad de ocurrencia utilizada (Anexo 7). También se utilizó una clasificación para el impacto del riesgo (Anexo 8).

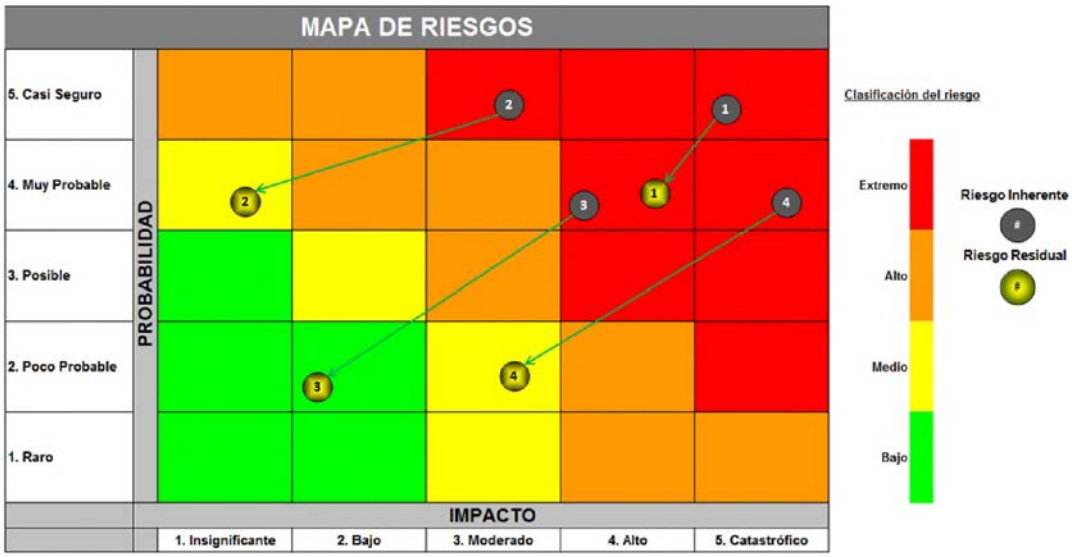
La clasificación de control es una clasificación utilizada para los controles para determinar el nivel de robustez, por ejemplo, un control fuerte es aquel que es preventivo, está documentado e implementado, es efectivo para mitigar los riesgos y siempre es aplicado con la intensidad y rigurosidad esperada. Como antes habíamos mencionado dentro de la clasificación se determina qué tipo de control es el control valga la redundancia, estos tipos de controles puede ser preventivos, correctivos o no hay control (Anexo 9 y Anexo 10)

Los riesgos identificados son ordenados en una matriz de colores con escalas de probabilidad e impactos de 1 al 5, según el cálculo del riesgo inherente y residual. Cada riesgo es identificado con un círculo y un color distintivo según su naturaleza, los círculos grises con letra blanca representan el riesgo inherente (antes del control) y los círculos amarillos con letra negra representan el riesgo residual (después de aplicar el control).

Figura 11,

Mapa de valoración de riesgos

Fuente: Elaboración propia



Los riesgos resultantes se clasifican de la siguiente manera:

Tabla 15,

Clasificación riesgos resultantes

Fuente: Elaboración propia

Extremo	El impacto del evento es "Catastrófico" y la probabilidad "Poco Probable" o "Casi Seguro". El impacto del evento es "Alto" y la probabilidad "Posible" o "Casi Seguro". El impacto del evento es "Moderado" y la probabilidad "Casi Seguro".
Alto	El impacto del evento es "Catastrófico" y la probabilidad "Raro". El impacto del evento es "Alto" y la probabilidad "Raro" o "Poco Probable". El impacto del evento es "Moderado" y la probabilidad "Posible" o "Muy Probable". El impacto del evento es "Bajo" y la probabilidad "Muy Probable" o "Casi Seguro". El impacto del evento es "Insignificante" y la probabilidad "Casi Seguro".
Moderado	El impacto del evento es "Moderado" y la probabilidad "Raro" o "Poco Probable". El impacto del evento es "Bajo" y la probabilidad "Posible". El impacto del evento es "Insignificante" y la probabilidad "Muy Probable".
Bajo	El impacto del evento es "Bajo" y la probabilidad "Raro" o "Poco Probable". El impacto del evento es "Insignificante" y la probabilidad "Raro" o "Posible".

Al realizar la evaluación de riesgos de continuidad enfocados en las dimensiones de procesos y personas, se identificó que existen oportunidades de mejora para lograr un nivel ideal en la administración de continuidad de negocio. Esta evaluación se centró en las áreas con los procesos de más impacto para la organización. Dentro del área de Operaciones tenemos los procesos de Operación de Tiempo Real y Programación de la Operación, de igual forma dentro del área comercial tenemos los procesos de Transacción y Mediciones.

Se realizó un recorrido por estas áreas del negocio y se observó la gestión de los procesos, los proveedores, la gestión del conocimiento, la percepción del servicio de tecnología y las medidas preventivas adoptadas para mantener los niveles de seguridad y salud ocupacional, que ayuden a mitigar riesgos de continuidad en la dimensión de personas. De los mismo se obtuvieron un total de 25 controles. (Anexo 11)

6.3. Evaluación y selección de estrategias

Según los resultados de la evaluación de riesgo, existen oportunidades de mejora en los riesgos relacionados a Gestión del Conocimiento, Seguridad Laboral y Gestión de Proceso. Así como se tienen niveles de impactos bajos en riesgos, también se encuentran los riesgos residuales (ya aplicado el control) que tiene impacto alto y extremos, por lo que se estará dando prioridad a los mismo debido a su impacto, se pueden visualizar en el anexo 16.

El resultado encontrado en los riesgos de gestión del conocimiento es no contar con estrategias de retención de empleados claves y la no definición de estrategias que permita retener al personal clave ante ofertas exteriores o por falta de incentivos laborales. En la seguridad laboral existe la imposibilidad de responder ante situaciones de emergencia por falta de un proceso de gestión de emergencia, no se ha implementado un proceso de gestión de emergencia laborales con guías de actuación inmediata para controlar daños sobre personas y/o los bienes durante un evento general no esperado, dificultad para responder

oportunamente a situaciones de emergencias por falta de capacitación en manejo y control de situaciones críticas, no se realizan capacitaciones periódicas en manejo y control de situaciones de emergencia a todo el personal, a fin de que pueda responder de manera oportuna y eficiente ante posibles situaciones críticas, imposibilidad de evacuar efectivamente al personal por no contar con un plan de evacuación ante emergencias y por último, no se cuenta con un plan de evacuación ante emergencias en la organización para el desplazamiento de las personas en una situación de peligro inminente a un sitio seguro.

Finalmente, en la gestión de procesos no cuenta con un plan alterno de trabajo para los procesos críticos de la institución, que contenga procedimientos de recuperación y/o contingencias y la organización no cuenta con planes de trabajo que considere los procedimientos alternos a ser llevados a cabo ante cualquier evento o suceso que afecte la continuidad de los procesos críticos, ya sea de carácter natural, físico, tecnológico o humano.

Para los riesgos de tecnología de información se evaluaron un total de 12 controles divididos de la siguiente manera:

Tabla 16,

Riesgos en tecnología de información

Fuente: Elaboración propia

Dominio	**Riesgo**
Disponibilidad	1 Falta de disponibilidad de servicios tecnológicos 2 Falta de disponibilidad por dependencia con proveedores 3 Incremento de fallas de componentes de tecnología
Recuperabilidad	4 Activación de contingencia a destiempo 5 Insuficiencia en abastecimiento de componentes tecnológicos 6 Insuficiencia en la provisión de servicios (soporte) al momento de salir de contingencia algún proveedor de la empresa 7 Afectación de las operaciones por no disponer de un centro alterno de tecnología

	8 Deficiencia en la recuperación de información crítica y/o necesaria
Confiabilidad	9 Falta de procedimientos para evaluación de eventos 10 Afectación o falla de las aplicaciones o de su rendimiento por cambios no programados 11 Fallas en la activación de contingencias por desconocimiento de la interdependencia entre aplicaciones 12 Información confidencial expuesta por no disponer de mecanismos de protección de datos.

Para poder estar preparados ante eventualidades, debemos trabajar estos 3 renglones dentro de los riesgos de tecnología de la información, disponibilidad, recuperabilidad y confiabilidad. A continuación, se detallan los riesgos los riesgos catalogados con mayor impacto y deben ser los primeros en ser mitigados:

Iniciando con el renglón de disponibilidad, existe una dependencia con proveedores externos la cual representa un punto único de falla al momento de una contingencia. Actualmente el enlace primario y en enlace redundante para la comunicación del sistema SCADA entre el Organismo Coordinador y la Empresa de Transmisión Eléctrica Dominicana (ETED) se encuentra contratado con un mismo proveedor.

En el renglón de disponibilidad en las tecnologías de la información, no se cuenta con un centro alternativo de tecnología para tomar control del centro primario ante una contingencia, por lo que toda información y equipos tecnológicos del Organismo Coordinador se encuentran en posible riesgo al estar concentrados en un único punto de falla.

A nivel de confiabilidad, no se cuenta con procedimiento formal para solicitud, evaluación, aprobación o rechazo e implementación de controles de cambio que permita hacer seguimiento del ciclo de vida de una aplicación o modificación. De igual forma, no se cuenta

con mecanismos de cifrado de información a fin de que no puedan ser entendidos o interpretados por personal no autorizado y así proteger la confidencialidad de los datos.

Con el fin de evaluar los riesgos en infraestructura física se realizaron recorridos en las instalaciones de la sede del Organismo Coordinador, en la cual se concentran el personal administrativo, y la infraestructura tecnológica.

Durante el recorrido por las instalaciones se observaron facilidades como: oficinas, parqueaderos, archivos, escaleras y salidas de evacuación, aires acondicionados, zona de planta eléctrica, entorno de las instalaciones, bodegas de almacenamientos, entre otros. El análisis del estado de preparación en aspectos físicos está dividido en cinco componentes a evaluar, el estado de preparación para atender emergencias y administración de crisis, los riesgos generadores de incendios, el estado de preparación para atender un corte de energía (Black-Out), la preparación en temas de seguridad física y accesos, y aires acondicionados y controles ambientales.

En el análisis comparamos el estado actual frente a buenas prácticas y estándares de seguridad física de edificaciones, estándares de construcción y preparación de emergencias (NFPA 10, 13, 72, 75, 76) y gestión de centros de cómputos (TIA-942).

Básicamente, estos estándares ilustran un estado ideal y un estado mínimo deseable, dentro de los cuales se deben mantener las métricas de una organización para demostrar su estado de preparación en la administración de los riesgos. Al hacer la comparación se identificó que hay oportunidades de mejora en los cinco componentes mencionados anteriormente.

Para los riesgos de instalaciones físicas se evaluaron un total de 43 controles los cuales se encuentran divididos en preparación ante emergencias, incendio, potencia eléctrica, aire acondicionado y centro de cómputo. Los riesgos más destacados que deben ser atacados

con más urgencia, debido a su calificación de impacto son la preparación ante emergencias, aires acondicionados, potencia eléctrica, centro de computas, seguridad y accesos.

En la preparación ante emergencias se destacan la falta de un plan de manejo de emergencias, es decir, no se cuenta con un plan de manejo de emergencia formalizado que contemple aspectos tales como: procedimientos, capacitación, roles y responsabilidades ante una situación de emergencia.

El OC carece de brigadistas que fungen como personal de socorro y guías ante una emergencia y el personal no está capacitado para utilizar los extintores en caso de emergencia. Es necesario que estos brigadistas cuentan con equipos especiales tales como: radios, linternas, pilas, cascos, chalecos (en algunos casos), y otros elementos indispensables para la atención de una emergencia. Las instalaciones no cuentan con señalización de las rutas de evacuación en caso de emergencias, tampoco están señalizadas las salidas. Ante una situación de emergencia no se identifican señalizaciones de ruta de escape para la evacuación del personal y visitantes de las instalaciones.

Las instalaciones del OC no cuenta con alarmas contra incendios, no fueron contempladas en el levantamiento. Las alarmas de detección de humo alertan al personal ante posibles situaciones de evacuación por focos de incendio. En la evaluación se evidenció que solo el centro de datos cuenta con alarma sonora. Las instalaciones tampoco cuentan con sistema automático de sofocación o extinción de incendios, únicamente el centro de datos cuenta con sistema automático de sofocación y extinción de incendios, pero el químico utilizado es el incorrecto para los componentes eléctricos y pudiera ocasionar pérdidas financieras y de activos tecnológicos.

Ninguna de las áreas del OC cuentan con sensores de temperatura y humedad. El aire acondicionado de la sala de operaciones en tiempo real y donde se encuentra los servidores,

no cuenta con un sensor de temperatura y humedad que permita detectar variaciones ambientales como aumento de temperatura y humedad.

Se determinó que no se realizan mantenimientos programados y periódicos de la planta eléctrica y del UPS, ni pruebas de funcionalidad. Carecen de un plan de mantenimiento para prevenir fallas. Dichos mantenimientos de la planta eléctrica y UPS son realizados esporádicamente o en caso de presentarse situación de fallas. No se programan pruebas de funcionalidad. Se pone a prueba la funcionalidad de la planta y del UPS cuando se presenta ausencia de energía eléctrica.

En el centro de datos no cuentan con controles que ayuden a monitorear aspectos como el nivel de agua en caso de inundaciones. No se cuenta con sensores de niveles de agua en caso de inundaciones que permitan tomar acciones de manera oportuna a fin de resguardar el equipamiento tecnológico. Se identificó que lo servidores tampoco cuenta con una altura adecuada para en caso de inundaciones la altura proteja el mismo.

En el centro de datos no se disponen de mecanismos electrónicos de restricción de accesos. Al no contar con mecanismos de restricción, esto aumenta el riesgo de interrupciones en caso de que algún intruso penetre el cuarto de servidores. El acceso al mismo se restringe mediante una cerradura común y cuya llave está en poder del personal de tecnología. De igual manera se identificó que la puerta de acceso es de madera y no evita ingresos forzados. No se cuenta con un mecanismo para registrar los accesos y las acciones a realizar del personal y/o visitantes que ingresan al centro de cómputo al igual que al área donde se encuentra los servidores.

La seguridad y accesos en el OC carece de controles de acceso físico. Durante la evaluación se pudo observar que no existen detectores de humo, no se realizan un control de registro del personal que visita, está permitido el acceso directo con vehículos a las instalaciones, no se realizan inspecciones de elementos que puedan portar los visitantes antes

de entrar y antes de salir de las instalaciones y no se realzan rondas periódicas por parte del personal de seguridad. De igual forma no se dispone de un área para el monitoreo de las cámaras de vigilancia. El sistema de vigilancia de cámaras no contempla un monitoreo activo que permita tomar acciones preventivas ante situaciones delictivas o irregulares.

6.4. Estrategias de Continuidad del Negocio

Las estrategias planteadas, cuatro de ellas cubren la integridad de los procesos, personas e infraestructura física y la quinta hace referencia al pilar tecnológico por la cual está montada las operaciones de la OC. Las estrategias en su conjunto se deben implementar para lograr que el OC (Organismo Coordinador) tenga continuidad de negocio.

La primera estrategia hace referencia al sistema de gestión de continuidad de negocio (BCM). Un sistema para administrar la continuidad se fundamenta en el ciclo de sistemas de gestión y mejora continua, y define el conjunto de políticas, procesos, funciones y estructura que ayudan a establecer el marco de actuación bajo el cual se administra la continuidad.

Tanto las políticas como los procesos de administración de la continuidad son la base para alcanzar un ambiente mejorado y dispuesto en organizaciones que buscan constantemente mantener y facilitar la continuidad de sus operaciones clave que son soporte del negocio. Lograr mantener la continuidad del negocio es una habilidad que requiere la definición de un marco de referencia proactivo que facilite la alineación de las personas, los procesos, la tecnología y las actividades del día a día.

El marco de referencia se establece mediante la implantación, adopción y cumplimiento de un sistema para administrar la continuidad, enmarcado en: políticas para administrar la continuidad, procesos para administrar la continuidad y, por último, estructura organizacional para administrar la continuidad.

Las políticas para administrar la continuidad hacen referencia a las acciones y actividades que ayudan a mantener la continuidad que deberán ser ampliadas e implantadas

por el OC, están enmarcadas para cada una de las dimensiones que de alguna forma inciden o impactan la continuidad de las operaciones de los servicios y/o procesos críticos del negocio. Las políticas que servirán como base para establecer el programa de continuidad son los compromisos directivos y de participantes, las instalaciones físicas, los procesos de negocio, las personas y la tecnología de información.

Los procesos de administración de la continuidad se definen como la gestión disciplinada de mejoramiento y monitoreo continuo con el fin de proporcionar niveles de continuidad acorde con las necesidades del negocio. Estos procesos se componen de cuatro fases basadas en el ciclo de sistemas de gestión de calidad.

El objetivo de la fase establecer (planear) es determinar que es importante para el OC, planear acciones para mantener la continuidad, definir roles y responsabilidades, y mejorar la cultura organizacional en tema de continuidad. En la fase implementar y operar (hacer) es determinar el estado actual de la continuidad, aspectos que representan riesgos e impactos para la continuidad del OC identificar y desarrollar soluciones de continuidad, definición de arquitecturas, políticas, normas y procedimientos orientados a elevar los niveles de continuidad. En la fase monitorear y revisar (verificar) es verificar el cumplimiento de las políticas y procedimientos definidos para mantener la continuidad. Monitorear los acuerdos de servicio que permitan mejorar y mantener la continuidad de la operación del OC. Por último, en la fase de mantener y mejorar (actuar) es actualizar, probar y entrenar los planes de continuidad de negocio y respuesta a incidentes. Definir acciones correctivas y de mejoramiento al sistema de continuidad, y a los productos y servicios del OC.

La estructura organización para administrar la continuidad según la norma ISO 22301, recomienda que sea un área fuera de la operación diaria, la que se encargue de liderar el Sistema de Gestión de Continuidad de Negocio (BCM). La independencia de las operaciones

diarias es un factor determinante para que un área con estas características sea quien lidere el BCM del OC.

Figura 12,

Estructura del Área de Gestión de la Continuidad

Fuente: Elaboración propia

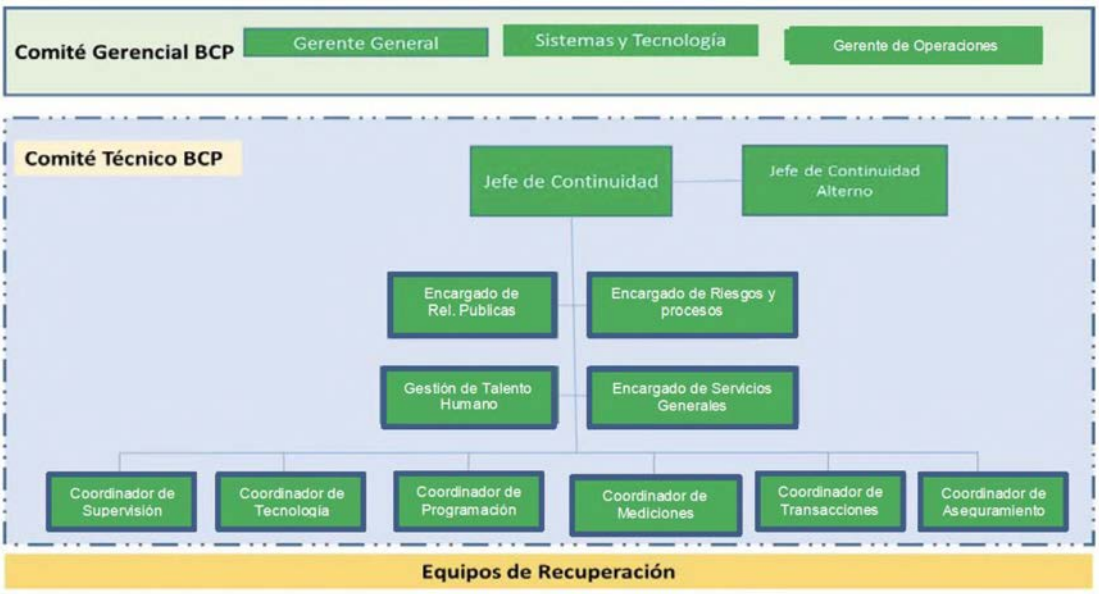
La segunda estrategia indica los procesos y gobernabilidad que debe llevar el plan de continuidad del negocio. Para ellos debe existir una política para administrar el plan de continuidad contemplará las pautas para gestionar los recursos mínimos necesarios para la recuperación de las operaciones del OC, administrar los acuerdos con proveedores, involucrar a todo el personal del OC los cuales deberán ser entrenado y capacitado en los procedimientos definidos.

El gobierno del plan de continuidad busca definir los equipos y el personal responsable de ejecutar las actividades para el funcionamiento del Plan de continuidad. Se considera que todos los participantes asignados tienen el perfil adecuado para ejecutar las actividades asignadas. El gobierno contiene los equipos de Comité Gerencial BCP, Comité Técnico BCP y Equipos de Recuperación.

Figura 13,

Gobierno del Plan de Continuidad

Fuente: Elaboración propia



El comité gerencial BCP es el nivel estratégico del plan y está encargado de tomar las decisiones frente al manejo de situaciones de crisis, que al presentarse interrumpan las operaciones normales del OC. Igualmente, valida y aprueba las estrategias planteadas para afrontar este tipo de situaciones. En el momento de declaración de contingencia velará por el cumplimiento del plan, la salvaguarda de la vida y activos del OC, además solicitará los informes del manejo del evento al comité técnico BCP.

El comité técnico BCP es el encargado del nivel táctico del plan, es quien realiza la evaluación inicial de los eventos de interrupción o crisis que se presenten y que afectan la operación normal del OC. Además, velará por actualizar y probar el Plan de continuidad en cada uno de sus componentes. Y como parte del plan capacitar al personal que forma parte de este plan.

Los equipos de recuperación estos equipos componen el nivel operativo del Plan de continuidad, están encargados de la ejecución de los procedimientos y actividades necesarias para salvaguardar la vida de las personas, los activos de la compañía, recuperar las

operaciones de procesos críticos de negocio y la tecnología. Además, deben colaborar con el comité técnico BCP por mantener actualizado y probado el Plan de continuidad.

La tercera estrategia busca establecer un centro alterno de operaciones con el objetivo de restaurar la operatividad de los procesos críticos de negocio afectados por un evento, en un centro alterno de operación y tiene como alcance el establecimiento de un centro alterno de operaciones, basado en los requerimientos mínimos identificados en el análisis de impacto del negocio (BIA).

El centro alterno debe contar con los requisitos mínimos para que el personal de operaciones pueda realizar las operaciones del día a día. Debe contar con una ubicación estratégica para el fácil trasporte del personal. Además de contar con respaldo energético, conexión a internet y red interna de los servidores.

La cuarta estrategia plantea que se deben definir los planes de recuperación de negocio. A fin de que las áreas de servicio puedan prepararse en caso de interrupción de los procesos, deben definirse los planes que establezcan los procesos y responsabilidades que deben llevarse a cabo ante un evento de interrupción. Los objetivos de esta estrategia son identificar los posibles escenarios de interrupción que se puedan presentar en los procesos de negocio, definir las estrategias de recuperación para mantener la continuidad en cada uno de los escenarios identificados, definir los servicios que pueden prestarse en cada proceso, dependiendo del escenario, interrupción y la estrategia de recuperación y el último objetivo es Identificar posibles riesgos, mecanismos de control, registros de información necesarios para la implementación de las estrategias de recuperación. Estas estrategias contemplan los procesos que hacen parte de la línea de continuidad de los servicios, es decir, aquellos identificados como procesos críticos en el Análisis de Impacto del Negocio (BIA).

La quinta y última estrategia establece la posibilidad el escenario de riesgo de que se presente una falla que inhabilite los sistemas de información de apoyo (aplicaciones) y de los equipos SCADA, de los cuales dependen los procesos de operaciones del negocio para el desarrollo normal de sus actividades.

Dos posibles escenarios de interrupción pueden ocurrir, como un evento que inhabilita los sistemas de información de apoyo a las operaciones, y un evento que inhabilita los sistemas de operaciones de tiempo real SCADA. Para los escenarios antes mencionados donde se asume la afectación y por ende, la no disponibilidad de la infraestructura técnica de las aplicaciones de índole crítica y el Sistema SCADA, se inició el análisis y definición de las estrategias de recuperación tecnológica para las aplicaciones identificadas en el análisis de impacto al negocio con nivel crítico "Indispensable", desplegando la infraestructura tecnológica que está involucrada y que conjuntamente permite asegurar los niveles de operación requeridos en condiciones normales. A continuación, las aplicaciones consideradas para estas estrategias, basada en los resultados de análisis de impacto de negocio:

Tabla 17,

Aplicaciones Críticas Estrategia Recuperación Tecnológica

Fuente: Elaboración propia

Sistemas	Otros Aplicativos
Tiempo de Recuperación: 0 a 30 minutos	
• SCADA • REGIO	• MODOM • DIGSILEN
Tiempo de Recuperación: 1 a 3 días	
• PSS/E • PFT • Internet • Microsoft Office • Prime Read	• Máquina virtual para correr PSS/E con Windows 98

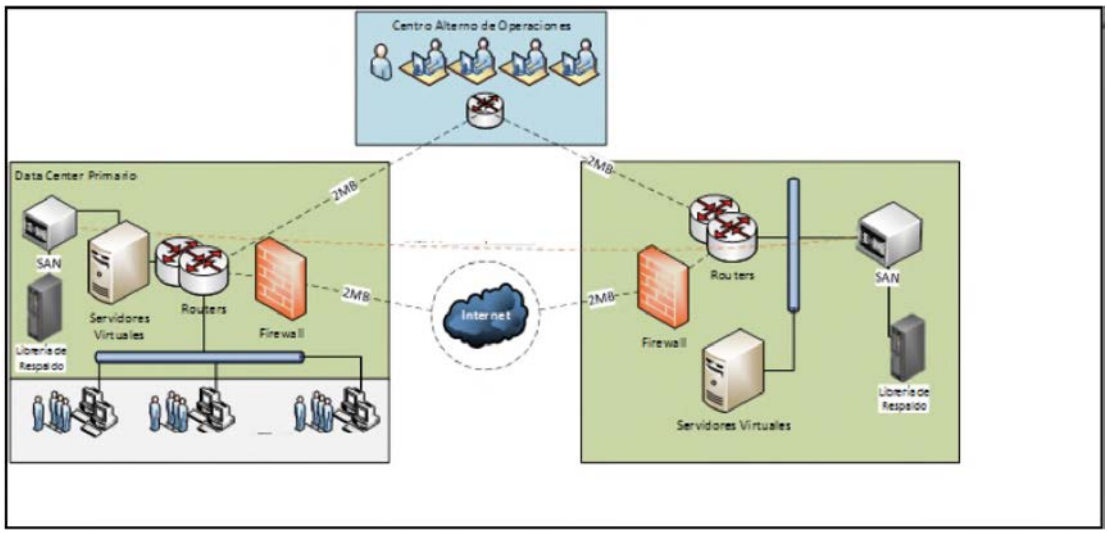
La estrategia que se describe a continuación incluye las definiciones generales de la solución de contingencia, replicación y respaldo a ser implementada por el OC para sus aplicaciones tecnológicas. En general, la solución propuesta involucra la disposición de sistemas redundantes y virtualizados o niveles de recuperación altamente automatizados de las aplicaciones con MTO menores a 1 hora. Las aplicaciones que entran en este esquema de solución son SCADA, REGIO, MODOM y DIGSILEN, respaldados en un centro de datos alterno independiente a la infraestructura de procesamiento actual.

La estrategia de recuperación de la infraestructura de tecnología en un centro de datos alterno para periodos menores a una hora requiere de la automatización de los procesos de recuperación en donde la intervención humana sea muy poca y solo se requiera cuando sea necesario tomar decisiones estratégicas. Este centro de datos alterno debe estar interconectado con el centro de datos primario para la replicación de la información y debe estar interconectado para que los usuarios finales puedan acceder a las aplicaciones de manera oportuna.

Figura 14,

Topología de Red Propuesta Con Data Center Alterno

Fuente: Elaboración propia



En relación con la solución de redes de datos, la estrategia no modifica la topología actual en la sede principal. Se debe implementar una solución para garantizar el tráfico de información entre la sede principal con el centro de datos alterno propuesto. Se plantea entonces la instalación y adecuación de un par de enrutadores de borde, conectados entre sí y con conexiones redundantes hacia la red del OC como alternativa de respaldo.

Para la replicación de información entre el centro de cómputo primario y el centro de cómputo alterno se recomienda tener un canal de comunicaciones adicional. El ancho de banda de este canal, dada una transaccionalidad media de las aplicaciones que se van a replicar entre ambos sitios, se ha estimado en 2MB para realizar la trasferencia de datos. Por otro lado, se requiere establecer un mecanismo de monitoreo del tráfico para determinar si la capacidad estimada sería suficiente.

Para garantizar el establecimiento de la conexión a los sistemas del sistema de cómputo primario y alterno, se propone implementar un esquema de enmascaramiento de direcciones IP a través de los sistemas de enrutamiento instalados en el centro de datos alterno. Esto, debido a que muchas aplicaciones están ligadas a la dirección IP asignada, y tener un esquema de enmascaramiento permitirá brindar transparencia en la conexión del usuario para situaciones donde se requiera utilizar uno u otro ambiente. Los requerimientos en aspectos de telecomunicaciones incluyen:

Tabla 18,

Requerimiento de Equipos de Telecomunicaciones

Fuente: Elaboración propia

Comunicación	Data Center Primario	Data Center Primario	Centro Alterno de Operación
Routers	Dos routers de borde, con interfaces LAN y WAN.	Dos routers de Borde, con interfaces LAN y WAN.	Un router de borde, con interfaces LAN y WAN.
Switches	Equipos compatibles con los instalados el día de hoy.	Equipos provistos por el proveedor de servicios de data center.	Switches de acceso que en forma conjunta entreguen al menos 12 puntos de conexión UTP.
Enlaces	• Un enlace dedicado entre la sede principal y el centro de cómputo alterno		
	• Dos enlaces dedicados entre el Centro Alterno de Operaciones y los Data Centers Primario y Alterno.		

Para la solución de seguridad tanto en el centro de datos primario como en el centro de datos alterno, se propone la implementación de sistemas de seguridad perimetral que permitan ejercer control sobre el tráfico entrante y saliente de los enlaces que intercambian información permanentemente con entes y/o redes externas como Internet. Según los requerimientos identificados en materia de seguridad perimetral, se requerirá la configuración de la solución actual de firewall en los siguientes componentes:

Tabla 19,

Requerimiento de Equipos de Seguridad

Fuente: Elaboración propia

Sistema	Data Center Primario	Data Center Primario	Centro Alterno de Operación
Sistema de seguridad Perimetral con capacidad para establecer VPNs site to site.	(1) Firewall	(1) Firewall	(1) Firewall

Para solucionar el procesamiento de información, en el centro de datos alterno se propone la virtualización de toda la infraestructura de respaldo que ha sido dimensionada para las aplicaciones con niveles de criticidad "indispensable". Esta sugerencia se hace por las múltiples ventajas que este tipo de tecnologías le aportan a la compañía en aspectos económicos, logísticos y administrativos, dentro de las cuales se destacan:

Llevando a cabo la virtualización, se garantiza la asignación dinámica de recursos, de esta forma tener una administración eficiente del hardware disponible y poder incrementar en las máquinas virtuales los recursos de memoria RAM, número de procesadores y administración de cuotas de disco, dependiendo del performance que sea necesario para dar un cubrimiento efectivo a la prestación de los servicios.

Tanto para el centro de datos primario como para el Alterno, se identifica el uso de tecnología para el almacenamiento de información se deben implementar soluciones que permitan la replicación de datos de manera confiable y eficiente. Un esquema sugerido sería la utilización del conjunto redundante de discos independientes en arreglo RAID 5, cuyas

ventajas consisten en poder realizar operaciones de lectura y escritura haciendo un uso más eficiente de las unidades de disco, lo que acelera los pequeños procesos de escritura en un sistema multiprocesador y facilita una cantidad de almacenamiento usable.

La protección de los datos en RAID 5, reside en la información de la paridad que se utiliza para reconstruir los datos si una unidad del grupo RAID falla o sufre una avería. Entre los inconvenientes, se encuentran: la necesidad de un mínimo de tres (y, normalmente, cinco) discos por grupo RAID, un nivel de rendimiento del sistema de almacenamiento significativamente inferior mientras se lleva a cabo la reconstrucción de una unidad, y la posibilidad de perder totalmente los datos de un grupo RAID si falla una segunda unidad mientras se está realizando la reconstrucción de la primera.

La replicación de datos es el procedimiento establecido para proteger los datos críticos del negocio de forma periódica mediante el uso de mecanismos de transferencia de datos confiables y flexibles. A través de la puesta en marcha de una estrategia de replicación de información, se busca la replicación de datos en un sitio alterno como respaldo para situaciones donde los datos del sistema en el ambiente de producción en el sitio primario se pierden.

Existen muchas tecnologías de replicación, sin embargo, se distinguen dos métodos de replicación: síncrona y asíncrona. La replicación síncrona es el nivel más alto para los puntos objetivos de recuperación (RPO) y los tiempos objetivos de recuperación (RTO), con RPO's donde no hay pérdida de datos, y RTO's que por lo general varían entre unos segundos y unos pocos minutos. La replicación síncrona funciona de manera que no se completan ni reconocen las operaciones de escritura locales hasta que no se han completado y reconocido las operaciones de escritura remotas. Esto implica que el rendimiento del sistema de información primario está directamente relacionado con el rendimiento del sistema de información de respaldo remoto.

Por otro lado, mediante la replicación asíncrona, las operaciones de escritura locales quedan completadas y reconocidas antes que las operaciones de escritura remotas. La replicación remota asíncrona es una técnica de "almacenamiento y envío" (store-and-forward), técnica que reduce las I/O y los retrasos por esperas. Esto significa que el RPO por la pérdida de datos puede variar de segundos a minutos, y en otros casos incluso horas. La ventaja de la replicación remota tanto síncrona como asíncrona es la mínima (asíncrona) o nula (síncrona) exposición al riesgo de pérdida de datos durante un desastre. Una ventaja adicional es la posibilidad de una rápida recuperación de datos cuando se produce un desastre.

La replicación remota no requiere de agentes en el servidor, y ofrece soporte para servidores y aplicaciones heterogéneos. Las aplicaciones de replicación remota a menudo tienen un precio elevado, la infraestructura suele ser costosa. Otra desventaja es que la replicación remota no impide los desastres en cadena (rolling disaster), ni ataques de ramsomware, ni la corrupción o el borrado accidental de los datos. Si los datos se han corrompido, dañado o eliminado del sitio primario, también lo estarán en el sitio alterno. Los productos de replicación remota asíncrona marcan la fecha y hora (timestamp) de cada operación permitiendo la recuperación a un punto en el tiempo anterior a la corrupción o la eliminación. Esto significa que se deben implementar otros procedimientos además de la replicación remota para permitir la recuperación de los datos corruptos, dañados o eliminados.

El backup y la recuperación a partir de cinta, la duplicación remota como almacenamiento o el envío de registros de bases de datos constituyen soluciones tradicionales en materia de protección de datos y recuperación ante desastres. Por desgracia, esas soluciones no son capaces de satisfacer objetivos contundentes en cuanto a punto de recuperación (RPO, protección de datos) y tiempo de recuperación (RTO, disponibilidad de datos). Los esquemas de planteamiento para la recuperación de los sistemas en el centro de

cómputo alterno estarían diversificados de acuerdo a los valores RTO y RPO determinados en el BIA.

Con la solución de virtualización se puede desarrollar un esquema de respaldo que permitiría tener un respaldo completo de los servidores virtuales en una locación alterna, simplificando la administración mediante la replicación del nivel de máquina virtual y permite tener objetivos de punto de recuperación en tiempos significativamente bajos. La replicación de las máquinas virtuales a través de esta herramienta, copia solo bloques modificados al sitio de recuperación. Este enfoque reduce la utilización del ancho de banda y permite obtener objetivos de puntos de recuperación (RPO, recovery point objectives) más efectivos que la replicación manual del sistema completo de las máquinas virtuales, garantizando el uso eficiente de la red mediante el seguimiento de las áreas del disco que se modificaron y la replicación únicamente de estos datos.

En la modalidad de Housing o Colocation el cliente requiere comprar y administrar su propio hardware y software, esto implica que se debe tener personal en sitio para el lugar donde se elija la ubicación del centro de datos alterno. El proveedor del servicio solamente suministra el espacio y los requerimientos de facilidades (aires, sistema eléctrico, entre otros). El sistema operativo, las aplicaciones son gestionadas por el personal del OC, así como el mantenimiento del hardware. En esta modalidad tendría que invertir en nueva infraestructura para incluir los aplicativos críticos que en la actualidad no cuenten con alternativas de recuperación.

La solución de un centro de datos alterno modalidad hosting, se enfoca en la contratación del servicio de centro de datos alterno en modalidad de hosting gestionado. En el ambiente de hosting el proveedor es el dueño y responsable de las facilidades incluyendo la infraestructura de telecomunicaciones, hardware, software, sistemas operativos,

administración de las aplicaciones, seguridad física y lógica y el soporte técnico. El trabajo del cliente debe estar enfocado en gestionar la administración por parte del proveedor.

En la modalidad de implementación de un centro de datos alterno propio el cliente requiere implementar y administrar toda la infraestructura. En esta alternativa, el OC tendría que invertir en todo lo que se requiera para incluir los aplicativos críticos que en la actualidad no cuenten con alternativas de recuperación. Esta solución aísla riesgos relacionados con el almacenamiento y eventos de desastre en sitio físicos, y requiere replica continua (sincrónica) de información entre el sitio primario hacia el sitio alterno.

La modalidad centro de datos alterno modalidad nube se enfoca en el nuevo paradigma que permite ofrecer servicios de computación a través de Internet, llamado Cloud Computing (Nube), el cual es un modelo de aprovisionamiento rápido de recursos tecnología de información (TI) que potencia la prestación de servicios TI y servicios de negocio, facilitando la operativa del usuario final y del prestador del servicio. Esta infraestructura plantea una escalabilidad capaz de atender fuertes cambios en la demanda no previsibles a priori, sin que esto suponga apenas un incremento en los costos de gestión.

Con esta modalidad se contaría como un respaldo para las aplicaciones críticas y mejor facilidad de acceso a las aplicaciones desde las distintas localidades a través de Internet y de los funcionarios del OC cuando se encuentren en una ubicación remota. Esta alternativa cuenta con varias opciones de implementación, sin embargo, el esquema sugerido, por sus facilidades de flexibilidad y seguridad, es el de nube público-privada (híbrida).

Este esquema incluye la ubicación de la infraestructura en una nube ubicada fuera de las instalaciones de la compañía, a través del Internet (nube pública); sin embargo, el proveedor de servicio crea una nube privada dedicada sólo para el OC dentro de sus facilidades y detrás de sus firewalls proveyendo una red privada virtual (VPN) para seguridad adicional.

6.5. Plan de Continuidad

Este plan busca establecer los procedimientos que se deben ejecutar para mantener la continuidad de los servicios considerados como críticos para el Organismo Coordinador del Sistema Eléctrico Nacional Interconectado y que son parte del alcance de este plan. Los procedimientos del plan de continuidad van ayudar con la efectividad de las operaciones ante un evento de interrupción.

El plan de continuidad del negocio se establece de acuerdo a las informaciones obtenidas en el análisis de impacto del negocio, la evaluación de riesgo de continuidad y las estrategias planteadas enfatizando los procesos elegidos. El plan de continuidad del negocio es conformado por el plan de comunicaciones antes incidentes, plan de administración de incidentes, plan de recuperación de negocio y plan de recuperación tecnológica.

6.5.1. Plan de Comunicaciones ante incidentes

El plan de comunicaciones plantea los lineamientos para establecer una efectiva comunicación durante un estado de contingencia. En este Plan se encuentran definidas las operaciones y la asignación de roles y responsabilidades al equipo de Relaciones Públicas durante la ocurrencia de un evento disruptivo. De igual forma, debe tomarse en cuenta el protocolo de comunicación definido por el Organismo Coordinador.

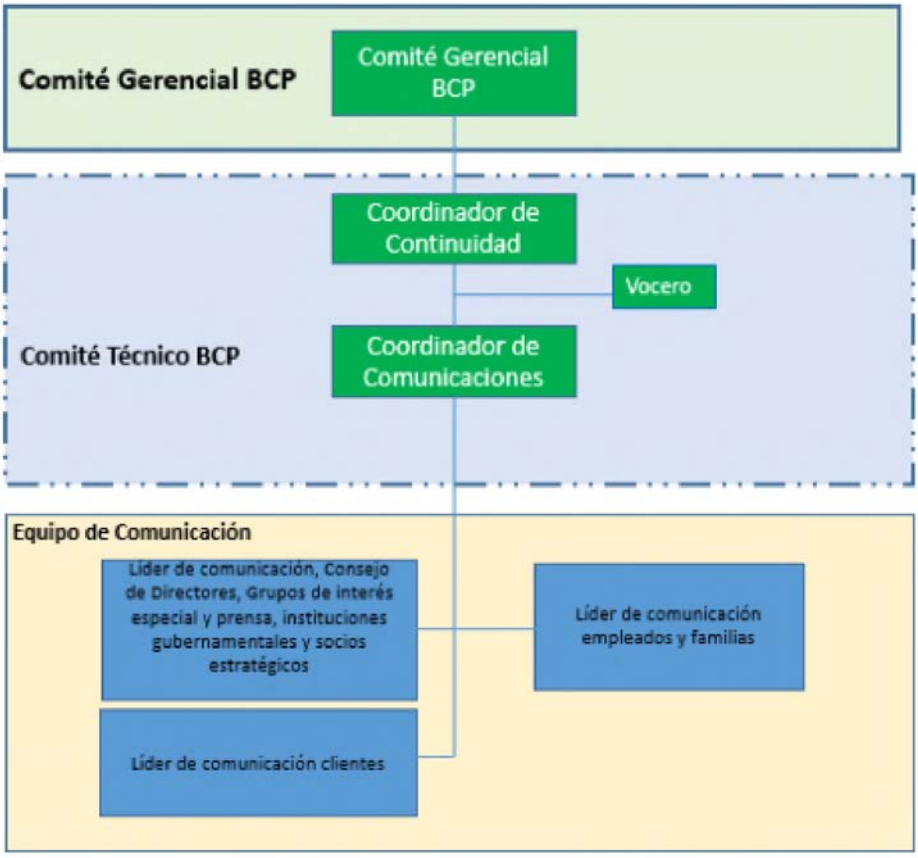
Proporcionar, complementariamente al protocolo de comunicación del Organismos Coordinador, procedimientos documentados para efectuar una comunicación interna o externa sobre los hechos de importancia durante la ocurrencia de un evento que afecte la línea de continuidad. El plan de comunicación abarca al personal interno, proveedores, agentes, público en general y medios de comunicación interna. Durante un evento, la comunicación gerencial juega un papel crucial, ya que es la encargada de salvaguardar la imagen reputacional de la organización.

En el plan de comunicaciones ante incidente se encuentran detallados el gobierno que compone el equipo de comunicación cuando ocurre un evento de interrupción. En el mismo se describen los roles y responsabilidades de cada uno de los integrantes ante un evento. Cada integrante es parte para el desenvolvimiento del plan. Todos los pasos a ejecutar en detalle se pueden visualizar en el documento "Plan de Continuidad del Negocio".

Figura 15,

Gobierno del equipo de comunicaciones ante incidentes

Fuente: Elaboración propia



El protocolo de comunicación de crisis incluye aspectos ya establecidos en este documento, como los roles y perfiles de quienes ejercerán papeles de importancia en el Plan de Comunicaciones ante Incidentes. Partiendo de esto, a continuación, se presenta un listado de las posibles preguntas que pueden surgir en un momento de crisis y sus respectivas respuestas, las cuales sugieren los procedimientos que

constituyen el protocolo.

Tabla 20,

Protocolo de Comunicación en crisis

Fuente: Elaboración propia

No.	Pregunta	Respuesta
1	¿Quién decide que existe un estado de emergencia o incidente?	El Comité gerencial BCP
2	¿Quién lo declara?	El Coordinador de continuidad o el coordinador de continuidad alterno, en caso de que el primero no esté disponible.
3	¿Quién reporta los posibles riesgos que puede enfrentar el OC?	Encargado de Gestión de Riesgos
4	¿Quién decide si la información tiene el grado de relevancia necesario para ser comunicada al público externo?	El Comité Técnico BCP apoyado en el Coordinador de Comunicaciones
5	¿Quién se encarga de generar los comunicados para el público interno y externo?	El Vocero
6	¿Quién se encarga de los aspectos logísticos internos cuando hay contingencia?	Los Encargados de Recuperación de Procesos
7	¿Quién se encarga del Plan de recuperación de negocio y tecnología?	Los Encargados de Recuperación de Procesos y el Encargado de TI, con sus respectivos equipos.

6.5.2. Plan de Administración ante Incidentes

El plan de administración de incidentes ayuda a gestionar el manejo efectivo de los incidentes antes, durante y después de los mismos, para minimizar los impactos ocasionados por un evento de interrupción. Tal como se menciona en el capítulo anterior sobre la gobernabilidad del plan de continuidad, el mismo está conformado por el comité gerencial, el comité técnico y el equipo de recuperación, cada quien con un rol y responsabilidad para la gestión de un evento crítico. (Ver figura 11). Los integrantes, roles y responsabilidades se encuentran detallados en el plan de continuidad. Todos los pasos a ejecutar en detalle se pueden visualizar en el documento "Plan de Continuidad del Negocio".

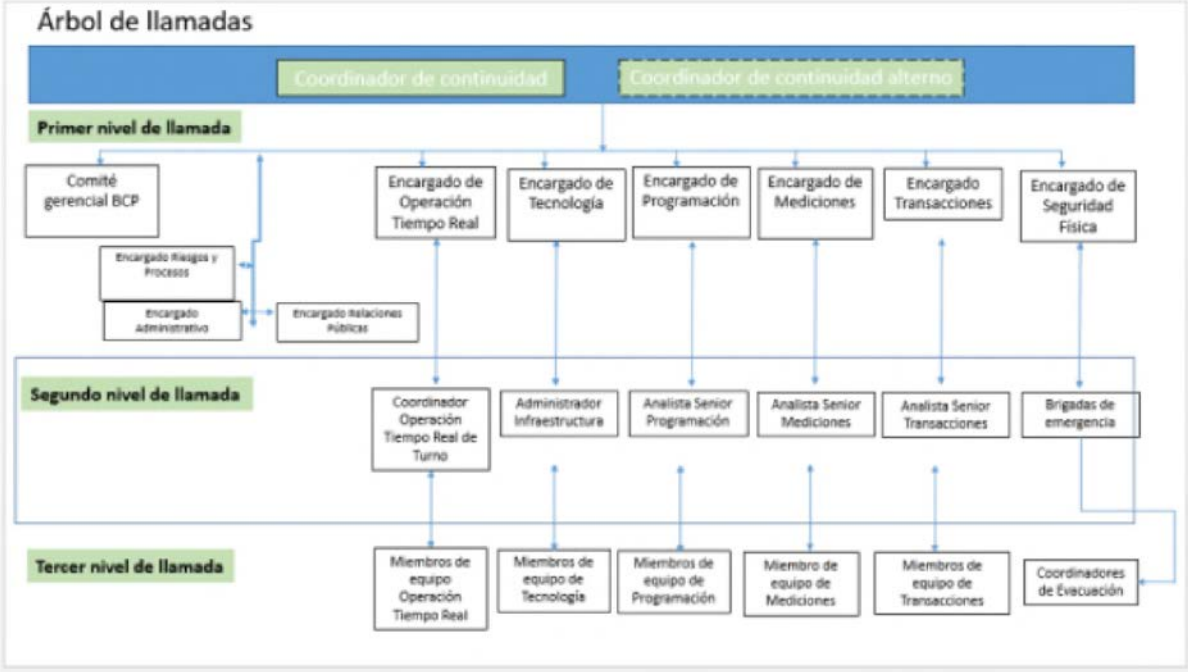
Para la administración de incidentes se cuenta con la herramienta del árbol de llamadas, esta representa la cadena de llamadas que se debe seguir para comunicar a los

integrantes del Plan de continuidad la activación de este. Se ejecuta después de la declaración de contingencia realizada por el Coordinador de continuidad. El árbol de llamadas está dividido en equipos o grupos para facilitar el flujo de información y las comunicaciones entre los diferentes integrantes requeridos, según el tipo de evento que se haya declarado (interrupción, crisis, desastre).

Figura 16,

Árbol de Llamadas

Fuente: Elaboración propia

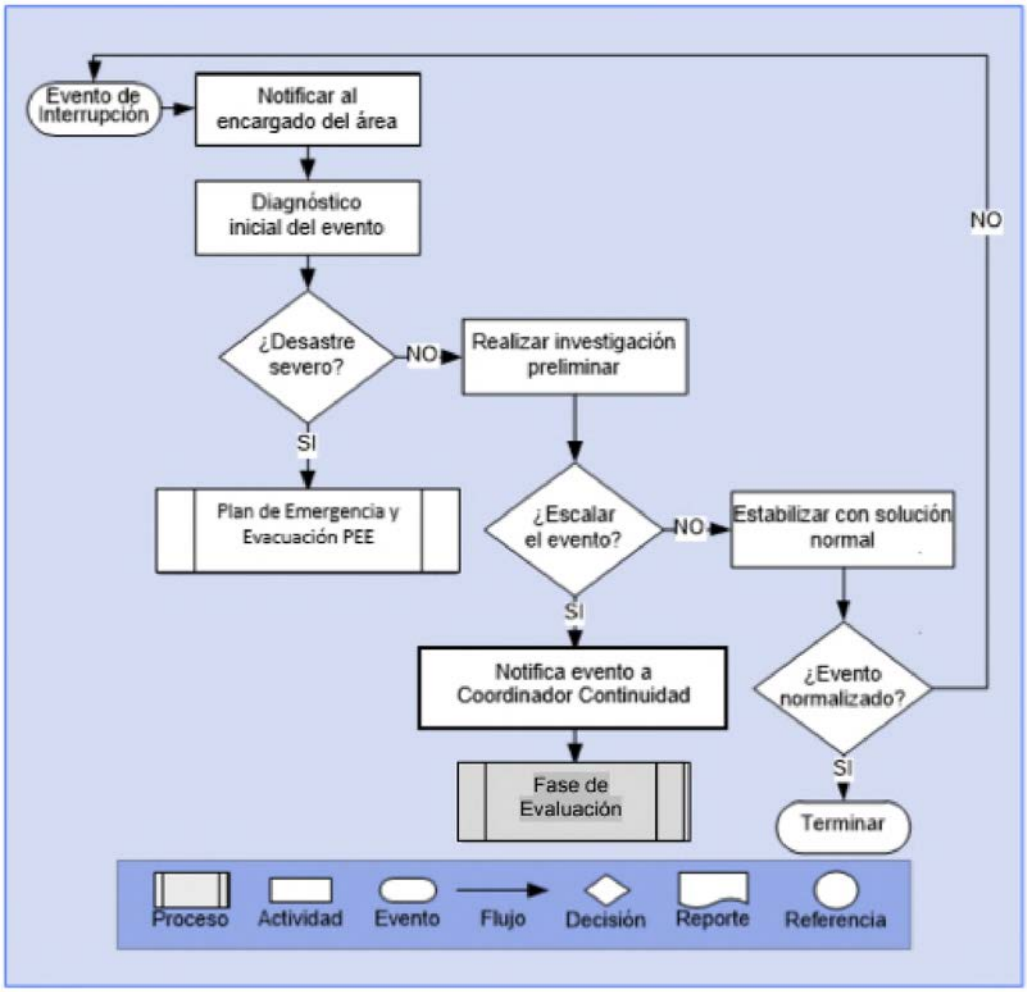


Existen diferentes fases por la que pasa la institución en caso de ocurrir un evento de interrupción o un evento de crisis. El flujo comienza con el evento materializado, luego inicia la fase de evaluación de evento, si se determina que es un evento de crisis el mismo pasa por la fase de activación y finalmente a la fase de retorno a la normalidad. Todos los pasos a ejecutar en detalle se pueden visualizar en el documento "Plan de Continuidad del Negocio".

Figura 17,

Flujograma de actividades

Fuente: Elaboración propia



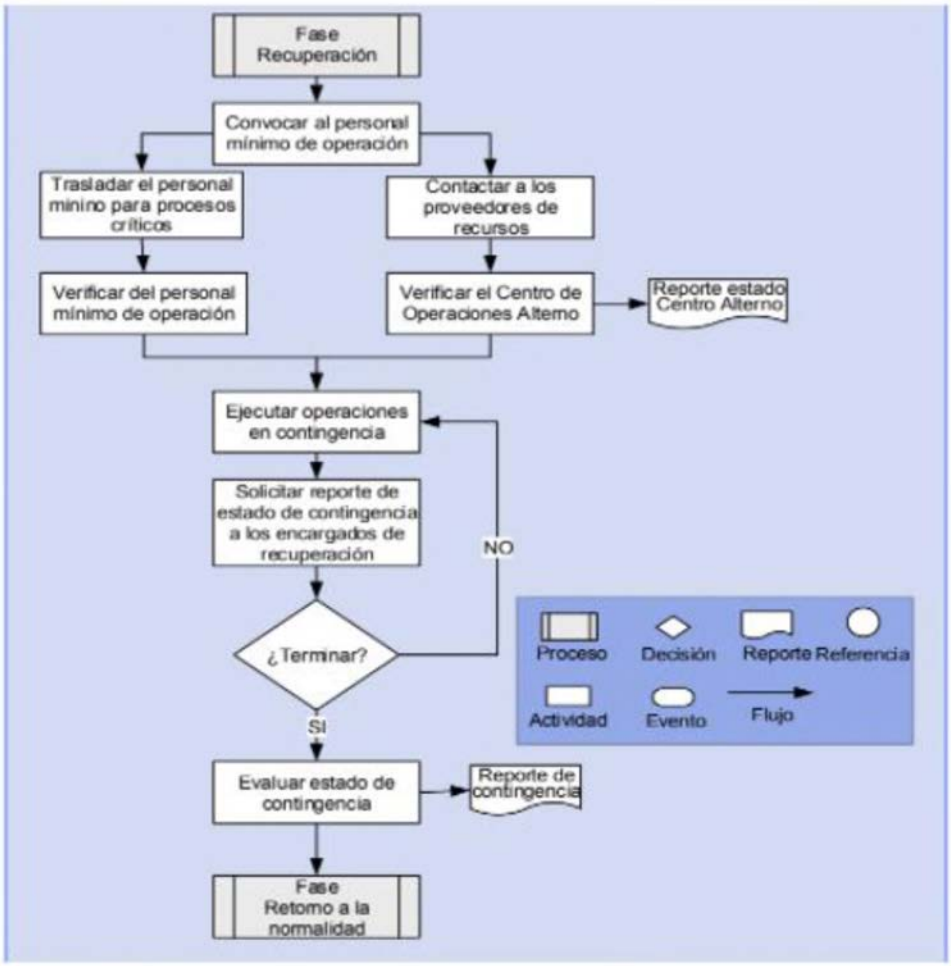
6.5.3. Plan de Recuperación de Negocio

El acápite entra en funcionamiento cuando el evento ha ocurrido y surge una interrupción en el negocio, ya sea porque los espacios físicos se vieron comprometidos o la realización de los procesos se vieron afectados. Este tiene como objetivo restaurar en un centro alterno la operatividad de los procesos de operaciones afectados por el evento. Se describen los procedimientos generales que permiten poner operativa la sede alterna y a su vez los procedimientos a ejecutar desde la sede alterna. Todos los pasos a ejecutar en detalle se pueden visualizar en el documento "Plan de Continuidad del Negocio".

Figura 18,

Flujograma actividades de recuperación

Fuente: Elaboración propia



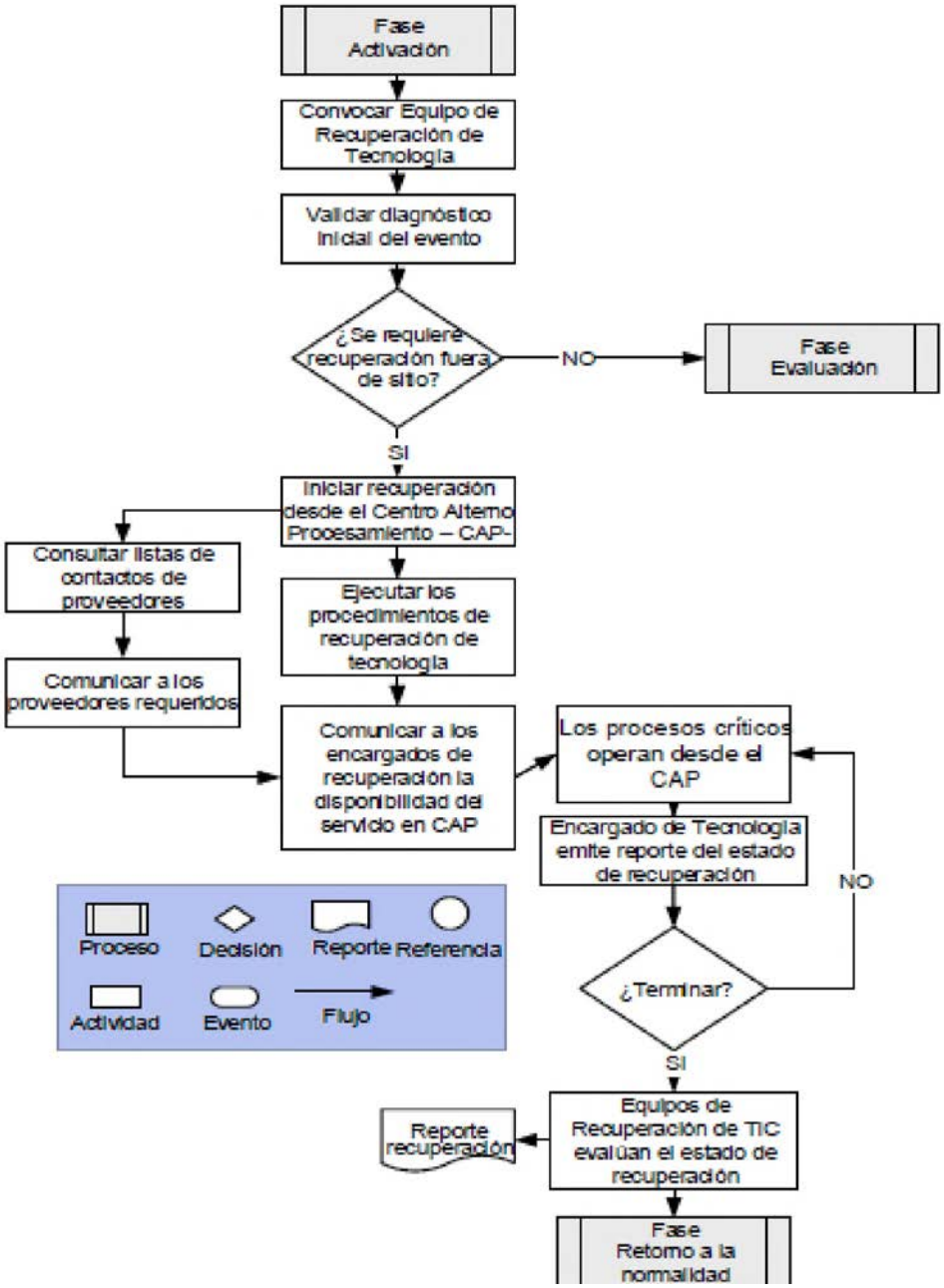
6.5.4. Plan de Recuperación de Tecnología

Al igual que el plan de recuperación de negocio, el plan de recuperación de tecnología describe los procedimientos para recuperar o restaurar la operatividad de la tecnología (hardware, software, aplicaciones de operación, datos y recursos relacionados) en un centro de procesamiento alterno ante a ocurrencia de un evento catastrófico que inhabilite los sistemas desde la sede principal del Organismo Coordinador por tiempos prolongados. Los tiempos de objetivos de recuperación (RTO) para los sistemas tecnológicos fueron determinados en el pasado análisis de impacto del negocio (BIA). Todos los pasos a ejecutar en detalle se pueden visualizar en el documento "Plan de Continuidad del Negocio".

Figura 19,

Flujograma de Recuperación de Tecnología (DRP)

Fuente: Elaboración propia



Capítulo 7: Conclusiones y Recomendaciones

7.1. Conclusiones

De los resultados presentados en los análisis realizados para poder crear el plan de continuidad del negocio del Organismo Coordinador del Sistema Eléctrico, podemos generar las conclusiones con respecto a cada uno de los objetivos específicos planteados al inicio del proyecto. Los objetivos planteados al inicio del proyecto son los siguientes:

Identificar los impactos que puedan generar interrupción sobre los procesos y servicios del Organismo Coordinador del Sistema Eléctrico Nacional.

Identificar los riesgos de continuidad del Organismo Coordinador del Sistema Eléctrico Nacional.

Definir los procesos que debe poseer el plan de continuidad del negocio para mejorar la capacidad de la organización en la prestación del servicio ante una interrupción.

Para identificar los impactos financieros como no financieros de los procesos ejecutados en el Organismo Coordinador del Sistema Eléctrico Nacional, primero se procede a documentar los procesos que se tomaran en cuenta para la evaluación. Con los procesos determinados se realizan las entrevistas con los usuarios dueños de los procesos, identificando cada uno de los componentes necesarios del BIA. El impacto se debe medir de acuerdo a las complicaciones que puede generar un proceso al estar interrumpido por algún evento, estas interrupciones pueden causar impactos financieros, reputacional, operacional, recursos humanos, social, estratégico y regulatorio. Con esto y la medición de los tiempos en la que el proceso puede no estar disponible, se determina el impacto del proyecto.

Se realizó un levantamiento exhaustivo de riesgo de continuidad, al cual se les asigno un impacto de riesgo dependiendo de la probabilidad de ocurrencia y el impacto que podría generar tal riesgo. Los riesgos con impactos altos o muy altos se le dio mayor prioridad a la hora de conformar las estrategias para la mitigación total o disminución de la probabilidad del

mismo. En fin, se tomaron en cuenta los riesgos más relevantes dentro de estas categorías, procesos y persona, tecnología de la información e infraestructura físicas.

En conclusión, aplicando las metodologías y procesos antes mencionados, fue posible crear el plan de continuidad del negocio. Según el levantamiento se tomaron en cuenta los procesos que tienen más impacto en la organización y se plasmaron los procedimientos a seguir para tratar un evento disruptivo en la organización. El plan de continuidad está conformado por cuatro pilares, plan de comunicación, plan de administración ante incidentes, plan de recuperación del negocio y plan de recuperación tecnológico.

7.2. Conclusión General

El resultado investigativo permite evidenciar que la empresa tiene las capacidades físicas y organizacionales para continuar con la generación de sus servicios y/o productos ante posibles eventos disruptivos, considerando que el marco de la norma ISO 22301:2019 debe ser implementado.

Considerando la aplicación de la norma ISO 22301, se reconocen diferentes procesos como críticos en la organización, la mayoría de los cuales se encuentran representados en la capacitación y disminución de riesgos de los empleados, quienes son las personas clave para darle continuidad al sistema de gestión. La implementación debido a ello debería realizarse con base en las posiciones que las personas tienen.

El establecimiento de planes de continuidad permite al OC enfrentar situaciones previsibles e impredecibles, ayudando a reducir los riesgos antes, durante y después de los incidentes y contar con procedimientos que se detallan y trabajan de manera continúa recuperando la operatividad de los procesos críticos de la organización en un tiempo apropiado, que no genere pérdidas significativas para la empresa, y sobre todo problemas en cuanto a su imagen. También crea un orden lógico en que operaciones y/o sistemas deben ser recuperados primero de acuerdo a la criticidad e impacto de los mismo.

Es necesario que se realicen auditorias enfocadas en la continuidad para identificar en un futuro una mayor cantidad de debilidades y oportunidades de mejora, considerando el nivel continuo de cumplimiento de la organización. Como parte del análisis BIA se identificaron las actividades que se deben tener en cuenta para generar soporte a la ejecución de procesos críticos que permiten la identificación de proveedores claves, procesos soporte, personal clave, sistemas de información, equipos, registros y recursos para el proceso.

Por último, el Organismo Coordinador del Sistema Eléctrico ahora mismo cuenta con los conocimientos y herramientas necesarias para continuar la actualización del plan de continuidad del negocio periódicamente, cada uno de los interesados estuvieron involucrados profundamente con el proceso entendiendo que se debe hacer en un futuro. Esto es un valor agregado al proyecto entregado y de mucha utilidad para el futuro del OC.

7.3. Recomendaciones

Se recomienda identificar y conocer los impactos financieros como no financieros de los procesos ejecutados en el Organismo Coordinador del Sistema Eléctrico Nacional, para saber el impacto y tiempo que pueda generar un proceso al estar interrumpido por algún evento.

Se recomienda mitigar los riesgos con impactos altos o muy altos en las categorías de procesos y persona, tecnología de la información e infraestructura físicas, para velar por la continuidad de negocio.

Se recomienda tener actualizado los pilares del plan de continuidad del negocio (plan de comunicación, plan de administración ante incidentes, plan de recuperación del negocio y plan de recuperación tecnológico), para tener una efectiva respuesta ante cualquier incidente.

Se recomienda generar un modelo de implementación que pueda aplicarse en otras empresas que se manejen bajo el mismo tipo de organización, es necesario indicar que el sistema puede ser aplicable siempre y cuando se deba analizar de manera consistente la ISO 22301. El proceso debe ser implementado dentro de la organización por personas que tienen conocimientos sobre el tema, con la intención de garantizar un proceso adecuado.

Se recomienda analizar el entorno externo constantemente, identificando riesgos que puedan conllevar a la paralización de las operaciones de la organización. Es necesario que el personal participe de manera consistente en el proceso de continuidad reconociendo que son estos los que generaran la mayoría de las actividades, respondiendo de manera óptima a procesos diarios que tiene implicaciones complejas, así mismo son estos los encargados de no poner en riesgo las actividades de reanudación y recuperación.

Se recomienda involucrar al consejo de coordinación como parte de la continuidad del negocio, considerando que no solo debe enviarse informes de conocimiento, sino una participación en donde se incluya la generación de espacios de participación.

Se recomienda en la gestión del conocimiento, contar con estrategias para la retención de los colaboradores claves ante ofertas exteriores, creando incentivos y motivaciones laborales. En la seguridad laboral, habilitar un proceso de gestión de emergencia para responder ante evento no esperado y daños sobre personas y bienes, capacitar al personal o crear una brigada de emergencia para que brinde soporte cuando exista cualquier tipo de emergencia. Por último, en la gestión de proceso crear un plan alterno de trabajo para los procesos críticos de la organización, con el fin de contener los procedimientos de recuperación y/o contingencia, para no afectar la continuidad de los procesos ante eventos naturales, físico, tecnológico o humano.

Parte 5. Referencias Bibliográficas

Alarcón, C., & Herrera, C. A. (2020). *Aplicación de la norma NTC 5722 en la consolidación del plan de continuidad del negocio para una entidad bancaria.*

Ángel, J. E., & Velasco, H. (2014). *Diseño y propuesta de implementación de un plan de continuidad del negocio aplicable a los hospitales en la ciudad de Bogotá .* (Bachelor's thesis).

Bazan, E. (2020). Primera Sesion - ISO 22301.

Business Continuity. (2012). *Antecedentes históricos de la Continuidad del Negocio.* Business Continuity.

Chiavenato, I. (2001). *Administración. Proceso Administrativo. .* Editorial McGraw-Hill, 3.

Collado, & et al, .. (2014). *Metodología de la Investigación. Editorial McGraw Hill.*

Cordero, J. C., & Nuñez, R. R. (2020). *Diseño de sistema de gestión de calidad según ISO 21001: 2018 para mejora continua en programa de ingeniería industrial.*

Fernández, S.; Díaz, S. (2002). *Investigación cuantitativa y cualitativa.* (p 76-78). Cad Aten Primaria, 9.

Granda, E. L., Espinosa, J. N., & Vásquez, C. C. (2017). *Modelo de evaluación de gestión de continuidad del negocio basado en la norma ISO 22301: 2012. .* Espacios, 38(1), 17.

Grajales, T. (2000). *Tipos de investigación.*

González, J. A. (2015). *Elaboración de un plan de auditoría para evaluación de cumplimiento en sistemas para gestión de la continuidad del negocio basado en la normativa ISO 22301.*

Hernandez, R. (2014). *Metologia de la Investigacion.* Mexico.

Hernández-Sampieri, R., & Torres, C. P. (2018). *Metodología de la investigación (Vol. 4). .* México^ eD. F DF: McGraw-Hill Interamericana.

INTECO. (2021). *ISO 22301: 2020.* Retrieved from https://www.inteco.org/shop/inte-iso-22301-2020-seguridad-y-resiliencia-sistemas-de-gestion-de-continuidad-del-negocio-requisitos-6030

ISO 22301. (2012). *Continuidad del Negocio.*

Maestro, E. (2004). *La gestión de la calidad en las organizaciones de educación superior. Aportación del enfoque de la Organización Internacional de Normalización (ISO). .* Revista complutense de educación, 15(2), 647-686.

Martins, P. (2010). *Metodología de la investigación cualitativa.*

Mendoza, C., & et al, .. (2019). *Metodología de la investigación holística.*

Minolli, C. B. (2005). *Empresas resilientes algunas ideas para construirlas.* (p 20-25) Temas de Management, 3(1).

NIST, S. 800–34 Rev. 1. . (2010). *Contingency Planning Guide for Federal Information Systems. Gaithersburg, MD.* United States: National Institute of Standards & Technology, 150.

Organismo Coordinador del Sistema Eléctrico. (2021). *Reseña histórica del Organismo Coordinador.* Organismo Coordinador.

Sotres, P. (2012). *ISO 22301: Continuidad dle negocio.* Interempresas.

Pedreros Méndez, R. F. (2018). *Diseño de un modelo conceptual para la gestión de la continuidad de negocios y respuesta ante crisis orientada a medianas y grandes empresas en Chile.*

Pita Fernández, S., & Pértegas Díaz, S. (2002). *Investigación cuantitativa y cualitativa. Cad Aten Primaria, 9, 76-78.*

Project Management Institute. (2017). A guide to the project management body of knowledge (PMBOK guide). (6a ed.). Newtown Square, Pa: Project Management Institute

Riera, & et al. (2018). *Norma ISO 19011.* Observatorio de la Economía Latinoamericana.

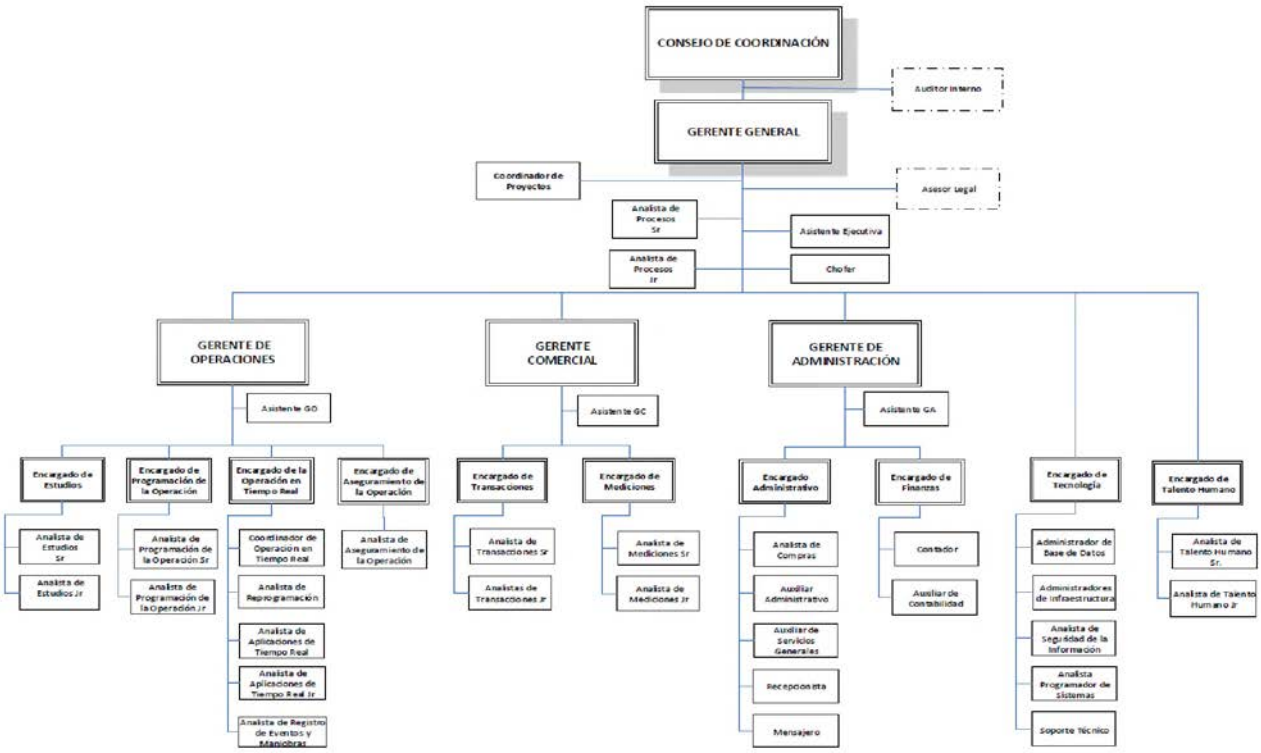
Sarabia Zapata, A. V. (2015). *Modelo de gestión de continuidad de infraestructura tecnológica para la operación de servicios de TI en empresas financieras sobre la base de las normas ISO 22301 e ISO 27001.* Aplicación a un caso de estudio (Master's thesis, Quito, Universidad de las Américas).

Velásquez, C. (2011). *La Investigación Holistica: Alternativa integradora en Ciencias Sociales. SABER.* Revista Multidisciplinaria del Consejo de Investigación de la Universidad de Oriente, 23(2), 170-173.

Zawada, B. (2014). *The practical application of ISO 22301.* . Journal of business continuity & emergency planning, 8(1), 83-90.

Parte 6. Anexos

Anexo No.1. Organigrama



Anexo No.2. Cumplimiento de la ISO 22301:2019

Norma ISO 22301	
4. Contexto de la información	
4.1. Entendimiento de la organización y su contexto	1
4.2. Entendimiento de las necesidades y expectativas	1
4.3. Determinación del campo de aplicación del sistema de gestión de la continuidad del negocio	2
4.4. Sistema de gestión de la continuidad del negocio	2
5. Liderazgo	
5.1. Liderazgo y compromiso	2
5.2. Compromiso de la dirección	2
5.3. Política	2

5.4. Funciones, responsabilidades y autoridad en la organización	2
6. Planificación	
6.1. Acciones para cubrir los riesgos y oportunidades	2
6.2. Objetivos de la continuidad del negocio y planes para conseguirlos	1
7. Apoyo	
7.1. Recursos	2
7.2. Competencia	1
7.3. Concientización	2
7.4. Comunicación	1
7.5. Información documentada	2
8. Operación	
8.1. Planificación y control operacional	2
8.2. Análisis de impacto en el negocio y apreciación del riesgo	1
8.3. Estrategia de continuidad del negocio	1
8.4. Establecimiento e implantación de procedimientos de continuidad del negocio	1
8.5. Pruebas y ensayos	1
9. Evaluación y medición del rendimiento	
9.1. Supervisión, medición, análisis y evaluación	2
9.2. Auditoria interna	2
9.3. Revisión de la dirección	2
10. Mejora	
10.1. No conformidad y acción correctora	1
10.2. Mejora continua	1

Anexo No. 3 Procesos críticos

1 Gerencia Operaciones
1.1 Coordinación y supervisión de la operación en tiempo real
1.1.1 Supervisión y coordinación en tiempo real y verificación del cumplimiento de los programas
1.2 Programación de la operación

1.2.1 Programación diaria
1.2.2 Verificación de costos variables
1.2.3 Programación semanal
2 Gerencia Comercial
2.1 Mediciones
2.1.1 Revisión de la entrega de medidas
2.1.2 Habilitación de SMC (Sistema de Medición Comercial)
2.2 Transacciones
2.2.1 Cálculos de transacciones económicas
2.2.2 Cálculos de costos marginales

Anexo No. 4 Procesos no críticos

1 Gerencia Operaciones
1.1 Supervisión de la operación en tiempo real
1.1.1 Monitoreo de variables del sistema eléctrico nacional interconectado (SENI)
1.1.2 Registros de eventos
1.1.3 Reprogramación de la operación
1.2 Programación de la operación
1.2.1 Verificación de restricciones operativas de centrales térmicas (VEROPE)
2 Gerencia Comercial
2.1 Mediciones
2.1.1 Contraste de los medidores de energía
2.1.2 Elaboración de informe de administración SMC
2.1.3 Visitas rutinarias a los agentes
2.2 Transacciones
2.2.1 Gestión de formularios de administración de contratos
2.2.2 Indisponibilidad en horas de punta
2.2.3 Realización de reliquidación de transacciones económicas de meses anteriores

2.2.4 Realización de reliquidación anual de transacciones económicas de potencia y derecho de conexión
3 Gerencia de Administración
3.1 Gestión administrativa
3.1.1 Gestión de Compras
3.1.2 Mantenimiento infraestructura
3.1.3 Gestión comunicaciones
3.2 Talento humano
3.2.1 Análisis valuación de puestos
3.2.2 Provisión de capital humano
3.2.3 Gestión del sistema de evaluación del desempeño
3.2.4 Desarrollo del talento humano
3.2.5 Administración del sistema de compensación de beneficios
3.3 Finanza
3.3.1 Gestión de nóminas de pagos
3.3.2 Gestión de desembolsos
3.3.3 Elaboración de estados financieros
3.3.4 Gestión de obligaciones tributarias y fiscales
3.3.5 Gestión de aportes
3.3.6 Gestión presupuestaria

Anexo No. 5 Criterio impactos no financieros

Tipo de impacto	Nivel de impacto	Criterio
Operativo	Catastrófico	Perdida de información crítica de la organización que no se puede recuperar
		Interrupción de las operaciones de la organización por más de tres días.
	Crítico	Perdida de información crítica de la organización o de terceros de difícil recuperación
		Genera reprocesos y retrasos que impacta a nivel de toda entidad
		Interrupción de las operaciones de la organización por entre 1 y 2 días

	Grave	Perdida de información crítica de la organización o de terceros que sea recuperable pero que ocasione retrasos en más de un área de la entidad
		Genera reprocesos y retrasos de más de un área de la entidad
		Interrupción de las operaciones de la organización entre 8 y 23 horas.
	Moderado	Perdida de información crítica de la organización o de terceros que sea recuperable pero que ocasione retrasos en un área de entidad
		Genera reprocesos y retrasos en un área de una entidad
		Interrupción de las operaciones de la organización por entre 4 y 7 horas
	Leve	Perdida de información crítica de la organización o de terceros que sea recuperable pero que no ocasione retrasos en las diferentes áreas de la entidad
		Genera reprocesos y retrasos puntuales en la entidad
		Interrupción de las operaciones de la organización menores a 4 horas
Reputacional	Catastrófico	Impacto que afecte la imagen de las organizaciones en el sistema eléctrico nacional
	Crítico	Impacto que afecte la imagen de la organización en el mercado eléctrico
	Grave	Impacto que afecte la imagen de la organización entre los agentes del sector eléctrico
	Moderado	Impacto que afecte la imagen de la organización en el mercado eléctrico a nivel local por no brindar los servicios acordados en la Ley General de electricidad 125-01 por dos días
	Leve	No hay impacto que afecte la imagen de la organización
Social	Catastrófico	Impacto que genera reclamos ante la organización por situaciones que pueden afectar el bienestar de las personas a nivel nacional por no brindar los servicios de calidad y menor costo según lo establecido en la Ley general de Electricidad 125-01
	Crítico	Impacto que genera reclamos ante la organización por situaciones que pueden afectar el bienestar de las personas a nivel nacional
	Grave	Impacto que genera reclamos ante la organización que puedan afectar uno o más grupos sociales
	Moderado	Impacto que genere reclamos ante la organización por situaciones que pueden afectar un grupo social
	Leve	Impacto imperceptible para la sociedad
Recursos Humanos	Catastrófico	25% o más del personal considerando algunos de los siguientes aspectos: perdida empleo, insatisfacción con el clima laboral, reducción de beneficios, paros y huelgas, descontento

	Crítico	15% o más del personal considerando alguno de los siguientes aspectos: pérdida de empleo, insatisfacción con el clima laboral, reducción de beneficios, paros y huelgas, descontento
	Grave	10% o más del personal considerando alguno de los siguientes aspectos: pérdida de empleo, insatisfacción con el clima laboral, reducción de beneficios, paros y huelgas, descontento
	Moderado	5% o más del personal considerando alguno de los siguientes aspectos: pérdida de empleo, insatisfacción con el clima laboral, reducción de beneficios, paros y huelgas, descontento
	Leve	No se identifica cambios que afecten el personal
Estratégico	Catastrófico	Perdida interoperabilidad con ETED
	Crítico	Pérdida de clientes importantes de la organización
	Grave	Pérdida significativa de clientes de la organización
	Moderado	Perdida no significativa de clientes de la organización
	Leve	No hay pérdida de clientes de la organización
Regulatorio	Catastrófico	Intervención de la organización por parte de la Superintendencia de la Electricidad por incumplimientos de la ley general de electricidad 125-01
	Crítico	Constantes llamados de atención por incumplimiento de los servicios ofrecidos
	Grave	Quejas y posibles demandas por parte de los agentes debido a incumplimientos con servicios establecidos
	Moderado	Solicitud de aclaraciones por parte de los agentes por incumplimientos de servicios
		Solicitud de investigación por parte del regulador
	Leve	No tiene efectos de cara al regulador
		Solicitud de aclaraciones por parte de agentes reguladores

Anexo No. 6 Recursos mínimos necesarios

1.1. Coordinación y superación de la operación en tiempo real		
Tecnología	**Sistema**	**Criticidad**
	SCADA	Indispensable
	REGIO	Indispensable
	MODOM	Importante
	DIGSILENT	Indispensable
	Paquete office	Indispensable
	PDF Reader	Indispensable
	Internet	Indispensable
Tecnología (otros)	**Aplicativo**	**Criticidad**

	Radio de frecuencia	Indispensable
Recursos mínimos	**Descripción**	**Cantidad**
	PC con conexión	5
	Puesto de trabajo básico	5
	Teléfono fijo	1
	Teléfono celular	1
1.2 Programación de la operación		
Tecnología	**Sistema**	**Criticidad**
	SCADA	Indispensable
	REGIO	Indispensable
	MODOM	Indispensable
	DIGSILENT	Indispensable
	Paquete office	Indispensable
	PDF Reader	Indispensable
	Internet	Indispensable
	Sistema de verificación de costos variables	Indispensable
Tecnología (otros)	**Aplicativo**	**Criticidad**
	N/A	N/A
Recursos mínimos	**Descripción**	**Cantidad**
	PC con conexión	2
	Puesto de trabajo básico	2
	Teléfono fijo	1
	Teléfono celular	1
2.1. Mediciones		
Tecnología	**Sistema**	**Criticidad**
	Prime read	Importante
	Paquete office	Indispensable
	Correo (Outlook)	Indispensable
	PDF Reader	Indispensable
	Internet	Indispensable
Tecnología (otros)	**Aplicativo**	**Criticidad**
	N/A	N/A
Recursos mínimos	**Aplicativo**	**Criticidad**
	N/A	N/A
2.1. Transacciones		
Tecnología	**Sistema**	**Criticidad**
	PSS/E	Indispensable
	PTF	Indispensable
	Paquete office	Indispensable
	Correo (Outlook)	Indispensable
	PDF Reader	Indispensable
	Internet	Indispensable
Tecnología (otros)	**Aplicativo**	**Criticidad**
	N/A	N/A
Recursos mínimos	**Aplicativo**	**Criticidad**
	N/A	N/A

Anexo No.7 Clasificación de Probabilidad

Probabilidad de Ocurrencia	
5. Casi Seguro	Es casi seguro que ocurran bajo muchas circunstancias. El evento es rutinario y puede presentarse frecuentemente en la operación del día a día. Se detectaron situaciones que permiten comprobar que este evento ha ocurrido durante los últimos seis meses. Se presenta en el día a día, su origen es atribuible a situaciones normales del proceso como interrupciones menores de los servicios de la tecnología, los recursos de papelería y otros similares.
4. Muy Probable	Se presenta con cierta regularidad y su causa es atribuible a los recursos mínimos del proceso, los cuales son necesarios para su operación. El evento es rutinario e inherente a causas específicas, puede presentarse en cualquier momento. Este evento podría suceder en períodos cortos de tiempo (minutos, horas, días). Se detectaron situaciones que permiten estimar que este evento ha ocurrido al menos una vez entre seis meses y un año.
3. Posible	Se detectaron situaciones que permiten estimar que este evento puede suceder al menos una vez entre uno y dos años. Se presenta por situaciones atribuibles al descuido o error humano. El evento no se clasifica como rutinario y su ocurrencia es condicionada bajo circunstancias que requieren supervisión controlada.
2. Poco Probable	Se detectaron situaciones que permiten estimar que este evento puede suceder al menos una vez entre dos y tres años. Se presenta por situaciones atribuibles a las personas y puede ser causada por hechos internos del país como paros, huelgas, o amenazas de terrorismo, asonadas. El evento se clasifica como no rutinario y no es inherente a la tecnología, su frecuencia se asocia con variables externas a la tecnología, los procesos o componentes.
1. Raro	No se detectaron amenazas o vulnerabilidades que aumenten su probabilidad de ocurrencia. No se ha presentado en menos de tres años. En condiciones excepcionales se podría presentar un evento entre 10 a 20 años. Se presenta bajo circunstancias extremas de orden público en el país, de catástrofe o bajo situaciones excepcionales fuera del alcance de la organización. El evento es no-rutinario. Se presenta solo bajo situaciones excepcionales o fuera de la operación normal.

Anexo No.8 Clasificación de Impacto

Impacto	
5. Catastrófico	Interrupción total del proceso. Amonestaciones por incumplimiento. Hay pérdida de imagen de la entidad. Posibles pérdidas de vidas humanas (empleados), por problemas ambientales y de seguridad. Pérdidas económicas mayores al 5% del ingreso neto. Destrucción total de instalaciones físicas.
4. Alto	Hay pérdida de imagen con publicidad adversa. No se pueden ejecutar actividades críticas del proceso. Imposibilidad de acceso a instalaciones físicas. Se presenta incumplimiento de ley y regulaciones. Pérdidas económicas entre 3% y 5% del ingreso neto. Interrumpe totalmente el servicio al cliente.
3. Moderado	Interrumpe parcialmente algún servicio crítico. Se afecta el proceso, pero se pueden ejecutar las actividades críticas. Pérdidas económicas entre 2% y 3% del ingreso neto. Acceso restringido a las instalaciones físicas (60%). Se presenta publicidad negativa (imagen) de la Entidad. Se presentan casos aislados de seguridad o salud para los empleados.
2. Bajo	Acceso restringido a las instalaciones físicas (80%). Puede verse afectada la imagen de la entidad ante el gobierno. Pérdidas económicas entre 0% y 2% del ingreso neto. Retraso actividades no críticas. El evento debe ser asistido bajo supervisión técnica continua. Afecta negativamente la satisfacción de los usuarios y los agentes del mercado eléctrico.
1. Insignificante	No afecta la operación del proceso. No existen impactos legales o regulatorios. No afecta la imagen en el mercado. No se presentan pérdidas económicas. No afecta las instalaciones físicas. No afecta a los clientes. El evento se resuelve por mesa de ayuda sin contra tiempos. No se presentan problemas de seguridad y salud para los empleados.

Anexo No.9 Clasificación de control

Clasificación del Control	
1. Fuertes	El control o procedimiento de control observado es preventivo, está documentado e implementado, es efectivo para mitigar los riesgos y siempre es aplicado con la intensidad y rigurosidad esperada.
2. Normal	El control y procedimiento de control observado es preventivo, está documentado e implementado, es apropiado para mitigar los riesgos, pero el personal no siempre lo cumple o aplica.
3. Moderado	El control y procedimiento de control observado es correctivo, está documentado, pero solo algunas veces es aplicado por múltiples motivos, cuando es implementado ayudan a reducir la exposición al riesgo, puede requerir rediseño.
4. Débil	El control existente es informal, casi siempre es correctivo, ayuda a mitigar los riesgos, pero no siempre es aplicado. Se debe realizar una documentación e implementación.
5. Inexistente	No se observó o evidenció procedimientos de control o controles que ayuden a reducir o mitigar el riesgo. Se debe definir, documentar, e implementar controles.

Anexo No. 10 Tipos de control

Tipo de Control	
No hay control	No se han establecido controles para el riesgo asociado.
Correctivo	El control o controles establecidos se utilizan para minimizar el impacto generado en caso de que el riesgo ocurra. Por ejemplo: Rociadores de agua para controlar el fuego, centros alternos de cómputos.

Preventivo	El control o controles que se han establecido buscan evitar la ocurrencia del riesgo y en caso de ocurrencia, ocasione el menor nivel de impacto mitigando o trasladando el riesgo. Por ejemplo: antivirus, políticas de ingreso a la entidad, indicadores de gestión.

Anexo No.11 Riesgos en procesos y personas

Dominio	Riesgo
Gestión del Conocimiento	1. Imposibilidad de efectuar labores operativas diarias por falta de capacidades técnicas del personal 2. Imposibilidad de entrenamientos cruzados por posible dependencia de empleados 3. Deficiencia en la contratación del personal 4. Deficiencia en la gestión operativa por falta de personal crítico
Seguridad Laboral	5 Imposibilidad de responder ante situaciones de emergencia por falta de un proceso de gestión de emergencias 6 Dificultad para responder oportunamente a situaciones de emergencias por falta de capacitación en manejo y control de situaciones críticas 7 Imposibilidad de evacuar efectivamente al personal por no contar con un plan de evacuación ante emergencias 8 Falta de capacidades técnicas del personal en manejo de emergencias 9 Pandemias y/o epidemias en empleados por no efectuar jornadas de vacunación 10 Pandemias y/o epidemias en empleados de manera generalizada 11 Deficiencia en la atención primaria ante accidentes debido a no efectuar acuerdos con instituciones de salud hospitalaria para atender emergencias 12 Deficiencias visuales de los empleados 13 Deficiencias auditivas de los empleados
Gestión de Proceso	14 Deficiencia en la realización y corrida de los procesos en caso de contingencia por no contar con documentación formal de los mismos 15 Insuficiencia en la puesta en marcha de planes de contingencia por no

	contar con certificación de procesos críticos 16 Definición errónea de procesos por no establecer indicadores de gestión 17 Culminación de servicios internos en tiempos errados debido a no establecer acuerdos de niveles de servicio. 18 Deficiencia en la gestión de procesos durante contingencia por no contar con planes alternos de trabajo para los procesos críticos 19 Falla en la gestión de procesos y aplicaciones tecnológicas ante emergencias por no probar los planes alternos 20 Procesos críticos no identificados debido a no realizar análisis de vulnerabilidades
	21 Falla en la provisión del servicio por insuficiencia de proveedores 22 Pérdida del servicio por no contemplar mecanismos de contingencia ante eventualidades con los proveedores 23 Afectación de las operaciones durante una contingencia real debido a que los mecanismos de contingencia establecidos con los proveedores no son probados de forma periódica. 24 Falla en la recuperación de aplicaciones y/o pérdida de información ante interrupciones de mantenimientos no programadas ni notificadas 25 Fallas en los procesos diarios debido a la no disponibilidad de aplicativos

Anexo No.12 Tipificación Riesgos de Instalaciones Físicas

Dominio	**Riesgo**
Preparación ante emergencias	1 Pérdida de activos intelectuales ante el surgimiento de una emergencia / evacuación del personal por falta de un plan de manejo de emergencias 2 Integridad física del personal afectada por falta de una brigada para de manejo de emergencias. 3 Afectación del personal por falta de señalización de rutas de evacuación ante una emergencia.

	4 Integridad del personal expuesta ante una evacuación de emergencia debido a la falta de identificación de las salidas de emergencia 5 Imposibilidad de detección temprana de incendios por falta de alarmas que alerte al personal
	6 Afectación de la integridad física del personal y de activos, por falta de sistemas automáticos de sofocación o extinción de incendios. 7 Afectación de la seguridad del personal debido a la desorientación visual del personal o de organismos de rescate durante una situación de emergencia o evacuación por la ausencia de energía eléctrica. 8 Afectación de la seguridad física del personal debido a que los organismos de rescate no cuentan con planos básicos de la ubicación e infraestructura del OC que permitan una acción oportuna. 9 Pérdida de activos por falta de entrenamiento en uso de extintores ante situaciones de fuego controlable. 10 Pérdida financiera ante demandas por afectación de emergencias a clientes/proveedores
Incendio	11 Propagación de incendio por no contar con paredes internas que permitan cortar el fuego. 12 Propagación de incendio por elementos tecnológicos generadores de calor debido a no contar con extintores de fuego que puedan sofocar un foco de incendio generalizado 13 Propagación de incendios externos hacia el interior de la edificación del OC debido a que no se realizan análisis o investigaciones en la zona aledaña a fin de identificar posibles generadores de incendios. 14 Pérdida de la edificación por no contar con una infraestructura reforzada que proteja de un incendio exterior.

Potencia eléctrica	15 Perdida de potencia eléctrica por exceso de calor en acometidas internas 16 Pérdida de potencia eléctrica por manipulación indebida de las acometidas 17 Falta de energía ante ausencia de electricidad alterna. 18 Falla de la planta eléctrica al momento de una contingencia por no efectuar mantenimientos periódicos 19 Falla de la planta eléctrica y la UPS al momento de una contingencia por no efectuar pruebas de funcionalidad programadas 20 Falla de la UPS por generación de calor en el cuarto donde se encuentra ubicada
Aire acondicionado	21 Sobrecalentamiento del equipamiento tecnológico SCADA y de los equipos del centro de datos por no contar con aire acondicionado de respaldo en caso de fallar el aire principal. 22 Mal funcionamiento de los equipos de aire acondicionado por falta de control de temperatura y humedad 23 Mal funcionamiento de los aires acondicionados por no efectuar mantenimiento preventivo 24 Daños intencionales al equipamiento de aire acondicionado por no contar con acceso restringido a los mismos.
Centro de cómputo	25 Daños o pérdida de los equipos tecnológicos por contar con un piso falso a prueba de fuego 26 Daños o pérdida de los equipos tecnológicos por no contar con paredes y cielo falso a prueba de fuego 27 Daños o pérdida de los equipos tecnológicos por existencia de combustibles. 28 Daños de los equipos tecnológicos por no contar sensores de agua. 29 Daños al equipamiento tecnológico por aumento de temperatura debido a la falta de espacio entre unidades. 30 Daños del equipamiento tecnológico por no contar con muros

	externos reforzados que eviten propagación de incendios. 31 Daños o hurto de equipamiento tecnológico e información confidencial por no contar con mecanismos electrónicos de control de acceso. 32 Imposibilidad de identificar situaciones irregulares por no contar con una bitácora de accesos que permita registrar las acciones efectuadas en el área donde se encuentra el equipamiento SCADA dentro sala de operaciones en tiempo real así como dentro del Centro de Datos.
Seguridad y accesos	33 Pérdida de activos e información confidencial debido a no contar con ronderos internos que puedan detectar personal no autorizado en las instalaciones fuera de horario laboral. 34 Actividades delictivas no detectadas oportunamente debido a no contar con cámaras de seguridad. 35 Pérdida de activos e información por no contar con monitoreo activo de las cámaras de vigilancia 36 Afectación de la seguridad de personal crítico por accesos a las instalaciones con artículos metálicos no autorizados debido a no contar con mecanismo de detección de metales. 37 Activos e información expuesta debido al acceso de personal no autorizado durante la jornada laboral en áreas restringidas 38 Fallas en los controles de accesos e imposibilidad de identificar personal no autorizado en áreas restringidas por no portar identificación en un lugar visible 39 Pérdida de activos y de información debido a que no se realice una inspección de los elementos que portan los visitantes tanto al ingreso como al momento de retirarse de las instalaciones
Seguridad y accesos	40 Plagio de información debido al uso no autorizado de cámaras o radios en áreas restringidas. 41 Afectación y daños a la estructura debido a no contar con protección contra impactos en las zonas de parqueos 42 Afectación reputacional debido a no efectuar estudios de antecedentes antes de realizar relaciones comerciales con

	proveedores de poca confianza 43 Exposición de información confidencial debido a no contar con un procedimiento para la destrucción de información.

Anexo No.13 Matriz de Interesados

Matriz de Interesados						
No.	**Función**	**Empresa**	**Nombre**	**Localización**	**Rol**	**Nivel de Influencia/Interés**
1	Patrocinador	Organismo Coordinador	Manuel López San Pablo	Santo Domingo	Inversionista	**Tipo de Interés:** Alto **Influencia:** Alto **Áreas en la que influye:** I,P,E, S, C
2	Gerencia del Proyecto	Tesis	Fernando Beras	Santo Domingo	Seguimiento y Control	**Tipo de Interés:** Alto **Influencia:** Alto **Áreas en la que influye:** I,P,E, S, C
3	Analista de Proyecto	Tesis	Heinar Novas	Santo Domingo	Ejecutor de Entrevistas y Análisis	**Tipo de Interés:** Alto **Influencia:** Baja **Áreas en la que influye:** E
4	Gerencia de Operaciones	Organismo Coordinador	Ivan Veras	Santo Domingo	Facilitador de Información	**Tipo de Interés:** Alto **Influencia:** Baja **Áreas en la que influye**: E
5	Gerentes de Comercial	Organismo Coordinador	Máximo Domínguez	Santo Domingo	Facilitador de Información	**Tipo de Interés:** Alto **Influencia:** Baja **Áreas en la que influye**: E
Leyenda: I: Inicio; P:Planificacion; E: Ejecución; S: Supervisión y Control; C:						

Anexo No.14 Matriz de Comunicación

Información	Contenido	Interesados	Medio para Comunicar	Frecuencia para Comunicar	Responsable de Comunicar
Kick Off del Proyecto	Primera reunión con todos los interesados para dar a conocer el proyecto	Patrocinador Gerente de Operaciones Gerente de Comercial	Reunión Virtual	Única	Gerente de Proyecto
Planificación del Proyecto	Presentación de Alcance, Tiempo, Costos, Recursos y Riesgos	Patrocinador	Reunión Virtual	Única	Gerente de Proyecto
Actividades	Planeación de todas las actividades	Patrocinador y Gerentes de la OC	Reunión Virtual, Llamadas Telefónicas	Semanal	Gerente de Proyecto
Informe del Estado del proyecto	Información sobre los avances del proyecto	Patrocinador	Correo Electrónico	Semanal	Gerente de Proyecto
Plan de Riesgo	Plan de Riesgos para el proyecto	Patrocinador	Reunión Virtual	Única	Gerente de Proyecto
Evaluación Equipo del Proyecto	Evaluación del desempeño del equipo de trabajo y puntos de mejora	Equipo del Proyecto	Correo Electrónico	Trimestral	Gerente de Proyecto
Cambios	Cambios que puedan surgir en el transcurso del proyecto	Patrocinador y Equipo del Proyecto	Correo Electrónico y Ficha de Gestión del Cambio	Única	Gerente de Proyecto
Presentación y Entrega del Plan de Continuidad del Negocio	Entrega del proyecto	Patrocinador	Reunión Presencial Presentación PPT	Única	Gerente de Proyecto

Anexo No.15 Diccionario EDT

Código Paquete Trabajo	1.1.1
Nombre Paquete Trabajo	Análisis y Formulación
Objetivo Paquete Trabajo	Analizar el alcance y tiempo del proyecto
Descripción Paquete Trabajo	Determinar el alcance y tiempo para desarrollar el proyecto, tomando en cuenta la magnitud de la organización
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 15/12/2020
	Fin: 21/12/2020
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	La organización suministrara las informaciones necesarias para la planificación del proyecto
Riesgos	Retrasos en la entrega del análisis y formulación ocasionando desplazamiento en los tiempo del proyecto
Dependencias	

Código Paquete Trabajo	1.2.1
Nombre Paquete Trabajo	Entrevistas
Objetivo Paquete Trabajo	Adquirir las informaciones necesarias
Descripción Paquete Trabajo	Levantamientos de informaciones necesarias para el BIA
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 22/12/2020
	Fin: 29/12/2020
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	El personal entrevistado suministrara todas las informaciones requeridas
	El personal asignado estará disponible
Riesgos	1- Los entrevistados no se muestren colaborativos a la hora de entrevistarlos 2- Los colaboradores de la empresa no cuenten con tiempo suficiente para poder participar en las entrevistas
Dependencias	

Código Paquete Trabajo	1.2.2
Nombre Paquete Trabajo	Identificación de Procesos
Objetivo Paquete Trabajo	Identificar los procesos críticos de la empresa
Descripción Paquete Trabajo	Levantamiento de los procesos de mayor impacto de la empresa
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 30/12/2020
	Fin: 12/01/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	La empresa tendrá y suministrara todos los procesos documentados
Riesgos	Identificar procesos que no sean críticos para el plan de continuidad
Dependencias	1.2.1 Entrevistas

Código Paquete Trabajo	1.2.3
Nombre Paquete Trabajo	Determinación del RTO, RPO y MTPD
Objetivo Paquete Trabajo	Determinar el tiempo objetivo de recuperación, el tiempo máximo de indisponibilidad tolerable y perdida de información en un periodo de tiempo
Descripción Paquete Trabajo	Determinación de los RTO, RPO y MTPD de los procesos que indican cuales tendrá mayor prioridad en la recuperación del mismo
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 13/01/2021
	Fin: 19/01/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	El entrevistado indicara los tiempos de recuperación recomendado
Riesgos	N/A
Dependencias	1.2.2 Identificación de Procesos

Código Paquete Trabajo	1.2.4
Nombre Paquete Trabajo	Determinación Impactos No Financieros
Objetivo Paquete Trabajo	Determinar el nivel de impactos no financieros de los procesos
Descripción Paquete Trabajo	Determinar los impactos operacionales, reputacionales, recursos humanos, social, estratégicos y regulatorio de los procesos identificados como críticos
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 20/01/2021
	Fin: 01/02/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	El entrevistador tendrá el conocimiento necesarios para poder impactar los procesos
Riesgos	N/A
Dependencias	1.2.3 Determinación del RTO, RPO y MTPD

Código Paquete Trabajo	1.2.5
Nombre Paquete Trabajo	Identificación de Interdependencia de los Procesos de Negocio
Objetivo Paquete Trabajo	Identificar las interdependencia de los procesos
Descripción Paquete Trabajo	Determinar cuales sistemas tecnológicos o aplicaciones soportan las operaciones criticas del día a día de la empresa
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 02/02/2021
	Fin: 05/02/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	La empresa otorgara un consolidado de los sistemas tecnológico utilizados.
Riesgos	N/A
Dependencias	1.2.4 Determinación Impactos No Financieros

Código Paquete Trabajo	1.2.6
Nombre Paquete Trabajo	Identificación de Recursos Mínimos Necesarios
Objetivo Paquete Trabajo	Identificar los recursos mínimos necesarios para continuar las operaciones
Descripción Paquete Trabajo	Determinar cuales son los recursos mínimos de personas, sistemas y instalaciones físicas para continuar las operaciones
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 08/02/2021
	Fin: 16/02/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	El entrevistado conoces los recursos mínimos para continuar las operaciones
Riesgos	N/A
Dependencias	1.2.5 Identificación de Interdependencia de los Procesos de Negocio
Código Paquete Trabajo	1.2.7
Nombre Paquete Trabajo	Identificación de Suplidores
Objetivo Paquete Trabajo	Identificar los suplidores críticos
Descripción Paquete Trabajo	Identificar los suplidores de las operaciones criticas de la empresa
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 17/02/2021
	Fin: 23/02/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	El entrevistado conoces los suplidores de las operaciones criticas
Riesgos	N/A
Dependencias	1.2.6 Identificación de Recursos Mínimos Necesarios

Código Paquete Trabajo	1.2.8
Nombre Paquete Trabajo	Consolidación de Información
Objetivo Paquete Trabajo	Consolidar las informaciones de las entrevistas del BIA
Descripción Paquete Trabajo	Consolidar y documentar en el informe del BIA los resultados de las entrevista realizadas
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 24/02/2021
	Fin: 02/03/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	Contar con todas las informaciones necesarias para el BIA
Riesgos	N/A
Dependencias	1.2.7 Identificación de Suplidores

Código Paquete Trabajo	1.2.9
Nombre Paquete Trabajo	Presentación de Resultados
Objetivo Paquete Trabajo	Presentar los resultados del BIA
Descripción Paquete Trabajo	Realización presentación informe de los resultados del BIA en Power Point
Asignación Responsabilidades	Responsable: Fernando Beras
	Aprobador: Manuel López San Pablo
Fechas Programadas	Inicio: 03/03/2021
	Fin: 04/03/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	La presentación será efectuada a tiempo
Riesgos	N/A
Dependencias	1.2.8 Consolidación de Información

Código Paquete Trabajo	1.3.1
Nombre Paquete Trabajo	Entrevistas
Objetivo Paquete Trabajo	Adquirir las informaciones necesarias
Descripción Paquete Trabajo	Levantamientos de informaciones necesarias para el Análisis de Riesgos
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 05/03/2021
	Fin: 11/03/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	El personal entrevistado suministrara todas las informaciones requeridas
	El personal asignado estará disponible
Riesgos	N/A
Dependencias	
Código Paquete Trabajo	1.3.2
Nombre Paquete Trabajo	Identificación de Riesgos
Objetivo Paquete Trabajo	Identificar los riesgos de continuidad
Descripción Paquete Trabajo	Levantamiento de los posibles riesgos que podrían interrumpir los procesos críticos de la empresa
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 12/03/2021
	Fin: 23/03/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	El dueño del proceso tendrá dominio de los posibles eventos de interrupción de sus procesos
Riesgos	Falla en la identificación de riesgos ocasionando que algunas estrategias no sean identificadas
Dependencias	1.3.1 Entrevistas

Código Paquete Trabajo	1.3.3
Nombre Paquete Trabajo	Evaluación de Riesgos
Objetivo Paquete Trabajo	Evaluar los riesgos de continuidad
Descripción Paquete Trabajo	Determinar el nivel de impacto de los riesgos de interrupción de los procesos críticos
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 24/03/2021
	Fin: 29/03/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	Estará disponible el historial de evento de interrupción en el pasado
Riesgos	N/A
Dependencias	1.3.2 Identificación de Riesgos

Código Paquete Trabajo	1.3.4
Nombre Paquete Trabajo	Creación Matriz de Riesgos
Objetivo Paquete Trabajo	Crear matriz de riesgos
Descripción Paquete Trabajo	Consolidar los riesgos identificados y su evaluación dentro de una matriz de riesgos junto a los controles que existen en la actualidad
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 30/03/2021
	Fin: 05/04/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	La matriz de riesgo cuenta con todos los riesgos identificados
Riesgos	N/A
Dependencias	1.3.3 Evaluación de Riesgos

Código Paquete Trabajo	1.3.5
Nombre Paquete Trabajo	Evaluación y Selección de Estrategias
Objetivo Paquete Trabajo	Evaluar y seleccionar las estrategias
Descripción Paquete Trabajo	Evaluar las mejores estrategias para mitigar los riesgos
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 06/04/2021
	Fin: 08/04/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	Se encontrara opciones para mitigar los riesgo de continuidad
Riesgos	No identificación oportuna de las estrategias
Dependencias	1.3.4 Creación Matriz de Riesgos
Código Paquete Trabajo	1.3.6
Nombre Paquete Trabajo	Consolidación de Información
Objetivo Paquete Trabajo	Consolidar las informaciones de las entrevistas del análisis de riesgos
Descripción Paquete Trabajo	Consolidar y documentar en el informe del análisis de riesgos los resultados de las entrevista realizadas
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 09/04/2021
	Fin: 12/04/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	Contar con todas las informaciones necesarias para el análisis de riesgos
Riesgos	N/A
Dependencias	1.3.5 Evaluación y Selección de Estrategias

Código Paquete Trabajo	1.3.7
Nombre Paquete Trabajo	Presentación de Resultados
Objetivo Paquete Trabajo	Presentar los resultados del análisis de riesgos
Descripción Paquete Trabajo	Realización presentación informe de los resultados del análisis de riesgos en Power Point
Asignación Responsabilidades	Responsable: Fernando Beras
	Aprobador: Manuel López San Pablo
Fechas Programadas	Inicio: 13/04/2021
	Fin: 14/04/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	La presentación será efectuada a tiempo
Riesgos	N/A
Dependencias	1.3.6 Consolidación de Información

Código Paquete Trabajo	1.4.1
Nombre Paquete Trabajo	Determinación y Recomendación de Estrategias
Objetivo Paquete Trabajo	Determinar y recomendar las estrategias
Descripción Paquete Trabajo	Crear estrategias que ayude a fortalecer la continuidad de negocio en la empresa de acuerdo a los resultados del BIA y Análisis de Riesgos
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 15/04/2021
	Fin: 21/04/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	Las estrategias serán aceptadas
Riesgos	N/A
Dependencias	

Código Paquete Trabajo	1.4.2
Nombre Paquete Trabajo	Consolidación de Información
Objetivo Paquete Trabajo	Consolidar las informaciones de las estrategias seleccionadas
Descripción Paquete Trabajo	Consolidar y documentar en el informe las estrategias seleccionadas
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 22/04/2021
	Fin: 23/04/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	Contar con todas las informaciones necesarias para las estrategias seleccionadas
Riesgos	N/A
Dependencias	1.4.1 Determinación y Recomendación de Estrategias

Código Paquete Trabajo	1.4.3
Nombre Paquete Trabajo	Presentación de Resultados
Objetivo Paquete Trabajo	Presentar los resultados de las estrategias seleccionadas
Descripción Paquete Trabajo	Realización presentación informe de los resultados de las estrategias seleccionadas en Power Point
Asignación Responsabilidades	Responsable: Fernando Beras
	Aprobador: Manuel López San Pablo
Fechas Programadas	Inicio: 26/04/2021
	Fin: 27/04/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	La presentación será efectuada a tiempo
Riesgos	N/A
Dependencias	1.4.2 Consolidación de Información

Código Paquete Trabajo	1.5.1
Nombre Paquete Trabajo	Plan de Comunicación Ante Incidentes
Objetivo Paquete Trabajo	Crear un plan de comunicación ante incidentes
Descripción Paquete Trabajo	Plantear los lineamientos para establecer una efectiva comunicación durante el estado de contingencia
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 28/04/2021
	Fin: 03/05/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	La comunicación será efectiva
Riesgos	N/A
Dependencias	
Código Paquete Trabajo	1.5.2
Nombre Paquete Trabajo	Plan de Administración Ante Incidentes
Objetivo Paquete Trabajo	Crear un plan de administración ante incidentes
Descripción Paquete Trabajo	Ayudar a gestionar el manejo efectivo de los incidentes antes, durante y después de los mismos, para minimizar los impactos ocasionados por un evento de interrupción
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 04/05/2021
	Fin: 07/05/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	Los incidentes serán administrados adecuadamente
Riesgos	N/A
Dependencias	1.5.1 Plan de Comunicación Ante Incidentes

Código Paquete Trabajo	1.5.3
Nombre Paquete Trabajo	Plan de Recuperación de Negocio
Objetivo Paquete Trabajo	Crear un plan de recuperación de negocio
Descripción Paquete Trabajo	Ayudar a recuperar lo ante posible las operaciones de los procesos críticos
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 10/05/2021
	Fin: 14/05/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	El plan ayudara a recuperar las operaciones en el menor tiempo posible
Riesgos	N/A
Dependencias	1.5.2 Plan de Administración Ante Incidentes
Código Paquete Trabajo	1.5.4
Nombre Paquete Trabajo	Plan de Recuperación de Tecnología
Objetivo Paquete Trabajo	Crear un plan de recuperación tecnológica
Descripción Paquete Trabajo	Describe los procedimientos para recuperar o restaurar la operatividad de los sistemas tecnológicos que soportan los procesos críticos
Asignación Responsabilidades	Responsable: Heinar Novas
	Aprobador: Fernando Beras
Fechas Programadas	Inicio: 17/05/2021
	Fin: 26/05/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	El plan ayudara a recuperar los recursos tecnológicos en el menor tiempo posible
Riesgos	N/A
Dependencias	1.5.3 Plan de Recuperación de Negocio

Código Paquete Trabajo	1.5.5
Nombre Paquete Trabajo	Presentación y Entrega
Objetivo Paquete Trabajo	Presentar y entregar el plan de continuidad de negocio
Descripción Paquete Trabajo	Entregar el proyecto final del plan de continuidad de negocio
Asignación Responsabilidades	Responsable: Fernando Beras
	Aprobador: Manuel López San Pablo
Fechas Programadas	Inicio: 27/05/2021
	Fin: 27/05/2021
Criterios de Aceptación	Terminado en el tiempo programado
Supuestos	El plan de continuidad de negocio será aceptado por la empresa
Riesgos	Incumplimiento en el alcance, tiempo y calidad del proyecto, causando sanciones por la empresa que contrata.
Dependencias	1.5.4 Plan de Recuperación de Tecnología

Anexo No. 16 Matriz de Riesgo de Continuidad del Negocio

# Riesgo	Riesgo	Descripción del Riesgo	Prob.	Impacto	Nivel de Riesgo Inherente	Control Actual	Observaciones	Tipo de Control	Calificación del Control	Prob.	Impacto	Nivel de Riesgo Residual
Personas y Procesos												
Gestión del Conocimiento												
1	Imposibilidad de efectuar labores operativas diarias debido a falta de capacidades técnicas del personal por no recibir capacitaciones periódicas	Se deben impartir capacitaciones periódicas al personal a fin de evitar reproceso, errores y dependencia de personal en la ejecución de la operativa diaria	4	2	Alto	Las areas funcionales y operativas, en conjunto con el departamento de recursos humanos gestionan los entrenamientos necesarios para el personal		Preventivo	2	2	1	Bajo
2	Imposibilidad de efectuar entrenamientos cruzados por posible dependencia de empleados	Se deben efectuar entrenamientos cruzados a fin de evitar la dependencia de empleados	3	2	Moderado	Los integrantes de cada equipo se distribuyen las tareas diarias a fin de mantener un entrenamiento cruzado entre todas las funciones		Correctivo	3	2	2	Bajo
3	Deficiencia en la contratación del personal técnico acorde a los perfiles requeridos debido a no contar con el acompañamiento del departamento de recursos humanos en el proceso de selección y contratación	Se debe contar con el acompañamiento del departamento de recursos humanos en el proceso de selección y contratación de todo el personal	3	2	Moderado	La contratación del personal se efectúa de acuerdo a las descripciones de cargo y al perfil requerido		Preventivo	2	2	1	Bajo
4	Deficiencia en la gestión operativa por falta de personal crítico	Se deben contar con medidas o políticas de retención sobre personal crítico a fin de evitar deficiencia en la gestión operativa diaria	3	3	Alto	No hay control	No hay contr		5	3	3	Alto

Seguridad Laboral											
5	Imposibilidad de responder ante situaciones de emergencia por falta de un proceso de gestión de emergencias	Se debe implementar un proceso de gestión de emergencias laborales con guías de actuación inmediata para controlar daños sobre personas y/o los bienes durante un evento general no esperado	2	4	Alto	La entidad se encuentra en proceso de documentación y aprobación de un plan de emergencias.	No hay contr	5	2	4	Alto
6	Dificultad para responder oportunamente a situaciones de emergencias por falta de capacitación en manejo y control de situaciones críticas	Se deben efectuar capacitaciones periódicas en manejo y control de situaciones críticas a todo el personal a fin de que puedan responder oportuna y eficiente ante situaciones de emergencia.	4	4	Extremo	La entidad brinda entrenamientos de seguridad para las áreas que realizan funciones en las subestaciones eléctricas. Sin embargo, no se imparten entrenamientos para el manejo de emergencias a todo el personal	Correctivo	4	4	4	Extremo
7	Imposibilidad de evacuar efectivamente al personal por no contar con un plan de evacuación ante emergencias	Se debe contar con un plan de evacuación ante emergencias en la organización para el desplazamiento de las personas en una situación de peligro inminente a un sitio seguro.	3	4	Extremo	No hay control	No hay contr	5	3	4	Extremo
8	Falta de capacidades técnicas del personal en manejo de emergencias	Los empleados deben recibir capacitación en seguridad, aplicable a su vida personal o laboral	4	3	Alto	La capacitación de seguridad personal está enfocada solo para el personal que realiza funciones en las subestaciones eléctricas	Preventivo	3	3	2	Moderad
9	Pandemias y/o epidemias en empleados por no efectuar jornadas de vacunación	Se deben efectuar jornadas de vacunación para todo el personal	1	3	Moderad	No se realizan jornadas periódicas de salud o de vacunación.	No hay contr	5	1	3	Moderad
10	Pandemias y/o epidemias en empleados de manera generalizada por no contar con mecanismos para afrontar eventos virus, epidemias, dentro del área de la organización	Se debe contar con mecanismos para afrontar eventos como virus, epidemias, dentro de la organización a fin de no afectar las operaciones diarias	1	3	Moderad	No hay control	No hay contr	5	1	3	Moderad
11	Deficiencia en la atención primaria ante accidentes debido a no efectuar acuerdos con instituciones de salud hospitalaria para atender emergencias	Se deben efectuar acuerdos con instituciones de salud hospitalaria para atender emergencias ocurridas en las instalaciones del OC	2	3	Moderad	No hay control	No hay contr	5	2	3	Moderad
12	Deficiencias visuales de los empleados	Evaluar la implementación de un plan anual de optometría.	1	3	Moderad	No hay control	No hay contr	5	1	3	Moderad
13	Deficiencias auditivas de los empleados	Evaluar la implementación de un plan anual de audiometría	1	3	Moderad	No hay control	No hay contr	5	1	3	Moderad

14	Deficiencia en la realización y corrida de los procesos en caso de contingencia por no contar con documentación formal de los mismos	Los procesos deben estar documentados	3	3	Alto	Al momento se encuenta un 70% de procesos documentados. Y el área de Calidad y Procesos se encuentra en proyecto de documentación de procesos tomando en cuenta los requerimientos de ceritficacion de calidad ISO		Correctivo	3	2	2	Bajo
15	Insuficiencia en la puesta en marcha de planes de contingencia por no contar con certificación de procesos críticos	Los procesos críticos deben estar certificados a fin de optimizar la puesta en marcha de planes de contingencia en caso de ser necesario	3	2	Moderad	documentación de los procesos se encuentran basadas en la ley general de electricidad (125-01), sin embargo no contienen un manual de procedimientos detallado paso a paso		Correctivo	3	2	2	Bajo
16	Definición errónea de procesos por no establecer indicadores de gestión	No deben establecer indicadores en los procesos a fin de evitar la ejecución de los mismos de forma independiente, sin alineación a metas generales ni métricas de desempeño.	3	2	Moderad	Se han implementado indicadores de gestión de los procesos		Correctivo	2	2	1	Bajo
17	Culminación de servicios internos en tiempos errados debido a no establecer acuerdos de niveles de servicio.	Se deben establecer acuerdos de niveles de servicios a fin de cumplir con los tiempos estipulados en el reglamento general de electricidad 125-01 para la entrega de servicios críticos	3	2	Moderad	Acuerdos de servicios establecidos conforme al reglamento general de electricidad 125-01		Correctivo	3	2	2	Bajo
18	Deficiencia en la gestión de procesos durante contingencia por no contar con planes alternos de trabajo para los procesos críticos	Se debe contar con planes de trabajo que consideren los procedimientos alternos a ser llevados a cabo ante cualquier evento o suceso que afecte la continuidad de los procesos críticos, ya sea de carácter natural, físico, tecnológico o humano	2	5	Extremo	No hay control		No hay contr	5	2	5	Extremo

19	Falla en la gestión de procesos y aplicaciones tecnológicas durante una emergencias debido a no efectuar pruebas de los planes alternos	Los planes o procedimientos alternos de trabajo de los procesos críticos deben ponerse a prueba de forma periódica a fin de alcanzar los objetivos propuestos ante una situación de contingencia real.	3	3	Alto	No hay control	No hay contr		5	3	3	Alto
20	Procesos críticos no identificados debido a no realizar análisis de vulnerabilidades	Se debe efectuar análisis de vulnerabilidades y/o amenazas de procesos a fin de identificar puntos críticos y fortalezas que puedan afectar la continuidad del proceso	2	4	Alto	Auditorias externas a los controles de los procesos de la institución. Se ha realizado una matriz de riesgo para la identificación y evaluación de vulnerablidades y amenazas en los procesos.		Correctivo	3	2	3	Moderad
21	Falla en la provisión del servicio por insuficiencia de proveedores	Se deben evitar las dependencias de proveedores externos a fin de no tener puntos únicos de falla	4	4	Extremo	Actualmente existe una dependencia con un mismo proveedor para el enlace entre el OC y ETED en cuanto a la conexión del SCADA.		Preventivo	4	4	4	Extremo
22	Afectación de las operaciones debido a no contemplar mecanismos de contingencia ante eventualidades con los proveedores	Se deben exigir mecanismos de contingencia a los proveedores de servicio en caso de contingencias	3	4	Extremo	Se tienen acuerdos de servicios con el proveedor		Preventivo	2	2	2	Bajo
23	Afectación de las operaciones durante una contingencia real debido a que los mecanismos de contingencia establecidos con los proveedores no son probados de forma periódica.	Se deben probar los mecanismos de contingencia con los proveedores a fin de optimizar la respuesta oportuna en contingencias reales.	4	4	Extremo	No hay control	No hay contr		5	4	4	Extremo
24	Falla en la recuperación de aplicaciones y/o pérdida de información ante interrupciones de mantenimientos no programadas ni notificadas	Las interrupciones deben ser programadas por tecnología y ser notificadas con oportunidad	2	2	Bajo	Todas las interrupciones son notificadas		Preventivo	2	1	1	Bajo
25	Fallas en los procesos diarios debido a la no disponibilidad de aplicativos	Se debe contar con mecanismos redundantes para la prestación efectiva y disponibilidad de servicios tecnológicos	3	3	Alto	Se cuentan con mecanismos redundantes, sin embargo todos se encuentran implementados en un mismo data center		Correctivo	4	3	3	Alto

# Riesgo	Riesgo	Descripción del Riesgo	Prob.	Impacto	Nivel de Riesgo Inherente	Control Actual	Observaciones	Tipo de Control	Calificación del Control	Prob.	Impacto	Nivel de Riesgo Residual
Tecnología												
Disponibilidad												
1	Falta de disponibilidad de servicios tecnológicos	Posible pérdida de información confidencial o privilegiada al momento de interrupción	4	4	Extremo	Servicios críticos identificados, Se cuenta con redundancia de componentes críticos, se realiza mantenimiento preventivo, se cuentan con herramientas para monitoreo de la disponibilida		Preventivo	2	2	2	Bajo
2	Falta de disponibilidad por dependencia con proveedores	Posible falta de disponibilidad debido a dependencias de servicios con un mismo proveedor	2	4	Alto	Enlace redundante para la comunicación del sistema SCADA entre el OC y ETED con un mismo proveedor		Preventivo	4	2	4	Alto
3	Incremento de fallas de componentes de tecnología	Posible pérdida de información confidencial o privilegiada al momento de interrupción	2	4	Alto	Mantenimientos cada 3 meses. Redundancia, pruebas de stress y se notifica a los usuarios. No se tiene programado de manera periódica pero se hace de manera espontánea al menos 2 veces al año.		Preventivo	2	1	2	Bajo

Recuperabilidad											
4	Activación de contingencia a destiempo	Posible pérdida económica / riesgo reputacional, por la falla en la activación de contingencia, tiempos de duración, entre otros.	2	4	Alto	No hay control	No hay contr	5	2	4	Alto
5	Insuficiencia en abastecimiento de componentes tecnológicos	Posible falla en la provisión de servicios	4	4	Extremo	Se contempla el almacenamiento de computadores personales, teclados, mouse, servidores, entre otros.	Correctivo	2	2	2	Bajo
6	Insuficiencia en la provisión de servicios (soporte) al momento de salir de contingencia algún proveedor de la empresa	Posible falla en la provisión de servicios	4	4	Extremo	En el contrato de los proveedores cuentan con penalidades, pero no se les exige estrategias de recuperación o planes de contingencia para sus servicios	Correctivo	3	3	3	Alto
7	Afectación de las operaciones por no disponer de un centro alterno de tecnología	Interrupción de las operaciones. Pérdida de operatividad de los procesos.	3	5	Extremo	No se cuenta con un centro alterno de tecnología	No hay contr	5	3	5	Extremo
8	Deficiencia en la recuperación de información crítica y/o necesaria	Falla en la provisión de servicios de la empresa	3	5	Extremo	Se realizan respaldos, pero no están basados en análisis de riesgos o necesidades del negocio	Preventivo	3	2	3	Moderad

Confiabilidad												
9	Falta de procedimientos para evaluación de eventos	Imposibilidad de tomar medidas defensivas y correctivas oportunamente	3	5	Extremo	Análisis de situaciones conforme al evento registrado		Preventivo	3	2	3	Moderado
10	Afectación o falla de las aplicaciones o de su rendimiento por cambios no programados	Posible falla de las aplicaciones que afecten la operatividad de los procesos	2	5	Extremo	Se realizan controles de cambio, pero no existe un procedimiento formal.		Correctivo	4	2	4	Alto
11	Fallas en la activación de contingencias por desconocimiento de la interdependencia entre aplicaciones	Imposibilidad de tomar medidas defensivas y correctivas oportunamente	2	4	Alto	Se han identificado interdependencias, sin embargo no se ha efectuado un levantamiento de interfaces entre todas las aplicaciones		Correctivo	3	2	3	Moderado
12	Información confidencial expuesta por no disponer de mecanismos de protección de datos	Posible uso no autorizado de información confidencial del OC.	2	4	Alto	No hay control		Correctivo	4	2	4	Alto

# Riesgo	Riesgo	Descripción del Riesgo	Prob.	Impacto	Nivel de Riesgo Inherente	Control Actual	Observaciones	Tipo de Control	Calificación del Control	Prob.	Impacto	Nivel de Riesgo Residual
Fisicos Infraestructura												
Preparación ante Emergencias												
1	Pérdida de activos intelectuales ante el surgimiento de una emergencia / evacuación del personal por falta de un plan de manejo de emergencias	Se debe contar con un plan de manejo de emergencias a fin de responder oportunamente ante una situación de emergencia o evacuación como terremotos, huelgas o incendios y evitar pérdidas intelectuales.	3	3	Alto	No hay control		No hay contr	5	3	3	Alto
2	Integridad física del personal afectada por falta de una brigada para de manejo de emergencias.	Contar con una brigada de manejo de emergencias a fin de responder eficientemente a la atención del personal ante situaciones de emergencia	3	3	Alto	No hay control		No hay contr	5	3	3	Alto
3	Afectación del personal por falta de señalización de rutas de evacuación ante una emergencia.	La edificación debe contar con la señalización adecuada para rutas de escape durante un evento de emergencia (terremotos, huelgas, incendios, etc)	3	4	Extremo	No hay control		No hay contr	5	3	4	Extremo
4	Integridad del personal expuesta ante una evacuación de emergencia debido a la falta de identificación de las salidas de emergencia	Las salidas de emergencias de las instalaciones deben estar señaladas para su inmediata identificación ante una evacuación de emergencia (terremotos, huelgas, incendios, etc.)	2	4	Alto	Se cuenta con salidas de emergencia pero no están debidamente señalizadas		Correctivo	4	2	4	Alto
5	Imposibilidad de detección temprana de incendios por falta de alarmas que alerte al personal	La infraestructura debe contar con alarma contra incendios que permita alertar oportunamente al personal a fin de resguardar su integridad física y evitar la afectación de activos.	3	4	Extremo	No se contempla en la infraestructura del OC, alarmas para la detección de incendios. Solo el Data Center posee una alarma de detección de humo.		Correctivo	4	3	4	Extremo

6	Afectación de la integridad física del personal y de activos, por falta de sistemas automáticos de sofocación o extinción de incendios.	La infraestructura debe contar con sistemas automáticos de sofocación o extinción de incendios que permitan el resguardo físico del personal y de los activos.	3	4	Extremo	Solo el data center cuenta con un sistema de sofocación de incendios, sin embargo el químico no es el adecuado para componentes eléctricos		Correctivo	4	3	4	Extremo
7	Afectación de la seguridad del personal debido a la desorientación visual del personal o de organismos de rescate durante una situación de emergencia o evacuación por la ausencia de energía eléctrica.	Debe contarse con iluminación de emergencia ante la ausencia de energía eléctrica principal, a fin de que tanto el personal como posibles organismos de rescate puedan tener una visión óptima durante una situación de emergencia o evacuación.	3	3	Alto	Lámparas de emergencias que se mantienen encendidas durante la ausencia de energía eléctrica principal		Preventivo	2	2	2	Bajo
8	Afectación de la seguridad física del personal debido a que los organismos de rescate no cuentan con planos básicos de la ubicación e infraestructura del OC que permitan una acción oportuna.	Se debe socializar planos básicos de la ubicación e infraestructura del OC con las entidades de resguardo, a fin de que los mismos puedan actuar oportunamente en beneficio de la integridad física del empleado ante una situación de emergencia o	3	3	Alto	Planos de infraestructura actualizados, sin embargo no se han efectuado acercamientos con organismos de rescate.		Correctivo	5	3	3	Alto
9	Pérdida de activos por falta de entrenamiento en uso de extintores ante situaciones de fuego controlable.	El personal no recibe entrenamiento en el uso de extintores, que permita la sofocación oportuna de focos de incendios.	4	3	Alto	Extintores de incendios instalados en la infraestructura, sin embargo no se da entrenamiento para el uso de los mismos a todo el personal		Preventivo	5	4	3	Alto
10	Pérdida financiera ante demandas por afectación de emergencias a clientes/proveedores	No se entregan o divulgan las principales medidas de seguridad por parte de los porteros o personal responsable a los visitantes	2	3	Moderado	No hay control		No hay contr	5	2	3	Moderado

Incendios												
11	Propagación de incendio por no contar con paredes internas que permitan cortar el fuego.	El edificio debe contar con paredes internas sólidas que permitan cortar fuego	2	4	Alto	Estructura sólida en la nueva sección de la sede y extintores instalados en algunas áreas		Correctivo	3	2	3	Moderado
12	Propagación de incendio por elementos tecnológicos generadores de calor debido a no contar con extintores de fuego que puedan sofocar un foco de incendio generalizado	Se debe contar con extintores de fuego en toda la infraestructura, a fin de poder controlar oportunamente focos de incendios.	2	4	Alto	Extintores de fuego distribuidos en la infraestructura		Correctivo	3	2	3	Moderado
13	Propagación de incendios externos hacia el interior de la edificación del OC debido a que no se realizan análisis o investigaciones en la zona aledaña a fin de identificar posibles generadores de incendios.	Al ser una zona residencial donde se encuentra ubicado el OC, se deben efectuar análisis o investigaciones en la zona aledaña a fin de detectar posibles generadores de incendios que pudieran propagarse hacia el interior	1	4	Alto	Perímetro de áreas verdes entre el OC y las estructuras externas. No se han efectuado análisis o investigaciones		Preventivo	3	1	3	Moderado
14	Pérdida de la edificación por no contar con una infraestructura reforzada que proteja de un incendio exterior.	La construcción del edificio debe ser reforzada y proteger de un incendio exterior	1	4	Alto	Infraestructura externa sólida pero no reforzada.		Correctivo	3	1	3	Moderado

Potencia Eléctrica												
15	Perdida de potencia eléctrica por exceso de calor en acometidas internas	Que las acometidas internas estén sobre canastillas de manera ordenada	1	2	Bajo	Acometidas internas sobre canastillas de forma ordenada		Correctivo	2	1	1	Bajo
16	Pérdida de potencia eléctrica por manipulación indebida de las acometidas	Que las acometidas eléctricas internas se encuentren demarcadas	1	1	Bajo	Canastillas y acometidas eléctricas demarcadas		Preventivo	2	1	1	Bajo
17	Falta de energía ante ausencia de electricidad alterna.	Que la planta eléctrica tenga autonomía mayor a 12 horas en caso de ausencia de la energía principal	4	1	Moderad	Planta eléctrica con autonomía de una semana.		Preventivo	2	2	1	Bajo
18	Falla de la planta eléctrica o UPS al momento de una contingencia por no efectuar mantenimientos periódicos	Que se efectúe mantenimiento periódico y programado a la planta eléctrica y UPS	3	3	Alto	No se efectúa mantenimiento programado y periódico.		Preventivo	4	3	3	Alto
19	Falla de la planta eléctrica y la UPS al momento de una contingencia por no efectuar pruebas de funcionalidad programadas	Que se efectúen pruebas programadas de funcionalidad de la planta eléctrica y las UPS	3	3	Alto	Se prueba la planta y el UPS cuando falla la energía principal. No se realizan pruebas programadas		Correctivo	4	3	3	Alto
20	Falla de la UPS por generación de calor en el cuarto donde se encuentra ubicada	Que el cuarto de las UPS's cuente con extractores de calor	1	5	Alto	Extractor de calor en el cuarto donde se encuentra la UPS		Preventivo	2	1	2	Bajo

Aire acondicionado												
21	Sobrecalentamiento del equipamiento tecnológico SCADA y de los equipos del datacenter por no contar con aire acondicionado de respaldo en caso de fallar el aire principal.	No contar con aire acondicionado de respaldo en la sala de operaciones en tiempo real y en el data center, pudiera ocasionar sobrecalentamiento y daños de los equipos tecnológicos.	2	4	Alto	Aires acondicionadas de respaldos en la sala de operaciones en tiempo real y en el data center		Preventivo	2	1	2	Bajo
22	Mal funcionamiento de los equipos de aire acondicionado por falta de control de temperatura y humedad	No contar con sensores de temperatura y de humedad en los equipos de aires acondicionado, pudiera ocasionar que no se detecte oportunamente un aumento de temperatura o de humedad, ocasionando una falla en los equipos de tecnología	2	4	Alto	Control de temperatura y humedad solo en el DataCenter y Cuarto de UPS.		Preventivo	4	2	4	Alto
23	Mal funcionamiento de los aires acondicionados por no efectuar mantenimiento preventivo	No efectuar mantenimiento preventivo de los aires acondicionados, pudiera acortar la vida útil de los mismos y ocasionar daños irreparables a largo plazo.	2	3	Moderado	Mantenimiento preventivo de los aires acondicionados de la sala de operaciones en tiempo real y del data center		Preventivo	2	1	2	Bajo
24	Daños intencionales al equipamiento de aire acondicionado por no contar con acceso restringido a los mismos.	El acceso al equipamiento del aire acondicionado de la sala de operaciones en tiempo real donde se encuentra el SCADA y al equipamiento del data center debe estar restringido solo a personal autorizado.	2	4	Alto	Acceso restringido solo a personal autorizado al equipamiento del aires acondicionado del data center y al equipamiento de la sala de operaciones en tiempo real donde se encuentra el SCADA		Preventivo	2	1	2	Bajo

Centro de cómputo											
25	Daños o pérdida de los equipos tecnológicos por contar con un piso falso a prueba de fuego	No contar con un piso falso a prueba en fuego en el centro de cómputo y en la sala de operaciones de tiempo real donde se encuentra el equipamiento SCADA, pudiera ocasionar afectación de los equipos tecnológicos en caso presentarse una situación de incendio.	2	4	Alto	No hay control	No hay contr	5	2	4	Alto
26	Daños o pérdida de los equipos tecnológicos por no contar con paredes y cielo falso a prueba de fuego	No contar con paredes y cielo falso a prueba de fuego pudiera ocasionar daños o pérdida de los equipos tecnológicos SCADA y Data center ante situaciones de incendios	2	4	Alto	No hay control	No hay contr	5	2	4	Alto
27	Daños o pérdida de los equipos tecnológicos por existencia de combustibles.	Combustibles generadores de incendios no deben almacenarse dentro de la sala operaciones en tiempo real donde se encuentra el equipamiento SCADA ni el en centro de cómputo	1	5	Alto	No se almacenan combustibles dentro de la sala de operaciones en tiempo real ni dentro del centro de cómputo	Preventivo	2	1	2	Bajo
28	Daños de los equipos tecnológicos por no contar sensores de agua.	No contar con sensores de agua en el centro de cómputo y en sala de operaciones en tiempo real donde se encuentra el equipamiento SCADA, pudiera ocasionar que no se tomen acciones oportunas que eviten una inundación.	2	4	Alto	No hay control	No hay contr	5	2	4	Alto

29	Daños al equipamiento tecnológico por aumento de temperatura debido a la falta de espacio entre unidades.	El espacio entre las unidades debe ser adecuado para permitir que el calor se disipe	2	3	Moderado	Actualmente se cuenta con espacio adecuado, sin embargo no está dimensionado para crecimiento		Correctivo	3	2	2	Bajo
30	Daños del equipamiento tecnológico por no contar con muros externos reforzados que eviten propagación de incendios.	Los muros o linderos que dan al exterior del centro de cómputo y de la sala de operaciones donde se encuentra el equipamiento SCADA, deben ser reforzados a fin de evitar propagación de incendios externos hacia el interior.	2	4	Alto	Muros solidos pero no reforzados		Correctivo	3	2	3	Moderado
31	Daños o hurto de equipamiento tecnológico e información confidencial por no contar con mecanismos electrónicos de control de acceso.	El acceso al centro de cómputo y la sala operaciones en tiempo real donde se encuentra el equipamiento SCADA, debería estar restringido por mecanismos electrónicos a fin de evitar accesos no autorizados y posibilitar la identificación del personal que ha ingresado al mismo.	3	3	Alto	El acceso al centro de cómputo se realiza con llave y no tiene mecanismos electrónicos de control de acceso. El acceso al equipamiento del SCADA ubicado en la sala de operaciones en tiempo real se		Correctivo	4	3	3	Alto
32	Imposibilidad de identificar situaciones irregulares por no contar con un mecanismo de accesos que permita registrar las acciones efectuadas en el área donde se encuentra el equipamiento SCADA dentro sala de operaciones en tiempo real así como dentro del Centro de Datos.	Se debe llevar un registro de accesos que contenga información del personal que ingresa al centro de datos así como al área donde se encuentra el equipamiento SCADA, a fin de registrar al personal que ingresa al mismo y las acciones a realizar.	4	4	Extremo	No se cuenta con mecanismos de registros de accesos al centro de datos ni para el área donde se encuentra el equipamiento SCADA. Sin embargo, el personal de tecnología es responsable de las actividades		Correctivo	4	4	4	Extremo

Seguridad y Acceso												
33	Pérdida de activos e información confidencial debido a no contar con ronderos internos que puedan detectar personal no autorizado en las instalaciones fuera de horario laboral.	Las instalaciones deben contar con vigilantes internos que efectúen rondas periódicas a través de toda la instalación a fin de detectar personal no autorizado fuera de horario laboral	2	3	Moderad	La empresa de vigilancia contratada trabaja 24-7 y efectúa rondas en las noches.		Preventivo	2	1	2	Bajo
34	Actividades delictivas o situaciones irregulares no detectadas oportunamente debido a no contar con cámaras de seguridad.	Contar con cámaras de seguridad en la infraestructura y áreas críticas a fin de identificar posibles situaciones irregulares o actividades delictivas oportunamente.	2	4	Alto	Cámaras de vigilancia en las zonas exteriores de la infraestructura.Solo el data center contiene cámaras en su interior.		Correctivo	2	1	2	Bajo
35	Pérdida de activos e información por no contar con monitoreo activo de las cámaras de vigilancia	Contar con una monitoreo activo de las cámaras de vigilancia de la infraestructura del OC, a fin de detectar oportunamente situaciones irregulares o delictivas.	2	4	Alto	No se realiza monitoreo activo de las cámaras de seguridad		Correctivo	4	2	4	Alto
36	Afectación de la seguridad de personal crítico por accesos a las instalaciones con artículos metálicos no autorizados debido a no contar con mecanismo de detección de metales.	Contar con mecanismo de detección de metales antes del ingreso a las instalaciones que permitan detectar el porte de metales no autorizados	2	4	Alto	No hay control		No hay contr	5	2	4	Alto

37	Activos e información expuesta debido al acceso de personal no autorizado durante la jornada laboral en áreas restringidas	El personal debe estar capacitado para cuestionar a extraños que se encuentren merodeando dentro de las instalaciones durante la jornada laborar	2	4	Alto	Todos los visitantes deben esperar al empleado solicitado en la recepción		Preventivo	3	2	3	Moderado
38	Fallas en los controles de accesos e imposibilidad de identificar personal no autorizado en áreas restringidas por no portar identificación en un lugar visible	Todo empleado y visitante debe portar una identificación en un lugar visible durante su permanencia en las instalaciones.	3	3	Alto	Se entregan carnets de identificación a todo el personal activo. En la recepción se debe entregar carnet temporal a los visitantes.		Correctivo	4	3	3	Alto
39	Pérdida de activos y de información debido a que no se realice una inspección de los elementos que portan los visitantes tanto al ingreso como al momento de retirarse de las instalaciones	Los elementos que portan los visitantes deben revisarse al momento de su ingreso y al momento de su retiro, a fin de identificar posible hurto de activos o información.	3	3	Alto	No hay control		No hay contr	5	3	3	Alto

40	Plagio de información debido al uso no autorizado de cámaras o radios en áreas restringidas.	El uso de cámaras o radios no autorizado debe estar restringido en áreas confidenciales.	2	2	Bajo	No hay control	No hay contr	5	2	2	Bajo
41	Afectación y daños a la estructura debido a no contar con protección contra impactos en las zonas de parqueos	Las zonas de parqueo deben contar con protección contra impactos de vehículos a la estructura, a fin de evitar posibles daños accidentales o deliberados.	2	3	Moderado	Las zonas de parqueo no contienen protección contra impactos a la estructura	Preventivo	4	2	3	Moderado
42	Afectación reputacional debido a no efectuar estudios de antecedentes antes de realizar relaciones comerciales con proveedores de poca confianza	Deben efectuarse estudios de antecedentes antes de realizar una realizar una relación comercial con un proveedor.	4	2	Alto	Se realiza estudio de antecedentes de los proveedores	Preventivo	2	2	1	Bajo
43	Exposición de información confidencial debido a no contar con un procedimiento para la destrucción de información.	Debe contarse con un procedimiento para la destrucción de información confidencial a fin de evitar exposición y uso no autorizado de la misma	2	3	Moderado	No hay control	No hay contr	5	2	3	Moderado