PLAN DE CONTINUIDAD DEL NEGOCIO REFERENTE A LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE LA DIRECCIÓN DE TECNOLOGÍAS E INFORMACIÓN DE LA EMPRESA CDA BASADO EN EL ESTÁNDAR 27031

FABIO FERNANDO ZUÑIGA LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2021

PLAN DE CONTINUIDAD DEL NEGOCIO REFERENTE A LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE LA DIRECCIÓN DE TECNOLOGÍAS E INFORMACIÓN DE LA EMPRESA CDA BASADO EN EL ESTÁNDAR 27031

FABIO FERNANDO ZUÑIGA LOPEZ

Proyecto de Grado – Proyecto aplicado presentado para optar por el titulo de ESPECIALISTA EN SEGURIDAD INFORMATICA

Msc. Katerine Marceles Villalba
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Cali Valle, Mayo 31 de 2022

DEDICATORIA

Dedico a mi hijo, esposa y madre, la realización de este trabajo ya que han sido ellos quienes han estado siempre para mí, y con este proyecto de vida no ha sido la excepción, con su compresión han entendido el tiempo que debo dejar de compartir con ellos para sacar adelante mis estudios.

AGRADECIMIENTOS

Agradezco a la Universidad Nacional Abierta y a Distancia UNAD, quienes con su incansable trabajo nos brindan la oportunidad de prepararnos para el futuro, así mismo, a cada uno de los tutores que me acompañaron simultáneamente, ya que, sin su ayuda y esfuerzo conjunto, este logro no habría sido posible.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

CLASIFICACIÓN DE LA INFORMACIÓN: Es la actividad mediante la cual se resuelve que los datos tengan un lugar con uno de los niveles de agrupación especificados por la organización. Espera garantizar que los datos tengan el grado de seguridad adecuado.

CONFIDENCIALIDAD: Propiedad que verifica que los datos son simplemente accesibles y descubiertos para personas, sustancias o ciclos aprobados.

DISPONIBILIDAD: Propiedad de que los datos estén disponibles y sean utilizables de acuerdo con una entidad aprobada, cuando así lo requiera.

INFORMACIÓN: Conjunto de datos relacionados que tiene importancia para la entidad. Los datos son un recurso importante para los procesos empresariales, lo cual es un elemento crucial en los ejercicios de la entidad, por tanto, necesita un seguro suficiente.

INTEGRIDAD: Propiedad de defender la precisión y el estado completo de los recursos de datos.

USUARIO: Cualquier individuo, elemento, carga útil, medida, marco mecanizado o grupo de trabajo que produce, adquiere, cambia, conserve o utiliza datos en papel o en un medio avanzado, de forma física o a través de organizaciones de información y sistemas de información de la entidad, por las razones de su trabajo y que tendrán el derecho de demostración de uso dentro del stock de datos.

ACTIVOS: Son cada uno de aquellos componentes que son esenciales para el Sistema de Información.

AMENAZAS: Son cada una de esas cosas que le pueden pasar a los recursos de forma anormal.

VULNERABILIDAD: Debilidades en los recursos que pueden ser mal utilizados por amenazas para dañar un recurso (son aperturas de seguridad).

IMPACTO: Consecuencia de la aparición de un peligro sobre un recurso

RIESGOS: Son el efecto secundario del análisis de peligros, es una ponderación del valor del recurso, la probabilidad de que ocurra un peligro y el efecto que debería tener en el marco. Riesgo = Valor del activo + Probabilidad + Impacto

Punto objetivo de recuperación (RPO): Define la pérdida de datos máxima tolerable que se acepta ante una situación de desastre. Por ejemplo, si ocurre un desastre y el nodo del búnker cuenta con dos horas de datos y usted acepta reproducir una hora de datos, el RPO es de una hora. Si no hay pérdida de datos aceptable, el RPO es cero.

MTD (Maximun Tolerable Downtime) o Tiempo Máximo de Inactividad Tolerable. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse

RTO (Recovery Time Objective) o Tiempo de Recuperación Objetivo. Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.

RPO (Recovery Point Objective) o Punto de Recuperación Objetivo. Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre.

WRT (Work Recovery Time): Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos

RESUMEN

La empresa CDA es una empresa industrial y comercial del estado (EICE), desarrollo del objeto social y para que el CDA continúe con los proyectos contenidos en los diferentes planes de acción, se requiere mantener una política de actualización y apropiación de tecnología de la información y telecomunicaciones que le permita ser cada vez más competitivo ofreciendo servicios de una manera óptima, ágil, segura y confiable. El objetivo de este proyecto es diseñar, estructurar y llegar a muy corto plazo implementar un plan de continuidad del negocio y lo referente a seguridad de la información en el CDA.

Este proyecto se realizó con base a la norma ISO/IEC 27031 que ofrece una guía para la preparación en la continuidad del negocio y recuperación de desastres, apoyado del estándar ISO/IEC 27001 que tiene un conjunto de controles para gestión segura de la información.

A partir de estos resultados obtenidos se busca mejorar la continuidad de los servicios prestados a los usuarios finales y la confiabilidad en la información.

ABSTRACT

The CDA company is an industrial and commercial company of the EICE state development of the corporate purpose and for the CDA to continue with the projects contained in the different action plans, it is necessary to maintain a policy of updating and appropriation of information technology and telecommunications that allows you to be increasingly competitive by offering services in an optimal, agile, secure and reliable way, taking this into account the CDA requires implementing, designing, structuring and implementing a business continuity plan and information security through the ISO / IEC 27031 standard that offers a guide for the preparation in business continuity and disaster recovery, supported by the ISO / IEC 27001 standard that has a set of international standards on information security.

INTRODUCCIÓN

Actualmente es de vital importancia para las organizaciones la protección de las personas, el manejo de la integral de la información, la protección y mejora de la reputación y credibilidad empresarial, pero día a día las entidades se encuentran expuestas a riesgos informáticos tanto en el sector público, como en el privado. Con el fin de mitigar dichos riesgos, se han generado toda una serie de procedimientos técnicos que permitan identificar la necesidad de implementar un plan de continuidad en las áreas necesarias, para no bloquear la prestación de los servicios, y crear una ventaja competitiva, con referencia a las normas internacionales, a las nacionales y las que requiere o regula cada compañía.

El presente proyecto de grado, que ofrece una guía para la preparación en la continuidad del negocio y recuperación de desastres en el CDA, implementado bajo la norma ISO/IEC 27031 y apoyado del estándar ISO/IEC 27001, con el fin de realizar una valoración pertinente, y la correspondiente implementación y ejecución, se hace necesario, también realizar una serie de entrevistas, las cuales se documentan en este trabajo de grado, y que se constituyen en evidencia, para el cumplimiento, o no, de ciertos criterios consignados en las normas técnicas antes referenciadas.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Los grandes volúmenes de información que se deben manejar en el mundo contemporáneo se presentan como herramienta fundamental para la competitividad y la eficiencia, que los escenarios socioeconómicos exigen en la actualidad en cualquier ámbito. Por tal motivo, todo avance que se quiera realizar en procura de la eficiencia informática, requiere avances la Ley 1955 de 2019 del Plan Nacional de Desarrollo 2018-2022 “Pacto por Colombia, Pacto por la Equidad” que en su Artículo 3o. Pactos del Plan Nacional de Desarrollo[1], donde especifica sus objetivos de política pública, y una de las estrategias transversales es: Pacto por la transformación digital de Colombia se orienta a que el país debe encaminarse hacia una sociedad digital, mediante el análisis realizado al plan estratégico de tecnologías de la información implementado en el CDA, se tiene una preocupación en el domino del negocio, ya que dentro de las brechas identificadas se encontró que no existe un plan de continuidad del negocio definido, lo cual ha generado consecuencias negativas para la empresas como son la indisponibilidad de aplicaciones o servicios transaccionales y de gestión, adicional a las pérdidas económicas se tienen en ese periodo de tiempo, generando una parálisis total o parcial de los servicios prestados ocasionando inconformidad en los usuarios y ponen en tela de juicio la calidad del servicio.

De todo esto se desprende que el CDA, debe aplicar un plan de continuidad, lo antes posible no solamente para evitar lo anteriormente mencionado sino, además, en búsqueda del mejoramiento continuo en sus procesos.

[1] PLAN NACIONAL DE DESARROLLO. 'Pacto por Colombia, pacto por la equidad' https://www.dnp.gov.co:443/DNPN/Paginas/Plan-Nacional-de-Desarrollo.aspx. 2018-2022

1.2 FORMULACIÓN DEL PROBLEMA

De lo anterior se genera la siguiente pregunta, ¿Cómo se podría construir un plan de continuidad del negocio de desastres para el área de TI del CDA?, por tal motivo se ve la necesidad de presentarle a la entidad una solución para que se implemente un plan de continuidad del negocio inicialmente enfocado al área de TI.

Este proyecto está enfocado en presentarle al CDA una solución para que se implemente un plan de continuidad del negocio inicialmente enfocado al área de TI. Es necesario establecer un plan de acción y evitar una falta de disponibilidad que ocasionan inconformidad en los usuarios y ponen en tela de juicio la calidad del servicio, adicional a esto las pérdidas económicas por cada minuto que se deje de prestar el servicio.

2 JUSTIFICACIÓN

El CDA tiene contemplado en su Plan Estratégico Institucional 2018-2023 en uno de sus objetivos estratégicos es garantizar la seguridad, confidencialidad y disponibilidad de la información, la cual está acorde con las políticas y lineamientos de la Ley 1955 de 2019 del Plan Nacional de Desarrollo 2018-2022 “Pacto por Colombia, Pacto por la Equidad” que en su Artículo 3o. Pactos del Plan Nacional de Desarrollo, donde especifica sus objetivos de política pública, y una de las estrategias transversales es: El Pacto para el cambio digital de Colombia se ajusta en la forma en que la nación debe avanzar hacia una sociedad avanzada, sin perjuicio de lo establecido en el artículo 147 °.[2] Transformación Digital Pública, Los elementos estatales de la orden nacional deben consolidar la parte de transformación digital en sus planes de actividad particulares, adhiriéndose a los principios caracterizados por ello por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Teniendo en cuenta esto la entidad debe adoptar esquemas y soluciones de continuidad del servicio y de recuperación de desastre que le permita a la entidad una alta disponibilidad de sus servicios tecnológicos, enmarcado en las buenas prácticas que nos ofrecen los marcos de referencia alineado con los principios de Arquitectura Empresarial que maneja la empresa, para maximizar la eficiencia operacional y la continuidad del servicio[3].

Por lo anterior, este proyecto está enfocado en presentarle al CDA una solución para que se implemente un plan de continuidad del negocio inicialmente enfocado al área de TI. es necesario establecer un plan de acción y evitar una falta de disponibilidad que ocasionan inconformidad en los usuarios y ponen en tela de

[2] TRUJILLO LÓPEZ, Marcelo. Planeación estratégica de tecnologías informáticas y sistemas de información

[3] GARCÍA MORA, Yury Andrea. Plan de Continuidad de Negocio frente a pandemia de COVID-19. 2020. Tesis Doctoral.

juicio la calidad del servicio, adicional a esto las pérdidas económicas por cada minuto que se deje de prestar el servicio.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar un plan de continuidad del negocio referente a la gestión de la seguridad de la información para el proceso de la dirección de tecnologías e información de la empresa CDA basado en el estándar 27031 con el fin de salvaguardar los activos de información.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los activos de información del proceso de la dirección de tecnologías e información mediante una metodología de gestión de riesgo.

- Determinar los activos críticos y los riesgos de seguridad de la información del proceso de la dirección de tecnologías e información.

- Analizar el impacto en la empresa ante la interrupción en la continuidad del negocio.

- Diseñar un plan de continuidad bajo estándares ISO/IEC 27031 que permita la recuperación de un incidente.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Importancia de un plan de continuidad en una organización. En las grandes y pequeñas empresas de los sectores privado y público, es necesario saber cuáles son los riesgos y amenazas a los cuales estarían expuestos en caso de que ocurran contingencias a nivel tecnológico, naturales, sociales, cambio de empleados o ciberterrorismo, para todo lo expuesto es de gran importancia tener implementado un plan de continuidad del negocio, basado en las mejores prácticas definidas en la serie de familia ISO/IEC 27000, la norma ISO/IEC 27031:2011 incorpora todas las ocasiones y ocurrencias que se identifican con la seguridad de los datos y que podrían afectar la base y los marcos de las TIC[4]. La norma busca dar la coherencia de las administraciones otorgada por la división de TI a los diferentes ciclos de la asociación y está relacionada con la norma ISO/IEC 27001, la cual es una mejora ideal para la Continuidad del Negocio, ya que mejora la respuesta a la interferencia de la ejercicios establecidos por la organización y protege todas las medidas comerciales básicas de los impactos que puedan producirse desastres o daños críticos en los Sistemas de Información, así como garantizar un reinicio tan pronto como el tiempo lo permita. Para el CDA es de gran importancia tener un plan de continuidad del negocio mediante el análisis de riesgos y las metodologías disponibles para el desarrollo de los planes, que se convierta en una herramienta para responder frente a eventos que pongan en riesgo el cumplimiento de los compromisos establecidos con sus clientes, proveedores y demás partes interesadas.[5]

[4] SÁNCHEZ GUERRA, Lidia. Implementación de un Sistema de Gestión de Continuidad de Negocio alineado con la ISO 22301 y la ISO 27031. (2017).

[5] FORTALECIMIENTO DE LA GESTIÓN TI EN EL ESTADO. (s. f.). Modelo de Seguridad -. Recuperado 27 de marzo de 2021, de https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/#5%20Gesti%C3%B3n%20Clasificaci%C3%B3n%20de%20Activos

4.1.2 Estructura de la Norma ISO/IEC 27001 y relación con la continuidad del negocio. Dentro del diseño de la norma ISO/IEC 27001 está la gestión de continuidad del negocio, esta relación incluye la seguridad de los datos para la coherencia empresarial la interacción del directorio, así como la investigación de peligros, estos riesgos pueden ser provocados por diferentes fuentes, tanto internas como externas, uno de ellos es el peligro operacional, que es una disposición impredecible de dificultades, donde hay un montón de trabajo por terminar con ciclos reconocidos, el peligro operacional se abre y percibe a todos los miembros de la asociación y, posteriormente, se convierte en un impulso fantástico para la recarga de Procesos de Gestión Estratégica que consolida lo mejor de las ideas existentes. La gestión de riesgos no es un programa, sino un ciclo con el que se reconoce la posibilidad de causar desgracias por decepciones, carencias e insuficiencias, en RR.HH(Recurso Humano), medidas, innovación, marco o por el evento de ocasiones exteriores[6]. Otro es el riesgo legal que surge por el incumplimiento con reglas o lineamientos y compromisos autoritarios, con los cuales la entidad podría estar autorizado u obligado a remunerar daños, este peligro legítimo surge adicionalmente como resultado de decepciones en acuerdos e intercambios, provenientes de actividades perniciosas, descuidos o manifestaciones obligatorias que influyan en la formalización o ejecución de acuerdos o intercambios. Finalmente, existe el peligro reputacional que ocurre cuando el servicio no es prestado, debido a diferentes situaciones, incurriendo en una imagen negativa, provocando pérdida de clientes y dinero para la empresa.[7]

[6] ICO, Hugo Vecino. Normas ISO y marcos de referencia para gobernanza de las TIC, revisión.
[7] BARATO, F. Impacto financiero en empresas constructoras de vivienda de interés social generadas por la no gestión del riesgo operativo

4.1.3 Preparación del plan de continuidad utilizando como base la norma ISO/IEC 27031. El estándar ISO/IEC 27031 establece las reglas para preparar a las TIC para la continuidad del negocio (IRBC). Presenta el término IRBC determinado a enfatizar todo el clima especializado, no simplemente TI, sino también dándole importancia a las comunicaciones, tanto de voz como de información. Por lo tanto, se construye como una necesidad y para ello los componentes que lo acompañan deben ser supervisados[8], a continuación, se definen los conceptos importantes de los componentes para tener en cuenta relacionados al plan de continuidad, estos son los siguientes:

Individuos: reconocer las técnicas adecuadas para mantener al día las habilidades y la información fundamentales de las TIC. Además de los socios y los trabajadores, también deben pensarse en stakeholders (interesados) que tengan amplia experiencia e información en TIC.

Oficinas: caracterización de procedimientos para disminuir el efecto de la ausencia de accesibilidad de oficinas TIC ordinarias. En esta línea, incluyen: oficinas electivas, lugares para trabajo a distancia.

Tecnología: garantizando que las administraciones TIC de las que dependen los ejercicios empresariales básicos sean accesibles antes de la reanudación de sus ejercicios empresariales básicos. La innovación incorpora: redes, TIC, y software.

Datos: planificación de acuerdos de continuidad que cumplan con el RPO de cada movimiento empresarial básico de la asociación.

[8] CAJAMARCA YUNGA, Jaime Santiago. Plan de recuperación de desastres de la Infraestructura de Tecnologías deInformación, para empresas de prestación de servicios tecnológicos. 2019. Tesis de Maestría. Quito

Procesos: considerando los ciclos importantes para garantizar la practicidad del procedimiento, que incorpora los ciclos esenciales para la evitación, identificación, reacción a episodios y recuperación de fiasco.

Proveedores: distinguiendo y archivando las condiciones externas que soportan la prestación de servicios TIC y tomando las medidas adecuadas para garantizar que sus proveedores puedan suministrar hardware y administraciones básicas dentro de los tiempos de corte preestablecidos y pactados.[9]

Todas las definiciones mencionadas son importantes en este tema, pero se debe resaltar el concepto de procesos, ya que es fundamental identificar la contingencia y recuperación de desastres.

[9] LADINO, Martha Isabel; VILLA, Paula Andrea; LÓPEZ, Ana María. Fundamentos de iso 27001 y su fghjgvcvho6ygtrsw2w aplicación en las empresas

4.2 MARCO CONCEPTUAL

4.2.1 Seguridad De La Información. La norma ISO/IEC 27001 caracteriza la seguridad de los datos como salvaguarda, preservación de la confidencialidad, la integridad y la disponibilidad de los datos; además, puede incluir diferentes propiedades como la autenticidad, la trazabilidad, la no renuncia y la calidad fiable, igualmente se caracteriza como una característica del marco de administración mundial, en vista de una forma de hacer frente a los peligros mundiales de una empresa, cuyo objeto es configurar, realizar, trabajar, hacer observación, exploración, mantenimiento y mejora de la seguridad de los datos, para ello se debe realizar una técnica de Gestión de Continuidad de Negocio para disminuir los impactos potenciales que se puedan producir en la asociación y tener la opción de recuperar a partir de las desgracias de los recursos de los datos, estos impactos pueden introducirse como secuelas de eventos catastróficos, fallos en equipos, actividades deliberadas y percances, para lo cual es necesario consolidar controles prudentes y de recuperación. Dentro de esta estrategia se deben conocer todos los procesos críticos de negocio y se debe coordinar cada uno de los prerrequisitos del Sistema de Gestión de Seguridad de la Información dependiente de la norma ISO/IEC 27001[10].

4.2.2 Seguridad Informática. Según el autor Álvaro Gómez Vietes, “se puede determinar la seguridad de la una computadora personal como cualquier acción que impida la ejecución de un procedimiento no aprobado en un marco u organización, cuyos impactos pueden provocar daños en los datos, confidencialidad, integridad, disminuir la utilidad de los equipos o bloquear el acceso de usuarios autorizados al sistema”[11]

[10] BALDECCHI, R., & DE CALIDAD, G. C. Implementación efectiva de un SGSI ISO 27001
[11] GÓMEZ VIEITES, Á.. Seguridad informática, básico

4.2.3 Sistema De Gestión De Continuidad Del Negocio. La continuidad del negocio se puede caracterizar como una metodología y estrategia de una asociación para recuperarse, restablecer sus capacidades, planificar y reaccionar ante sucesos o calamidades que puedan influir en la accesibilidad, para ofrecer una continuidad en la prestación del servicio. El sistema de gestión de continuidad del negocio (SGCN) comprende tener una base proactiva para la recuperación de cursos de acción alternativos, así como de los servicios básicos de la empresa, a través de la mejora de los instrumentos de investigación y ciclos clave para la recuperación rápida con el fin de limitar impactos y aliviar oportunidades.[12] Según lo indica la norma "ISO/IEC 27031 brinda orientación de continuidad de negocio y recuperación ante desastres TI sobre cómo planificar la continuidad y recuperación TI como parte de un sistema de gestión de continuidad de negocio. El estándar ayuda al personal de TI a distinguir los requisitos previos para la innovación de datos y ejecutar estrategias para reducir el peligro de interrupción, al igual que percibir, reaccionar y recuperarse de una interrupción de las TIC".[13]

[12] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. tecnología de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información (sgsi). Requisitos. NTC-ISO 27001.

[13] GARNICA CARRILLO, Victor Manuel, et al. Plan de gestión mediante la guía del PMBOK para la planificación estratégica del sistema de gestión de la seguridad informática (SGSI) NTC ISO 27001: 2013 para la Clínica Medical Duarte

4.2.4 Análisis de impacto en el negocio (Business Impact Analysis-BIA). La investigación de efectos permite distinguir la gravedad de la recuperación para cada uno de los servicios de la empresa y determinar el impacto, ya que esta continuidad gira en torno al impacto.[14] En el caso primario se valora el efecto administrativo / legítimo, monetario, reputacional, operativo y de atención al cliente para decidir los ciclos básicos y servicios, a los cuales se le aplicará una técnica de recuperación y se les prioriza una continuidad. A estos ejercicios básicos también se le resolverán los tiempos de recuperación, es decir, hasta qué hora la empresa estará en capacidad de soportar una interrupción del servicio, así como los trabajos y grupos encargados de la recuperación.[15]

4.3 ANTECEDENTES

El primer trabajo de investigación que se cita es el que corresponde a “Propuesta de un modelo de plan de continuidad: Un estudio de caso. In Memorias de la Décima Quinta Conferencia Iberoamericana en Sistemas, Cibernética e Informática”.[16] Trabajo de grado presentado en el 2016, por Dante Carrizo, A. Alfaro, y Rodrigo Loyola, donde se enseñan los planes de acción para la continuidad del negocio de informática Minera el Cobre apuntando a las emergencias potenciales y catastróficas. El objetivo fundamental de este proyecto es registrar de manera ideal, clara y concisa la dispersión de los Planes de Contingencia a las distintas áreas o grupos incluidos. De manera coordinada, proponiendo un plan continuidad de negocio, total a la organización, presentando las actividades a continuar en caso de crisis en la operación. Este trabajo se relaciona con la investigación en curso, dado que hace referencian a los aspectos

[14] OLIVARI TAVERA, Juan Mauricio; RAMÍREZ COLL, Carlos Elías. Plan de continuidad del negocio. 2013. Tesis deLicenciatura. Universidad Piloto de Colombia.
[15] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de gestión de continuidad denegocio. NTC- ISO 22301:2012
[16] CARRIZO, DANTE, A. ALFARO, and RODRIGO LOYOLA. "Propuesta de un modelo de plan de continuidad: Un estudio de caso." Memorias de la Décima Quinta Conferencia Iberoamericana en Sistemas, Cibernética e Informática. 2016.

más importante de la continuidad del negocio que pueda causar una interrupción en las operaciones informáticas, independiente de su dimensión, y muestra los diferentes planes de acción que se pueden implementar por medio de listas de distribución que se puedan replicar en las diferentes áreas.

El segundo proyecto de investigación corresponde a “evaluación y tratamiento del análisis de riesgos de la facultad de ciencias informáticas”.[17] Trabajo presentado por Gema Guerrera Bravo y Evelyn Mera en el año 2018, en éste se revelan los riesgos y vulnerabilidades existentes. La búsqueda se realizó en base a las normas ISO/IEC 27001:2005 y Magerit. Reafirmando que la empresa no cuenta con la adecuada seguridad informática que debe ser implementada, se toma como referencia este proyecto, ya que se encuentran varias propuestas de mecanismos de control y gestión de información con el fin de minimizar los riesgos y adicional se tiene un documento complementario donde se incentiva al desarrollo de buenas prácticas en el manejo de los recursos con el fin de apoyar el aseguramiento de la información.

El tercer proyecto es en base a una “Propuesta de un plan de continuidad de innovación de datos para la Dirección de Tecnologías de la Información y las Comunicaciones del Ministerio de Deportes.”[18] Proyecto de grado presentado por Daniel David Uribe en el año 2018. En este trabajo se propone la elaboración de un Plan de Continuidad de Negocio de las Tecnologías de la Información y las Comunicaciones, en el cual se presenta una adecuada gestión de riesgos de la Dirección Tecnológica de las instalaciones principales del Ministerio de Deportes. Este proyecto intenta reducir la probabilidad de fallas en los sistemas y servicios informáticos ante la presencia de ataques o desastres.

[17] GUERRERA BRAVO Gema y MERA Evelyn: “evaluación y tratamiento del análisis de riesgos de la facultad de ciencias informáticas” 2018.
[18] URIBE PUPIALES, Daniel David. "Propuesta de un plan de continuidad de tecnologías de información para la Dirección de Tecnologías de Información y Comunicación del Ministerio del Deporte." 2018.

En este prototipo se presenta una propuesta que sirve para la administración de equipos, permitiendo así asegurar niveles satisfactorios en la disponibilidad de los sistemas y servicios de tecnología, teniendo en cuenta los marcos de referencia como la ISO 22301 e ISO/IEC 27001, permitiendo así disminuir los efectos causados por la suspensión del servicio, teniendo en cuenta esto y lo importante que es para la prestación del servicio en el CDA, se plantea un plan de continuidad basado en la norma antes indicada.

4.4 MARCO LEGAL

Según la misión corporativa de la empresa CDA cita que “estimula una cultura de movilidad, seguridad vial y respeto por el clima; mediante la preparación y evaluación de la capacidad de conducción, la auditoría del estado de los vehículos, los servicios y programas de tránsito y transporte, con esto busca ser la empresa líder de servicios de tránsito y transporte en el Valle del Cauca, destacando la calidad, legalidad y generación de valor a sus grupos de interés, y reconocida por el aporte a la movilidad y seguridad vial”.

4.4.1 Ley 1581 del 2012. La motivación detrás de esta ley es promover el derecho sagrado que toda persona necesita para conocer, actualizar y corregir los datos que se hayan recopilado sobre ella en conjuntos de datos o documentos, y los diferentes derechos, oportunidades y garantías protegidas aludidos en el artículo 15 de la Ley. Constitución Política; así como el derecho de los datos inmersos en el artículo 20 de este mismo.[19]

[19] CÁMARA DE COMERCIO DE BOGOTÁ, Ley 1581 de 2012. 2012.

4.4.2 Ley 1341 de 2009. Por el cual se establecen los estándares y principios sobre la sociedad de datos y la asociación de Tecnologías de la Información y la Comunicación - TIC-, se establece la Agencia Nacional del Espectro y se dan diferentes arreglos.[20]

4.4.3 Ley 1273 de 2009. Conocida como la Protección de datos e información, y preservación de los sistemas que usen las TIC, la cual contiene dos capítulos el primero de ellos trata sobre los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos dentro de este se tienen varios artículos que indican los delitos y las penas a las cuales se enfrentan los actores, igualmente pasa en la segunda parte que habla sobre los atentados informáticos y otras infracciones [21]

[20] CONGRESO, Ley 134, 2009.
[21] "CONGRESO DE LA REPÚBLICA DE COLOMBIA promulgó el 5 de enero de 2009 Ley 1273."

5 DISEÑO METODOLÓGICO

Este trabajo de grado se creó bajo la metodología de un proyecto aplicado, el cual comprende el diseño y el desarrollo avanzado en la solución de conflictos a nivel geográfico y a partir de las técnicas disciplinares y profesionales propias de la especialización en seguridad informática enfocado a la elaboración de un plan de continuidad del negocio que depende de la estrategia propuesta de la norma ISO[22], donde se muestra cómo una organización y en qué orden debe recuperar y restablecer sus capacidades básicas incompleta o completamente interrumpidas dentro de un tiempo preestablecido luego de una interrupción no deseada o desastre[23].

Se recolectará información a través de procesos de observación en cada área de la empresa y a partir de esto un análisis estadístico para manejar los datos cuantitativos y cualitativos[24] con un enfoque experimental y descriptivo.

Este proyecto se desarrollará en 4 fases:[25]

Fase 1: Identificación los activos de información del area de la dirección de tecnologías e información mediante una metodología de gestión de riesgo.

Fase 2: Determinación de los activos críticos y los riesgos de seguridad de la información del proceso de la dirección de tecnologías e información

Fase 3: Analizar el impacto en la empresa ante la interrupción en la continuidad del negocio.

Fase 4: Diseñar un plan de continuidad bajo estándares ISO/IEC 27031 que permita la recuperación de un incidente.

[22] GUERRA ERASO, José Daniel, et al. “Software para el diagnóstico y evaluación de la seguridad de la informaciónempresarial basado en la norma ISO/IEC 27001 de 2013”. 2016.
[23] FERREYRO, A., & Longhi, A. L. D. “Metodología de la investigación.”
[24] “BAENA PAZ, Guillermina María Eugenia. Metodología de la investigación.”
[25] FORTALECIMIENTO TI. (s. f.). Modelo de Seguridad -. Recuperado 27 de marzo de 2021

6 DESARROLLO DE LOS OBJETIVOS

6.1 IDENTIFICAR LOS ACTIVOS DE INFORMACIÓN DEL PROCESO DE LA DIRECCIÓN DE TECNOLOGÍAS E INFORMACIÓN MEDIANTE UNA METODOLOGÍA DE GESTIÓN DE RIESGO.

6.1.1 Selección de metodología de gestión riesgo para identificación de activos. Para el análisis y la gestión se utilizó la metodología Magerit, aplicada a la empresa CDA para la identificación y estimación de los activos y de las posibles amenazas a la infraestructura tecnológica de la organización.

Para citar un ejemplo de la implementación de la metodología MAGERIT para la seguridad de la información "en la empresa Pesquera e Industrial Bravito S.A, pues en ella no se había realizado ningún estudio basado en estándares o metodologías de seguridad de información, por tal motivo se había escogido a MAGERIT. La situación actual en la que se encontraba la empresa en ese tiempo era alarmante, ya que en sus procesos no implementaba medidas de seguridad apropiada, por lo cual provocaba que existiera inseguridad; sin embargo, gracias al análisis de riesgos permitió a la empresa sistematizar las medidas actuales y mejorarlas con algunas otras que fueron suficientes para lograr un nivel de seguridad mayor. [26]

Otro ejemplo es en la Universidad Nacional Toribio Rodríguez de Mendoza (UNTRM) – Chachapoyas Perú, con el fin de mejorar la gestión de seguridad de la información surge la necesidad de establecer una línea de soporte técnico basada en alguna metodología que permita identificar, evaluar y tratar los riesgos de TI, y de esta manera realizar una gestión eficiente de los controles necesarios para

[26] "CRESPO-MARTÍNEZ, Esteban; CORDERO-TORRES, Geovanna. Estudio comparativo entre las metodologías cramm y magerit para la gestión de riesgo de ti en las mpymes. UDA AKADEM", 2016, no 1, p. 38-47.

mitigar los potenciales escenarios de riesgo que podrían afectar o impactar negativamente en la continuidad del negocio, llegando a ocasionar no solo perdida de la información sino también pérdidas económicas, es por ello que se motivan a realizar la implementación de MAGERIT, con el fin de descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.[27]

Por último el Análisis de Riesgos y Recomendaciones de Seguridad de la Información al Área de Información y Tecnología del Hospital SUSANA LÓPEZ DE VALENCIA de la Ciudad de Popayán. Trabajo de grado presentado en el año 2014 por Henry Eduardo Bastidas, Iván Arturo López y Hernando José Peña donde a través de un análisis de riesgos y vulnerabilidades basados en la metodología MAGERIT se realizan una serie de propuestas de mecanismos de control y gestión de información para minimizarlos y se propone también un documento complementario donde se incentiva al desarrollo de buenas prácticas en el manejo de los recursos con el fin de apoyar el aseguramiento de la información.[28]

El modelo MAGERIT, fue desarrollado por el Consejo Superior de Administración Electrónica de España, con el fin de mitigar los riesgos informáticos y de comunicación dentro de las organizaciones, debido al mayor uso que hace hoy en día de ellos, esta metodología de gestión del riesgo nos ofrece beneficios y oportunidades para ser utilizados en el análisis del impacto en una empresa independiente al sector que pertenezca, uno de estos beneficios es la identificación de los activos que son mas sensibles a las amenazas y riesgos por diferentes factores. Es por esto y con base a los antecedentes anteriores, que se selecciona esta metodología con el fin de establecer el marco general de referencia del proyecto, determinando con el análisis de riesgo, el nivel de

[27] ÑAÑEZ CAMPOS, Oscar. "Modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza–Chachapoyas Perú." (2019).
[28] BASTIDAS, Henry, Iván LOPEZ, and Hernando PEÑA. "Análisis de riesgos y recomendaciones de seguridad de la información al área de información y tecnología del hospital Susana López de Valencia de la Ciudad de Popayán." (2014).

inseguridad, de los activos en el CDA, permitiendo la implementación de salvaguarda donde se podrá conocer, impedir y reducir los riesgos identificados, logrando un nivel de seguridad estable dentro de la empresa.

6.1.2 Reconocimiento y clasificación de los activos del proceso. Por medio de esta actividad se reconocieron los activos que hacen parte de la organización definiendo la dependencia entre ellos, realizando su valoración según su importancia, es de anotar que esta clasificación se realizó basado en la metodología Magerit, como se presenta en el cuadro 1, en el cual se establece como convención un código de 3 letras, que corresponden a las primeras letras del nombre de cada activo

Cuadro 1 Listado de activos

ACTIVOS	
[SW] Software	
	[sgf] sistema para gestión financiera
	[sgh] sistema para gestión del recurso humano
	[scv] sistema para el control de versiones
	[smp] sistema para modelamiento de procesos
	[sgf] sistema para la gestión de firmas digitales
	[sgd] sistema para gestión documental
	[sgm] sistema para gestión de la mesa de ayuda
	[sgv] sistema para gestión de videovigilancia
	[sgo] sistema para gestión de ofimática
	[sgot] sistema para gestión de operaciones de transito
	[sar] sistema para acceso remoto
	[sgp] sistema para gestión de pqrs
	[sgi] sistema para gestión de integraciones
	[sgcu] sistema para la gestión de cuentas de usuario
	[sac] sistema para agendamiento de citas
	[ant] antivirus
	[web] Pagina web
[D] Datos / Información	
	[dbo] BD Oracle
	[dbp] BD PostgreSQL
	[dbm] BD MySQL
[HW] Hardware	
	[hsd] Servidor de dominio
	[hsr] Servidor remoto
	[hss] Servidor de soporte

ACTIVOS	
	[hsa] Servidor de aplicaciones
	[hso] Servidor de Oracle
	[hsd] Servidor de DataWareHause
	[hsb] Servidor de BI
	[hsf] Servidor files
	[hsi] Servidor de impresiones
	[hst] Servidor de telefonía
	[hce] Equipos de cómputo de escritorio
	[hpc] Equipos de cómputo de portátiles
[srd] Soporte de la red	
	[swt] switch
	[rou] router
	[apl] Appliance
[COM] Redes de Comunicación	
	[lan] Red local
	[int] internet
[MEDIA] Soporte de información	
	[disk] servidor NAS
[AUX] Equipos auxiliares	
	[ups] Sistema de alimentación ininterrumpida.
	[pe] Planta eléctrica
	[sen] sensor
	[air] Aire Acondicionado
[L] Instalaciones	
	[ofi] Oficinas de la empresa
[P] Personal	
	[use] usuarios finales

Fuente: Elaboración propia

Se tomaron en cuenta estos activos, ya que están relacionados al proceso del área de TI del CDA, la identificación de estos permite a la organización hacer un reconocimiento efectivo de sus activos y como se encuentran relacionados con cada uno de los procesos organizacionales.[29]

Seguido de esto se realizó una la clasificación de activos teniendo en cuenta el inventario de los activos presentes en el proceso de TI de la empresa, la cual corresponde a los dispositivos que realizan el procesamiento de información, infraestructura y sistemas de información, esta clasificación es significativa porque

[29] FRANCO D. Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma iso/iec 27001

le permite a la empresa gestionar y categorizar de manera eficiente, a continuación, se relacionan en el cuadro 2.

Cuadro 2 Clasificación de activos

	CLASIFICACIÓN	ACTIVO	FINALIDAD	TIPO
1	[sgf]	SIESA	Solución de software ERP, diseñada para ajustarse a la plataforma de la empresa (necesidades del negocio). Integra de manera efectiva todas las áreas del negocio.	Software / Aplicaciones Informáticas
2	[sgh]	Nomina WEB	Modulo del ERP que realiza la liquidación de nómina, prestaciones sociales, maneja la gestión de personal.	Software / Aplicaciones Informáticas
3	[scv]	GitLab	Herramienta para el servicio de alojamiento basado en web y donde se lleva el control de versiones de los desarrollos In-hause - Herramienta "open source"	Software / Aplicaciones Informáticas
4	[smp]	BIZAGI	Software BPMN para el modelado y automatización de procesos de todas las áreas del CDA	Software / Aplicaciones Informáticas
5	[sgf]	CERTIFIRMA	Aplicativo que permite identificar a una persona ante un sistema de información.	Software / Aplicaciones Informáticas
6	[sgd]	GFIles	Herramienta para gestión documental que permite automatizar el proceso de gestión documental del CDA	Software / Aplicaciones Informáticas
7	[sgm]	GLPI - Mesa de Ayuda	Herramienta para gestión de servicios de TI, para su funcionamiento y gestión de la mesa de ayuda	Software / Aplicaciones Informáticas

	CLASIFICACIÓN	ACTIVO	FINALIDAD	TIPO
8	[sgv]	HIKVISION IVMS-4200	Este paquete de software proporciona funciones básicas de videovigilancia, que incluyen visualización en vivo en tiempo real, reproducción, grabación de video, búsqueda remota, recuperación de datos e informes.	Software / Aplicaciones Informáticas
9	[sgo]	Office 365	Software usado en todas las áreas del CDA en la cual viene incluida, Correo web institucional como medio de comunicación, Herramienta ofimáticas (Word, Excel, ppt), servicio de alojamiento de archivos en cloud onedrive con capacidad de 1 TB y una herramienta de videollamada Teams.	Software / Aplicaciones Informáticas
10	[sgot]	QX transito	Software diseñado para administrar y asignar a los funcionarios los recursos necesarios para poder acceder a cada una de las operaciones en el Organismo de Tránsito que le corresponde, en CDA es utilizado por tecnología y licencias	Software / Aplicaciones Informáticas
11	[sar]	ONEGATE	Centralizar accesos remotos de los usuarios. Control de aplicaciones, servicios y url's por cada usuario remoto. Reforzar la seguridad de accesos mediante las autenticaciones de doble factor	Software / Aplicaciones Informáticas
12	[sgp]	Virtual Tickets	PST - SaaS, plataforma para gestión de solicitudes, esta aplicación brinda el servicio en una plataforma que permite registrar, escalar, clasificar, organizar y responder requerimientos y/o radicar PQRS por parte de los usuarios o ciudadanos	Software / Aplicaciones Informáticas
13	[sgi]	WSO2 Enterprise Service Bus	Permite integrar aplicaciones existentes en la entidad, aplicaciones externas y las nuevas aplicaciones que sean adquiridas por el CDA, que estén diseñadas bajo una arquitectura orientadas a servicios,	Software / Aplicaciones Informáticas

	CLASIFICACIÓN	ACTIVO	FINALIDAD	TIPO
14	[sgcu]	Directorio activo	Software que permite la administración de cuentas que tienen acceso a varios procesos y SIS - INF de la entidad. Tiene replica en la nube de Office 365, no tiene respaldo activo actualmente	Software / Aplicaciones Informáticas
15	[sac]	Agenda CDA	Sistema para realizar los procesos de agendamiento de citas para licencias, salida vehículos, RTM ,PYG	Software / Aplicaciones Informáticas
16	[ant]	Kaspersky (Protección Antivirus)	Software de protección que detecta y elimina virus y otros tipos de amenazas informáticas. Esta herramienta cuenta con soporte para Windows	Software / Aplicaciones Informáticas
17	[web]	Página web	Pagina institucional de la empresa donde se puede acceder a información básica e informativa para los trámites	Software / Aplicaciones Informáticas
18	[dbo]	TMP_GENERAL	BD Oracle 12c - Principal con información de OT. Contiene información de las licencias de tránsito.	Base de Datos
19	[dbp]	DWH	BD PostgreSQL. Bodega de datos con información de diferentes SI	Base de Datos
20	[dbm]	CDA_CDAparq	BD MySQL Esta base de datos se integra con las aplicaciones del CDA	Base de Datos
21	[hsd]	Servidor XS0104	Servidor hp – servidor de dominio	Hardware / Infraestructura
22	[hsr]	RDS	Servidor remoto instalado en una VM que contiene todos los servidores que va a usar para servicios de Escritorio	Hardware / Infraestructu

	CLASIFICACIÓN	ACTIVO	FINALIDAD	TIPO
			remoto al Administrador del servidor	ra
23	[hsa]	CPU Dell	Servidor de aplicaciones - SO win 10 - Ser App Apache	Hardware / Infraestructura
24	[hso]	sunsol2	Servidor Sun Oracle - Se usan para bases de datos Oracle sobre sistema operativo solaris 11.2	Hardware / Infraestructura
25	[hsd]	DataWH	Servidor HP destinado para el DWH	Hardware / Infraestructura
26	[hsb]	Qlikserver	Server iCloud destinado para BI	Hardware / Infraestructura
27	[hsf]	cda	Servidor de archivos	Hardware / Infraestructura
28	[hsi]	Abka	Servidor de impresión	Hardware / Infraestructura
29	[hst]	Mitrol	Servidor de telefonía	Hardware / Infraestructura
30	[hce]	Dell	Computador de escritorio área TI	Hardware / Infraestructura
31	[hpc]	Lenovo	Computador portátil	Hardware / Infraestructura
32	[swt]	Switch 4	Switch que soporta dispositivos de protección perimetral, vlans (PFS, Internet, PST, wifi, usuarios)	Hardware / Infraestructura
33	[swt]	SW01 - RACK - SERVIDORE	Switch utilizado realizar administración de servidores (Switch52)	Hardware / Infraestructura

	CLASIFICACIÓN	ACTIVO	FINALIDAD	TIPO
		S		
34	[swt]	Switch8	Para conectividad de usuarios, servidores, datos, wifi y voz IP	Hardware / Infraestructura
35	[swt]	Switch28	Cisco Small business 28-port Gigabit PoE Managed Switch, actualmente utilizado para conexión de usuarios, servidores, VoIP y 3 AP,	Hardware / Infraestructura
36	[swt]	Switch-54	Usado para conexión de servidores, usuarios, VoIP, Wi-fi	Hardware / Infraestructura
37	[swt]	Switch Cisco	Switch administrable puertos PoE para internet del operador claro	Hardware / Infraestructura
38	[swt]	switch83e0f2 (Switch 25,16)	Switch Administrable Cisco Small Business 52-port gigabit managed switch, ubicado en el rack del área de licencias para conexión de usuarios, Wi-Fi, VoIP (VLAN 1 -VLAN 90)	Hardware / Infraestructura
39	[rou]	Router NeoGate	Gateway en funcionamiento para VoIP, GSM - Telefonía celular (1 puerto en uso)	Hardware / Infraestructura
40	[rou]	Router Huawei AR161	Proveedor Claro - Internet corporativo - Router de servicios integrados concentra canal backup de internet de la entidad	Hardware / Infraestructura
41	[rou]	Router Cisco Claro	Router Cisco Meraki, Alimenta red Wi-fi	Hardware / Infraestructura
42	[apl]	camaleon2	Appliance UTM para Seguridad (Software Endian firewall) - conexión activo - pasivo	Hardware / Infraestructura
43	[disk]	NAS Soporte	Equipo de almacenamiento en red NAS usado para guardar respaldos de información (backup del principal)	Hardware / Infraestructura

	CLASIFICACIÓN	ACTIVO	FINALIDAD	TIPO
44	[ups]	UPS1	Ups ubicada en el sótano, usada para soportar temporalmente las fallas o caídas de energía que se puedan ocasionar, para garantizar el funcionamiento de los equipos del centro de datos del área de TI del CDA	Hardware / Infraestructura
45	[ups]	UPS2	Ups para respaldo de energía y protección, exclusiva para el centro de datos del CDA, ubicada en el área de TI	Hardware / Infraestructura
46	[sen]	Sensor de temperatura y humedad	Sensor para monitorear temperatura y humedad en el centro de datos	Hardware / Infraestructura
47	[air]	Aire acondicionado	Refrigeración del centro de datos	Hardware / Infraestructura
48	[pe]	Planta Eléctrica	Planta eléctrica que sirve de respaldo cuando ocurren cortes de energía, funciona para toda la entidad	Hardware / Infraestructura
49	[lan]	Red LAN	Estructura de red implementada en el CDA que contiene 100 host para la intranet.	Hardware / Infraestructura
50	[int]	internet	Es un servicio que lo proporciona un proveedor externo CLARO a través de una conexión FO	Hardware / Infraestructura
51	[clt]	Cableado eléctrico	Conexiones eléctricas del CDA	Hardware / Infraestructura
52	[crd]	Cableado de red	Las conexiones de red de datos del CDA utilizan cable UTP cat 7	Hardware / Infraestructura
53	[ofi]	Oficinas de la empresa	Oficina área TI de la empresa CDA	Instalaciones

	CLASIFICACIÓN	ACTIVO	FINALIDAD	TIPO
54	[use]	Usuarios - Funcionarios	Usuarios finales de los diferentes departamentos de la empresa CDA comercial, financiero, recursos humanos, operaciones incluyendo el departamento TI.	Personal

Fuente: Elaboración propia

Para facilitar la clasificación e identificación de los activos del CDA, se ha organizado por categorías, así resulta ideal para que los lideres de procesos entiendan la importancia de los servicios e información que maneja y su responsabilidad en el proceso que les corresponde para el desarrollo del trabajo.

6.2 DETERMINAR LOS ACTIVOS CRÍTICOS Y LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO DE LA DIRECCIÓN DE TECNOLOGÍAS E INFORMACIÓN.

6.2.1 Listar y clasificar activos críticos del proceso. En el desarrollo del proyecto se establecieron los activos que tienen mayor importancia operativa dentro de la organización, es decir los que permiten cumplir de manera efectiva los objetivos, para esta identificación se tuvieron reuniones en las cuales participaron el director del área de TI y los profesionales encargados de los catálogos de servicios a nivel de software, infraestructura y datos.

Una vez se identificados, se realiza la evaluación de los activos en las dependencias, la cual tiene como objetivo realizar una correcta valoración de los riesgos, se procedió a realizar un levantamiento de la información, en el cual se realizan entrevistas con los lideres de los procesos, los cuales nos permiten tener una información más real sobre los riesgos que ya se han presentado, cuáles han sido las causas y como han sido subsanadas esas vulnerabilidades, adicional preguntarles como consideran que la empresa hubiera podido aportar de una manera más eficiente en la solución de los riesgos.

De las entrevistas realizadas en conjunto con la dirección de TI del CDA se definieron los riesgos que se van a trabajar durante el desarrollo del proyecto, en el cual se prioriza los riesgos que representan mayor importancia para la empresa, a continuación, se explican las categorías y dimensiones que se tuvieron en cuenta en la empresa para la identificación del as vulnerabilidades:

Categorías de activos:

[SW] Software: las aplicaciones para llevar a cabo la gestión de los procesos de la organización.
[D] Datos e información: hace referencia a los datos que se genera y recopila, como la gestión documental.
[HW] Hardware: son los equipos físicos que son necesarios para el desarrollo de las labores, como computadores, dispositivos móviles, entre otros.
[SRD] Soporte de la red: Son los equipo activos o pasivos que intervienen en la comunicación de la red interna
[COM] Redes de Comunicación: Hace referencia a los dispositivos que son utilizados para la conectividad de redes, tales como switches, pasarelas, routers, entre otros.
[MEDIA] soporte de información: los medios que permiten almacenar información.
[AUX] equipos auxiliares: soporte a los sistemas de información, como por ejemplo elementos para distribuir datos, climatizadores, entre otros.
[L] Instalaciones: son los sitios donde se ubican los sistemas de la empresa, como oficinas, vehículos, entre otros.
[P] Personal: hace referencia al personal que tiene acceso a la información de la empresa.

Dimensiones

[D] "Disponibilidad.": es la disponibilidad de la información para los usuarios.

[I] "Integridad.": la información debe ser veraz, precisa y completa.

[C] "Confidencialidad.": la información debe estar protegida para evitar alteración o robo.

[A] "Autenticidad de los usuarios y de la información.": se deben acatar los reglamentos internos.

[T] "Trazabilidad." Identificar los procesos que se deben realizar para el tratamiento de la información.

A continuación, como se muestra en el cuadro 3, se identificará la manera en que un activo de mayor orden puede ser afectado por una amenaza materializada sobre un activo de menor orden, donde se encuentran:

Cuadro 3 Valoración dependencias entre activos

	[SW]	[D]	[HW]	[SRD]	[COM]	[MEDIA]	[AUX]	[L]	[P]
[SW]		x	x	x	x				x
[D]									
[HW]							x	x	x
[SRD]									
[COM]								x	x
[MEDIA]									x
[AUX]								x	x
[L]									x
[P]						x			

Fuente: Elaboración propia

La valoración se realizó teniendo en cuenta la categoría de los activos y cada uno de estos como impactaría al verse afectado por una amenaza materializada, de la valoración en cada dimensión descrita, por lo que se puede identificar que la organización al ejecutar sus actividades se vé expuesta a diferentes situaciones que pueden poner en riesgo la información, de allí la importancia de estimar y evaluar los riesgos que se identificaron.

6.2.2 Establecer la criticidad y los riesgos del activo. El análisis de los riesgos se realizó utilizando una valoración por intervalos, analizando estos riesgos según la probabilidad y el impacto, de este análisis se definieron cuáles fueron los activos que superaron el nivel de riesgo tolerable para ser tratados inicialmente. Para lograr estimar el riesgo los activos de la información del CDA se estableció una clasificación las cuales se presentaron a la gerencia y una vez aprobadas se procedió con su implementación teniendo en cuenta los diferentes niveles de probabilidad como se muestra en la tabla 1.

Tabla 1. Criterios de valoración

CRITERIOS		
A+	“Grado alto +”	8
A	“Grado alto”	7
A-	“Grado alto –”	6
M+	“Grado medio +”	5
M	“Grado medio”	4
M-	“Grado medio –”	3
B+	“Grado bajo +”	2
B	“Grado bajo”	1
0	“No tiene valor”	0

Fuente: Metodología MAGERIT

A continuación, en el cuadro 4 se realiza una valoración cuantitativa de los activos del área de TI(Tecnología de la información) del CDA según metodología MAGERIT y norma ISO 27001:2013, el cual permite tener un orden relativo de magnitud del riesgo.

Cuadro 4 Valoración de activos

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[SW] Software					
[sgf] sistema para gestión financiera	B+	A	M+	B	B
[sgh] sistema para gestión del recurso humano	B+	A	M+	B	B
[scv] sistema para el control de versiones	B+	A	M+	B	B
[smp] sistema para modelamiento de procesos	B+	A	M+	B	B
[sgf] sistema para la gestión de firmas digitales	B+	A	M+	B	B
[sgd] sistema para gestión documental	B+	A	M+	B	B
[sgm] sistema para gestión de la mesa de ayuda	B+	A	M+	B	B

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[sgv] sistema para gestión de videovigilancia	B+	A	M+	B	B
[sgo] sistema para gestión de ofimática	B+	A	M+	B	B
[sgot] sistema para gestión de operaciones de transito	B+	A	M+	B	B
[sar] sistema para acceso remoto	B+	A	M+	B	B
[sgp] sistema para gestión de pqrs	B+	A	M+	B	B
[sgi] sistema para gestión de integraciones	B+	A	M+	B	B
[sgcu] sistema para la gestión de cuentas de usuario	B+	A	M+	B	B
[sac] sistema para agendamiento de citas	B+	A	M+	B	B
[ant] antivirus	B+	A	M+	B	B
[web] Pagina web	B+	A	M+	B	B
[DI] Datos / Información					
[dbo] BD Oracle	M+	A+	A	B+	M
[dbp] BD PostgreSQL	M+	A+	A	B+	M
[dbm] BD MySQL	M+	A+	A	B+	M
[HW] Hardware					
[hsd] Servidor de dominio	A+	B+	M+	B	B
[hsr] Servidor remoto	A+	B+	M+	B	B
[hss] Servidor de soporte	A+	B+	M+	B	B
[hsa] Servidor de aplicaciones	A+	B+	M+	B	B
[hso] Servidor de Oracle	A+	B+	M+	B	B
[hsd] Servidor de DataWareHause	A+	B+	M+	B	B
[hsb] Servidor de BI	A+	B+	M+	B	B
[hsf] Servidor files	A+	B+	M+	B	B
[hsi] Servidor de impresiones	A+	B+	M+	B	B
[hst] Servidor de telefonía	A+	B+	M+	B	B
[hce] Equipos de cómputo de escritorio	A+	B+	M+	B	B
[hpc] Equipos de cómputo de portátiles	A+	B+	M+	B	B
[SRD] Soporte de la red					
[swt] switch	A+	A+	A+	A+	A+
[rou] router	A+	A+	A+	A+	A+
[apl] Appliance	A+	A+	A+	A+	A+
[COM] Redes de Comunicación					
[lan] Red local	A+	A+	A+	A+	A+
[int] internet	A+	A+	A+	A+	A+
[MEDIA] soporte de información					
[disk] servidor NAS	A+	A+	A+	A+	A+
[AUX] equipos auxiliares					
[ups] Sistema de alimentación ininterrumpida.	A+	B+	B+	B+	B+
[pe] Planta eléctrica	A+	B+	B+	B+	B+
[sen] sensor	A+	B+	B+	B+	B+
[air] Aire Acondicionado	A+	B+	B+	B+	B+
[L] Instalaciones					
[ofi] Oficinas de la empresa	A+	A+	A+	A+	A+
[P] Personal					
[use] usuarios finales	A+	A+	A+	A+	A+

Fuente: Elaboración propia

Teniendo en cuenta los resultados se puede indicar que para los activos de software y de datos se tiene un nivel de valoración alto en la integridad y que para

los activos de hardware el nivel de valoración más alto es la disponibilidad, por lo cual se debe realizar el tratamiento de los activos que tienen una valoración alta.

De acuerdo con el análisis anteriormente realizado se procedió a realizar un análisis de riesgo para identificar las vulnerabilidades (Ver Anexo 1). Los resultados que muestra la siguiente tabla son de gran importancia, ya que es donde se muestra el nivel de riesgo, los niveles muy alto (MA), serán los escenarios donde se deben desarrollar las alternativas de solución que harán que se evite, mitigue, transfiera o también que se acepten determinados riesgos.

A continuación, en el cuadro 5 se tiene la evaluación de las amenazas y vulnerabilidades de cada uno de esos activos críticos que se identificaron previamente.

Cuadro 5. Amenazas y vulnerabilidades de activos de información

SISTEMA TI	ACTIVO DE INFORMACIÓN	AMENAZA	VULNERABILIDAD	PROBABILIDAD DE OCURRENCIA	IMPACTO	RIESGO
Aplicaciones	Siesa	Defacement (desfiguración página web)	Mal diseño del sitio web	Medio	Alto	Alto
	Nomina Web	Acceso no Autorizado	Ausencia de Control de Acceso a Funciones	Medio	Alto	Alto
	Certifirma	Pérdida de Autenticación	Incorrecta Gestión de la Información	Medio	Alto	Alto
	QX transito	Denegación de servicio	Indisponibilidad de los servicios	Medio	Alto	Alto
	Agenda CDA	Errores de mantenimiento / actualización de programas (software)	Fallas Tecnológicas en los Sistemas de Procesamiento	Medio	Alto	Alto
	Integrador de aplicativos	Ingeniería social	Fraude Interno de obtener Información para intereses	Medio	Alto	Alto

SISTEMA TI	ACTIVO DE INFORMACIÓN	AMENAZA	VULNERABILIDAD	PROBABILIDAD DE OCURRENCIA	IMPACTO	RIESGO
			propios o hacia terceros			
	Alat P&G	Denegación de servicio	Pérdidas económicas	Medio	Alto	Alto
	Acciweb	Espionaje de un Usuario a otro Usuario	Exposición de datos sensibles	Medio	Alto	Alto
	Innova	Fallo de servicios de comunicaciones	Indisponibilidad de los servicios	Medio	Alto	Alto
	RUNT	Pérdida de Autenticación y Gestión de Sesiones	Sanciones legales derivado del incumplimiento de ley	Medio	Alto	Alto
Sistemas de Bases de datos	MySQL	Ataques basados en datos	Acceso no Autorizado a la Información o a los recursos de los Sistemas de Procesamiento.	Medio	Alto	Alto
	Oracle	Caída del sistema por agotamiento de recursos	Suspensión de las actividades misionales de la organización	Medio	Alto	Alto
	PostgreSQL	Alteración de la información / Modificación de la Información	Exposición de datos sensibles	Medio	Alto	Alto
Seguridad de la Información	Directorio activo	Errores del administrador	Acceso no Autorizado a la Información o a los recursos de los Sistemas de Procesamiento.	Medio	Alto	Alto
Sistemas de almacenamiento	Servidor de Archivos	Degradación de los soportes de almacenamiento de la información	Indisponibilidad de los servicios	Medio	Alto	Alto
Comunicaciones	Red LAN	Avería de origen físico o lógico	Indisponibilidad de los servicios	Medio	Alto	Alto

SISTEMA TI	ACTIVO DE INFORMACIÓN	AMENAZA	VULNERABILIDAD	PROBABILIDAD DE OCURRENCIA	IMPACTO	RIESGO
	Internet	Caída del sistema por agotamiento de recursos	Pérdidas económicas	Medio	Alto	Alto
Infraestructura	Centro de datos	Condiciones inadecuadas de temperatura y/o humedad	Fallas Tecnológicas en los Sistemas de Procesamiento	Medio	Alto	Alto

Fuente: Elaboración propia

"Las vulnerabilidades son las debilidades de seguridad de Información asociadas a los activos de información y se hacen efectivas cuando una amenaza la materializa en los sistemas de información de las Entidades".[30] En la tabla anterior, se identificó, que tanto el impacto como el riesgo de los activos analizados es alto, lo que quiere decir es que no precisamente son causa de daño, sino que son condiciones que pueden hacer que una amenaza afecte al activo de la información.

6.3 ANALIZAR EL IMPACTO EN LA EMPRESA ANTE LA INTERRUPCIÓN EN LA CONTINUIDAD DEL NEGOCIO.

Una de las partes clave para el desarrollo de un plan de continuidad en una empresa, es el BIA (Análisis de Impacto de Negocio), ya que este análisis permite determinar principalmente el impacto operacional de los servicios como también el impacto económico.

Teniendo en cuenta este análisis se utilizó la metodología del Análisis de Impacto del Negocio, que consiste en definir una serie de pasos con el objeto de identificar claramente los impactos de las interrupciones y tomar decisiones respecto a aquellos procesos que se consideran críticos para la organización y que afectan directamente el negocio ante la ocurrencia de un desastre, abordando las

[30] MINTIC. Guía para realizar el Análisis de Impacto de Negocios BIA. 2015

actividades y resultados obtenidos en la identificación del riesgo y la caracterización de los procesos de la empresa que se identificaron como prioritario dentro del área de gestión de TI.

Para llevar a cabo esta etapa es necesaria la elaboración de un plan de trabajo detallado, donde se enumeren las actividades que se llevaran a cabo para poder implementar estas normas desde el punto de vista de la documentación.[31]

- Definición e implementación de política de objetivos de la seguridad informática.
- Declaración de la aplicabilidad.
- Plan de tratamiento de riesgos.
- Marco legal y jurídico de la seguridad informática.
- Definición de funciones y responsabilidades de seguridad.
- Política de seguridad para proveedores.

Para el desarrollo, se realiza un levantamiento de la información mediante:

- Entrevista con los lideres de proceso para conocer los procesos, procedimientos, instructivos, manuales, normativas, para el desarrollo.
- Observación de los procesos.
- Reunión con el gerente general para definir prioridad procesos.

[31] (IDB.) BANCO INTERAMERICANO DE DESARROLLO, Ciberseguridad riesgos, avances y el camino a seguir en américa latina y el caribe.

6.3.1 Identificación de la situación de riesgo Se realizo un análisis de impacto en el negocio, a los servicios críticos de la entidad, en el análisis se tuvieron en cuenta todos los procesos del área TI, como los activos de información, que soportan el catálogo de los servicios que son considerados importantes para la recuperación, los roles de los encargados de soportar los servicios y establecer los tiempos de recuperación, que debe tener en caso de que se presente una interrupción, se identificó la prioridad de los elementos de recuperación, y se les brindara la continuidad de negocio para luego establecer la estrategia de recuperación. Los servicios esenciales tratados en su mayoría son operacionales, ya que estos interactúan directamente con los funcionarios de otras dependencias y entes externos.

Teniendo en cuenta los elementos operacionales de la organización, se requiere determinar el nivel de impacto de una interrupción dentro de la empresa, para ello se realizó un esquema de valoración en el cual se evalúa el nivel negativo en varios aspectos de las operaciones del negocio.
Para determinar qué tan crítico resulta un activo para la empresa, se estableció el nivel como aparece en la tabla 2

Tabla 2 Niveles de criticidad de servicio

VALOR	INTERPRETACIÓN DEL PROCESO CRÍTICO
A	Crítico para el negocio
B	No es crítico para el negocio
C	No es parte integral del negocio

Fuente: Guía N° 10 MINTIC “Identificación de Procesos Críticos”

En el siguiente cuadro 6, se evalúa el impacto operacional para los servicios críticos del CDA, esto permite definir el nivel de tolerancia en horas en caso de la ocurrencia de una falla en alguno de los servicios, para esta valoración se toma como referencia los niveles ya definidos en el análisis de riesgos que se muestra en la tabla 2.

Cuadro 6. Evaluación de impactos operacionales para los servicios críticos

CATEGORÍA DEL SERVICIO	SERVICIO	NIVEL	TOLERANCIA A FALLAS (HORAS)	DESCRIPCIÓN
Aplicaciones	SIESA	A	4	ERP de la empresa
	Nomina WEB	A	4	Sistema de Nomina de la empresa
	GitLab	B	12	Herramienta de control de versiones
	BIZAGI	C	12	BPMN
	CERTIFIRMA	A	4	Sistema de identificación
	GFIles	A	4	Sistema de gestión documental
	GLPI - Mesa de Ayuda	A	4	Gestión mesa de ayuda
	Office 365	B	8	Herramienta ofimática
	QX transito	A	4	Módulos que permiten la realización de varios procesos transversales de la empresa
	Virtual Tickets	B	12	Sistema para la atención de PQRS
	WSO2 Bus	B	8	Sistema que realiza la comunicación segura entre aplicaciones
	Agenda CDA	A	4	Sistema de agendamiento
	Qlik sense	B	8	Sistema de BI
	Outlook	B	8	Correo corporativo
	Integrador de aplicativos	A	2	sistema que integra varios procesos críticos de la empresa
	Alat P&G	A	2	Sistema para el registro de infracciones online
	Acciweb	A	4	Sistema para el registro de accidentes
	Innova	A	4	Sistema que recolecta la información de las pruebas RTM
	Página web	B	8	Página web CDA
	HQ RUNT	A	4	Aplicación para realizar los procesos de licencias
	ONEGATE	B	12	Centraliza los accesos remotos desde afuera hacia la empresa
	Share Point	B	12	Sistema para compartir información
Base de datos	MySQL	A	2	BD utilizado por diferentes aplicaciones
	Oracle	A	2	BD utilizado por diferentes aplicaciones
	PostgreSQL	B	8	BD utilizado por el DWH
	Sql server	B	8	BD utilizado por Bizagie
Seguridad de la Información	Directorio activo	A	2	Sistema de administración y gestión centralizada de las cuentas de usuario
	Kaspersky (Protección	B	8	Software de protección que detecta y elimina virus

CATEGORÍA DEL SERVICIO	SERVICIO	NIVEL	TOLERANCIA A FALLAS (HORAS)	DESCRIPCIÓN
	Antivirus)			
	Firewall	A	4	Equipo que brinda seguridad perimetral
	Radius	B	8	Servicio de seguridad para los puntos de red.
Sistemas de almacenamiento	Servidor de Archivos	A	2	Servidores para guardar / compartir información
	NAS Soporte	B	6	Dispositivo para almacenamiento de información en red
Comunicaciones	Switch Cisco	B	4	Equipo para conexión de usuarios, Wi-Fi, VoIP (VLAN 1 - VLAN 90)
	Red Lan	A	2	Cableado físico
	Internet	A	2	Servicio para navegar en Internet
	MPLS	A	2	Servicio de conexión entre sedes del CDA
Infraestructura	Centro de datos	A	2	Control de operaciones de Servidores, Equipos de Comunicaciones, Sistemas de Almacenamiento, Sistemas de Backups, Aire Acondicionado, Acometida Eléctrica
Soporte Informático	Equipos de cómputo de las áreas	B	6	Equipos de cómputo de las áreas

Fuente: Elaboración propia

La evaluación se basa en una matriz de impactos operacionales que ofrece el (MINTIC) en el 2015 publicó una guía para la elaboración del BIA, en el punto 5.1.3.2. Evaluación de Impactos Operacionales[32].

Con lo anterior se logró identificar con las categorías de los servicios principales y que son críticos prestados por el área de TI del CDA, a estos procesos se les definió el nivel de criticidad y su tiempo tolerable a fallas.

[32] MINTIC. Guía para realizar el Análisis de Impacto de Negocios BIA. 2015.

Posterior a la identificación de los procesos críticos de la empresa, se definen los tiempos de recuperación los cuales corresponden al tiempo de disponibilidad para la recuperación ante una falla o alteración de estos, estos se fundamentan en el BIA como muestra la siguiente tabla:

Tabla 3. Descripción tiempos de recuperación

TIEMPO DE RECUPERACIÓN	DESCRIPCIÓN
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo.
MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

Fuente: Guía N° 10 MINTIC “Descripción tiempos de recuperación”

Teniendo en cuenta esta descripción, se realiza la identificación del MTD que corresponde al tiempo Máximo de Inactividad que puede soportar la empresa antes de que colapse su operación, con esto se establece la prioridad para la recuperación del servicio.

Para conocer los servicios críticos se evaluará de 4 maneras; un impacto cuantitativo representando por pérdidas financieras en el momento que se presenta una interrupción, un impacto cualitativo o de imagen frente a los funcionarios y la ciudadanía, un impacto legal regulatorio y un impacto operativo. De acuerdo con esto se pueden diferenciar escenarios de interrupciones por la que puede afectar el proceso.

- Ausencia de Personal: se presenta cuando el funcionario o contratista que ejecuta el proceso no puede asistir a trabajar para desarrollar las actividades propias de su cargo.

• No acceso al sitio normal de trabajo: se presenta cuando por algún evento como desastre natural, enfermedad contagiosa, actividad terrorista, problemas de transporte, huelgas, entre otros, el personal no puede acceder a su lugar de trabajo para desarrollar las actividades propias de su cargo. En este caso y con el ánimo de no interrumpir la operación del proceso crítico se debe contar con un sitio alterno de trabajo, el cual puede ser:

- Suministrado por la Entidad, ejemplo: otra sede.
- Suministrado por un proveedor, contratista o aliado estratégico.

• Caída de los sistemas tecnológicos: se presenta cuando el hardware y/o software presenta falla(s) o cuando haya interrupción prolongada de las comunicaciones, ocasionados por: datos corruptos, fallos de componentes, falla de aplicaciones y/o error humano.

• No contar con los Proveedores Externos: Se presenta cuando una o varias actividades del proceso crítico son realizadas por el proveedor y cualquier falla de éste, generaría la no realización efectiva del proceso. En este caso se debe garantizar que en el contrato con el proveedor se especifique la existencia de un Plan de Continuidad del Negocio documentado, adicional, sea probado en conjunto con los colaboradores de la Entidad y aprobado la dirección de TI.

En el siguiente cuadro se relacionan los tiempos establecidos para lograr la recuperación de los procesos:

Cuadro 7. Tiempos de recuperación por procesos

CATEGORÍA	PROCESO CRÍTICO	MTD (en Horas)	PRIORIDAD DE RECUPERACIÓN
Aplicaciones	SIESA: ERP de la empresa	0.5	1
	Nomina WEB: Sistema de Nomina de la empresa	0.5	1

CATEGORÍA	PROCESO CRÍTICO	MTD (en Horas)	PRIORIDAD DE RECUPERACIÓN
	GitLab: Herramienta de control de versiones	2	3
	BIZAGI: BPMN	3	3
	CERTIFIRMA: Sistema de identificación	0.5	1
	GFIles: Sistema de gestión documental	1	2
	GLPI - Mesa de Ayuda: Gestión mesa de ayuda	1	2
	Office 365 :Herramienta ofimática	1	2
	QX transito: Módulos que permiten la realización de varios procesos transversales de la empresa	0.5	1
	Virtual Tickets: Sistema para la atención de PQRS	1	2
	WSO2 Bus: Sistema que realiza la comunicación segura entre aplicaciones	1	2
	Agenda CDA: Sistema de agendamiento	0.5	1
	Qlik sense: Sistema de BI	2	3
	Integrador de aplicativos: sistema que integra varios procesos críticos de la empresa	0.5	1
	Alat P&G: Sistema para el registro de infracciones online	0.5	1
	Acciweb: Sistema para el registro de accidentes	0.5	1
	Innova: Sistema que recolecta la información de las pruebas RTM	0.5	1
	Página web: Página web CDA	1	2
	Outlook: Correo corporativo	1	2
	Office 365 :Herramienta ofimática	1	2
	RUNT: Aplicación para imprimir las licencias de tránsito, liberar sustratos, reimpresiones, liquidación, imprimir certificado de RTM	0.5	1
	ONEGATE: Centraliza los accesos remotos desde afuera hacia la empresa	2	3
	Share Point: Sistema para compartir información	2	3
Sistemas de Bases de datos	MySQL: BD utilizado por diferentes aplicaciones	0.5	1
	Oracle: BD utilizado por diferentes aplicaciones	0.5	1
	PostgreSQL: BD utilizado por el DWH	0.5	1
	Sql server: BD utilizado por Bizagie	1	2
Seguridad de la Información	Directorio activo: Sistema de administración y gestión centralizada de las cuentas de usuario	0.5	1
	Kaspersky (Protección Antivirus): Software de protección que detecta y elimina virus	1	2

CATEGORÍA	PROCESO CRÍTICO	MTD (en Horas)	PRIORIDAD DE RECUPERACIÓN
	Firewall: Equipo que brinda seguridad perimetral	1	2
	Radius: Servicio de seguridad para los puntos de red.	2	3
Sistemas de almacenamiento	Servidor de Archivos: Servidores para guardar / compartir información	0.5	1
	NAS Soporte: Dispositivo para almacenamiento de información en red	1	2
Comunicaciones	Switch Cisco: Equipo para conexión de usuarios, Wi-Fi, VoIP (VLAN 1 -VLAN 90)	1	2
	Router Neogate: Proveedor Claro Internet	1	2
	Red Lan: Cableado físico	0.5	1
	Internet: Servicio para navegar en Internet	0.5	1
	MPLS: Conexión con otras sedes del CDA	1	2
Infraestructura	Centro de datos	0.5	1
Soporte Informático	Equipos de cómputo de las áreas	1	2

Fuente: Elaboración propia

De las diferentes actividades contempladas en la función crítica del negocio, deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio; por lo tanto, es clave en este punto, la identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomar acciones para medir el impacto del negocio de las Entidades.

Dicho lo anterior con los lideres de procesos y realizando una integración con las amenazas conocidas y relacionadas con la metodología MAGERIT, en el siguiente cuadro se identificaron los recursos críticos del Sistema de Tecnologías e Información.

Cuadro 8. Identificación de recursos críticos del sistema TI

CATEGORÍA	PROCESO CRÍTICO	IDENTIFICACIÓN DE RECURSOS CRÍTICOS DE SISTEMAS TI
Aplicaciones	Siesa	ERP de la empresa
	Nomina Web	Sistema de Nomina de la empresa
	Certifirma	Sistema de identificación
	QX transito	Módulos de pagos que permiten la realización de varios

CATEGORÍA	PROCESO CRÍTICO	IDENTIFICACIÓN DE RECURSOS CRÍTICOS DE SISTEMAS TI
		procesos transversales de la empresa
	Agenda CDA	Sistema de agendamiento
	Integrador de aplicativos	sistema que integra varios procesos críticos de la empresa
	Alat P&G	Sistema para el registro de infracciones online
	Acciweb	Sistema para el registro de accidentes
	Innova	Sistema que recolecta la información de las pruebas RTM
	RUNT	Aplicación usada para imprimir las licencias de tránsito, liberar sustratos, reimpresiones, liquidación, imprimir certificado de RTM.
Sistemas de Bases de datos	MySQL	BD utilizado por diferentes aplicaciones
	Oracle	BD utilizado por diferentes aplicaciones
	PostgreSQL	BD utilizado por el DWH
Seguridad de la Información	Directorio activo	Sistema de administración y gestión centralizada de las cuentas de usuario
Sistemas de almacenamiento	Servidor de Archivos	Servidores para guardar / compartir información
Comunicaciones	Red LAN	Cableado físico
	Internet	Servicio para navegar en Internet
Infraestructura	Centro de datos	Control de operaciones de Servidores, Equipos de Comunicaciones, Sistemas de Almacenamiento, Sistemas de Backups, Aire Acondicionado, Acometida Eléctrica

Fuente: Elaboración propia

Posterior a esta identificación de los procesos críticos del área TI de la empresa CDA, se aplica el WRT que significa el tiempo requerido de trabajo para la recuperación del servicio, para esto se específica en el siguiente cuadro:

Cuadro 9. Disposición de los RTO/RPO

CATEGORÍA	PROCESO CRÍTICO	IDENTIFICACIÓN DE RECURSOS CRÍTICOS DE SISTEMAS TI	RPO (Horas)	RTO (Horas)
Aplicaciones	Siesa	ERP de la empresa	2	0.5

CATEGORÍA	PROCESO CRÍTICO	IDENTIFICACIÓN DE RECURSOS CRÍTICOS DE SISTEMAS TI	RPO (Horas)	RTO (Horas)
	Nomina Web	Sistema de Nomina de la empresa	2	0.5
	Certifirma	Sistema de identificación	2	0.5
	QX transito	Módulos de pagos que permiten la realización de varios procesos transversales de la empresa	2	0.5
	Agenda CDA	Sistema de agendamiento	1	0.5
	Integrador de aplicativos	sistema que integra varios procesos críticos de la empresa	1	0.5
	Alat P&G	Sistema para el registro de infracciones online	1	0.5
	Acciweb	Sistema para el registro de accidentes	3	0.5
	Innova	Sistema que recolecta la información de las pruebas RTM	1	0.5
	RUNT	Aplicación usada para imprimir las licencias de tránsito, liberar sustratos, reimpresiones, liquidación, imprimir certificado de RTM.	2	0.5
Sistemas de Bases de datos	MySQL	BD utilizado por diferentes aplicaciones	1	0.5
	Oracle	BD utilizado por diferentes aplicaciones	1	0.5
	PostgreSQL	BD utilizado por el DWH	1	0.5
Seguridad de la Información	Directorio activo	Sistema de administración y gestión centralizada de las cuentas de usuario	1	0.5
Sistemas de almacenamiento	Servidor de Archivos	Servidores para guardar / compartir información	1	0.5
Comunicaciones	Red LAN	Cableado físico	1	0.5
	Internet	Servicio para navegar en Internet	1	0.5
Infraestructura	Centro de datos	Control de operaciones de Servidores, Equipos de Comunicaciones, Sistemas de Almacenamiento, Sistemas de Backups, Aire Acondicionado, Acometida Eléctrica	1	0.5

Fuente: Elaboración propia

El resultado del análisis RPO/RTO teniendo en cuenta que el primero indica el punto de recuperación objetivo que significa el rango de tolerancia que el CDA puede tener sobre la pérdida de datos y el evento de desastre, que esta en un promedio de 1,4 horas y el segundo que es el tiempo de recuperación objetivo que indica el tiempo disponible para recuperar sistemas el cual esta en un promedio de 0,5 horas.

6.4 DISEÑAR UN PLAN DE CONTINUIDAD BAJO ESTÁNDARES ISO/IEC 27031 QUE PERMITA LA RECUPERACIÓN DE UN INCIDENTE.

6.4.1 Formulación de la seguridad informática en la entidad. Consiste en la identificación de aquellos sistemas de información y/o recursos informáticos aplicados que son susceptibles de deterioro, violación o pérdida y que pueden ocasionar graves trastornos para el desenvolvimiento normal de la entidad, con el propósito de estructurar y ejecutar aquellos procedimientos y asignar responsabilidades que salvaguarden la información y permitan su recuperación garantizando la confidencialidad, integridad y disponibilidad de ésta en el menor tiempo posible y a unos costos razonables[33].

Teniendo como base la definición que una contingencia es una eventualidad y/o fatalidad, se determina como situación para la activación del Plan de Contingencia cuando hay una ausencia del sistema por más de media hora, este plan de continuidad se desarrolla inicialmente con la identificación de los procesos críticos de la empresa y con los que se deben ejecutar siempre , la responsabilidad de la ejecución del plan le corresponde a cada líder de proceso del área de TI y a los usuarios internos que tienen acceso al sistema y la información de la empresa, la vigencia de este plan está sujeto a cambios en el proceso tecnológico o de equipamiento relacionado con la empresa.

6.4.2 Alcance. El alcance del plan es la implementación de un análisis de riesgos basado en la metodología Magerit para el área de TI en el Centro de Diagnostico Automotor (CDA).

El CDA es una organización dedicada a dedicadas al examen técnico – mecánico y revisión de control ambiental de emisión de gases de los vehículos automotores (Motos, Automóviles, Servicio Público, Transporte de Carga) y se hace necesario establecer un plan de acción y evitar una falta de disponibilidad que ocasionan

[33] TAMAYO, Jhnny. plan de contingencia informático [En línea]. Colombia: Universidad Nacional de Colombia. Manizales. 2003. p. 5. Disponible en http://bdigital.unal.edu.co/57872/1/plandecontingenciasinformatico.pdf

inconformidad en los usuarios adicional de las altas pérdidas económicas que se obtienen por cada minuto que se deje de prestar el servicio.

6.4.3 Objetivos

- Restablecer en el menor tiempo posible las funciones definidas como críticas, con el fin de reducir el impacto de manera que la correcta recuperación de los sistemas y procesos quede garantizada y se conserven los objetivos del CDA
- Evaluar los procedimientos de contingencia requeridos cuando se presenta una interrupción de las operaciones, de forma que sólo se inviertan los recursos necesarios.
- Optimizar los esfuerzos y recursos necesarios para atender cualquier contingencia de manera oportuna y eficiente, definiendo las personas responsables de las actividades a desarrollar antes y durante la emergencia.
- Presentar recomendaciones que permitan disminuir la probabilidad de ocurrencia de una eventualidad e implementar las acciones preventivas resultantes de estas.
- Listar posibles fallas que se pueden presentar en el funcionamiento del hardware y el software que conforman la plataforma tecnológica.

6.4.4 Organización. Los deberes primarios de la implementación de la continuidad del negocio o de contingencia son:

a) Proteger los activos y a los empleados hasta que las operaciones se reanuden.
b) Hay que asegurar de que exista una capacidad para responder a un incidente.
c) Cuando se reestablezcan las operaciones se deben realizar pruebas y comunicar igualmente el fin de la contingencia.

6.4.5 Procesos y Servicios Por Proteger

- **Fallos en Servidor (software):**

a) Comunicar a todo el personal por teléfono, en caso de que este también se encuentre afectado, se debe comunicar de manera presencial.

b) Utilizar los formatos y/o manuales previamente establecidos en el listado maestro de documentos para continuar la operación manualmente mientras se recupera el sistema.

c) Cuando se reestablezcan las operaciones se deben realizar pruebas y comunicar igualmente el fin de la contingencia.

d) El personal encargado deberá alimentar el sistema de información reestablecido con la información que se llevó manualmente durante la contingencia.

e) Realizar auditoria para verificar que la información del sistema concuerde con lo que fue llevado a mano durante la duración de la contingencia.

- **Fallos en Servidor (Hardware):**

Puede producir Pérdida de Hardware y Software, perdida del proceso automático de backup e Interrupción de las operaciones. Las actividades para seguir en este caso serán:

a) Comunicar al personal el inconveniente presentado a través del sistema de mensajería institucional. En caso de que este también se encuentre afectado se debe hacer de manera presencial.

b) Utilizar los formatos y/o manuales previamente establecidos en el listado maestro de documentos para continuar la operación manualmente mientras se recupera el sistema.
c) Bajar el sistema y apagar el equipo.
d) Determinar el origen de la falla para estimar el tiempo estimado de desconexión
e) Si no se puede recuperar rápidamente el servidor afectado reemplazando la pieza dañada entonces se procederá a montar la última copia de seguridad que se tenga en otro de los servidores de la organización para restablecer el servicio, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
f) Realizar pruebas locales para verificar el correcto funcionamiento de la aplicación
g) Habilitar las entradas para los usuarios
h) Comunicar el fin de la contingencia
i) El personal encargado deberá alimentar el sistema de información restablecido con la información que se llevó manualmente durante la contingencia.
j) Realizar auditoria para verificar que la información del sistema concuerde con lo que fue llevado a mano durante la duración de la contingencia.

Recursos de Contingencia:

- Servidor de contingencia
- Componente de Remplazo (Memoria, Disco Duro, etc.).
- Backup diario de información del servidor

- **Perdida de servicio internet:**

a) Comunicar al personal el inconveniente presentado a través del sistema de mensajería institucional. En caso de que este también se encuentre afectado, se debe realizar de manera presencial.
b) Realizar pruebas para identificar posible problema dentro de la entidad

c) Si se evidencia problema en el hardware, se procederá a cambiar el componente.
d) Si no se evidencia falla en los equipos de la entidad, se procederá a comunicarse con la empresa prestadora del servicio, para asistencia.
e) Si el servicio no se puede restablecer rápidamente o el proveedor informa que la caída se extenderá por mucho tiempo entonces se procederá a configurar el servicio de internet alternativo de la entidad.
f) Es necesario registrar la avería para llevar un historial que servirá de guía para futuros daños.
g) Realizar pruebas de operatividad del servicio y comunicar su restablecimiento.

Recursos de Contingencia:

- Router
- Software
- Herramientas de Internet

- **Perdida del servicio de correo electrónico:**

Para restablecer los servicios de correo electrónico se deben seguir los siguientes pasos:

a) Comunicar al personal a través del sistema de mensajería institucional.
b) Se desconecta totalmente de la red el servidor de correo electrónico donde se encuentre alojado el servidor.
c) Realizar pruebas y verificar si se puede corregir el inconveniente
d) En caso de que no se pudiera corregir el inconveniente se procederá a restablecer las copias de configuración del servicio.
e) Reiniciar los servicios de correo y verificar que el servicio quede funcionando.
f) Comunicar el restablecimiento del servicio a todo el personal.

Recursos de Contingencia

- Manual de funciones actualizado del Administrador del sistema
- Relación de los sistemas de información de la organización
- Copia de la configuración del servidor de correo correctamente almacenada

- **Daño total o parcial en equipo de cómputo:**

En caso de daño total o parcial de algún equipo de cómputo se realizará lo siguiente:

a) Verificar el daño en sitio y verificar si se puede arreglar allí mismo o si es necesario trasladarlo al taller ubicado en la oficina de sistemas.
b) Informar al líder o encargado de la oficina que el Computador personal (pc) va a ser retirado del sitio (en caso de ser necesario).
c) En caso de que la falla sea muy grave y de la relevancia de las labores efectuadas en el pc averiado se procederá a pasar la información del disco duro del pc dañado a un pc temporal que será ubicado en el mismo lugar donde fue retirado el pc mientras se realiza el arreglo del pc averiado.
d) Cuando el pc sea reparado se volverá a realizar el intercambio de equipos pasando los archivos actualizados al pc reparado y luego borrándolos del pc temporal para tenerlo listo en caso de que se dañe algún pc en otra área.
e) Informar al líder y a los usuarios del pc que ya fue retornado el pc al sitio de trabajo.

6.4.6 Pruebas y mantenimiento. El plan de continuidad debe ser actualizado y revisado constantemente por el área de TI, garantizando que los fallos que se van presentando se tengan estructurados para resolver de manera mas eficiente en futuros daños similares, con el fin de que las operaciones básicas de la organización no se vean interrumpidas, se hace necesario contar con dos o más personas que tengan conocimiento en la administración de la red para garantizar en caso de falla se realice de manera rápida y eficiente el levantamiento de los servicios; así mismo se debe tener actualizados las licencias y pólizas de aseguramiento del hardware y software y hacer de conocimiento general el contenido del presente plan de continuidad del negocio, con la finalidad de instruir adecuadamente al personal del CDA.

Como parte del proceso de continuidad del negocio, la preparación de las TIC para la continuidad del negocio (IRBC), hace referencia a un sistema de gestión que complementa y suporta la continuidad del negocio de la organización y los programas de Sistemas de Gestión de Seguridad de la Información (SGSI), para mejorar la preparación de la Entidad que le permita:

a) Responder al cambiante ambiente de riesgos.

b) Asegurar la continuidad de las operaciones críticas del negocio soportadas por servicios de TIC.

c) Estar preparado para responder antes de que una disrupción de los servicios de TIC ocurra, identificar los eventos o la serie de eventos relacionados provenientes de incidentes.

d) Responder y recuperarse de incidentes y/o desastres y fallas.

Según la revisión documental de los procesos identificados que pueden generar interrupción de mayor a menor prioridad, se determinaron los procesos principales para lograr cumplir con los objetivos fijados, así mismo los puntos del proceso con el fin de obtener resultados favorables ya que son necesarios para el cumplimiento con éxito de los objetivos de manera eficiente y coherente.

7 CONCLUSIONES

Se logró identificar todos los activos del proceso de la dirección de tecnologías, utilizando la metodología de análisis de riesgos Magerit, posteriormente se realizó el reconocimiento y la clasificación de los activos, los cuales son importantes para la continuidad de las actividades de la empresa.

El análisis de riesgo permitió identificar las amenazas y vulnerabilidades a las cuales se encuentra expuesta la compañía, implementando un plan de despliegue para la prevención y recuperación de estas y finalmente realizar una valoración de los activos de mayor importancia estableciendo la criticidad y los riesgos a los que se encuentran expuestos con el fin de darles la prioridad para la implementación de un plan de continuidad.

Mediante el análisis de impacto BIA se consiguió identificar el impacto en la empresa ante la interrupción en la continuidad del negocio logrando una comprensión del funcionamiento integral del proceso, permitiendo establecer estrategias con las cuales se logra disminuir las probabilidades de que la empresa se encuentre en un estado de contingencia.

Se planteó un diseño de un plan de continuidad para el CDA bajo estándares ISO/IEC 27031, que permita la recuperación de un incidente, en este se describe una guía de cómo actuar rápidamente para restablecer los servicios en caso de que se presente una falla y como mantener las operaciones durante la misma sin que se afecten los activos de la información o los recursos tecnológicos de la empresa.

8 RECOMENDACIONES

El CDA no cuenta actualmente con lineamientos claros para afrontar fallas en diferentes áreas de la empresa, se requiere entonces que se implemente el plan de continuidad diseñado para el CDA, las siguientes recomendaciones, se exponen a la gerencia las cuales muestran las implicaciones positivas que puede traer para su operación:

- Definir personas responsables de las actividades antes, durante y después de la emergencia, estas personas serán también las encargadas de que el plan sea probado periódicamente para evaluar su eficacia.

- Establecer un reconocimiento para todos los activos de información de la empresa, es necesario para la protección de la información siempre conocer la fuente generadora hasta su uso final, de esta manera se lograra tener un mayor control.

- Trabajar en conjunto el área de T.I y recursos humanos, para concientizar a los empleados con el manejo de la seguridad informática, haciendo énfasis en los lideres de proceso como responsables, para que el personal que tienen a cargo acaten de manera más efectiva las medidas.

- Concientizar y enseñar a cada uno de los funcionarios del área TI del CDA sobre la importancia de diligenciar y actualizar los formatos diseñados en el plan de contingencia, con el fin de mantener documentada la información.

Estructurar y ejecutar un plan de continuidad del negocio, ya que es de vital importancia para estar preparados en caso de alguna falla a nivel técnica, física o ambiental.

BIBLIOGRAFÍA

BAENA PAZ, Guillermina María Eugenia. *Metodología de la investigación.* s.l. : Grupo Editorial Patria. ProQuest Ebook Central, 2014. págs. pp. 79-95.

BALDECCHI, R., & DE CALIDAD, G. C. *Implementación efectiva de un SGSI ISO 27001.* (2014).

BARATO, F. *impacto financiero en empresas constructoras de vivienda de interés social generadas por la no gestión del riesgo operativo.* Bogotá: s.n., (2013).

BORDA PÉREZ, M. *El proceso de investigación: visión general de su desarrollo.* Barranquilla: Universidad del Norte, 2013. págs. pp. 14-16, 80-89.

CAJAMARCA YUNGA, Jaime Santiago. Plan de recuperación de desastres de la Infraestructura de Tecnologías de Información, para empresas de prestación de servicios tecnológicos. 2019. Tesis de Maestría. Quito.

CARRIZO, Dante; ALFARO, A. y LOYOLA, Rodrigo. Propuesta de un modelo de plan de continuidad: Un estudio de caso. En Memorias de la Décima Quinta Conferencia Iberoamericana en Sistemas, Cibernética e Informática. 2016.

CORREA SALAZAR, Renzo Giancarlo. Diseño de un plan de continuidad para los servicios críticos del área de Tecnología de la Información de la empresa JJC Contratistas Generales S.A. basado principalmente en la norma ISO/IEC 27031:2011. Obtenido de 10.19083/tesis/625692. (2021)

CRESPO MARTÍNEZ, Esteban y CORDERO TORRES, Geovanna. Estudio comparativo entre las metodologías cramm y magerit para la gestión de riesgo de ti en las mpymes. UDA AKADEM, 2016, no 1, p. 38-47.

FERREYRO, A., & LONGHI, A. L. D. *Metodología de la investigación.* Córdoba: s.n., 2014. págs. pp. 15-34.

FORTALECIMIENTO DE LA GESTIÓN TI EN EL ESTADO (s. f.). Modelo de Seguridad -. Recuperado 27 de marzo de 2021, de https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/#5%20Gesti%C3%B3n%20Clasificaci%C3%B3n%20de%20Activos

GAONA VÁSQUEZ, Karina del Rocío. Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito SA en la ciudad de Machala. 2013. Tesis de Licenciatura.

GARCÍA MORA, Yury Andrea. Plan de Continuidad de Negocio frente a pandemia de COVID-19. 2020. Tesis Doctoral.

GARNICA CARRILLO, Víctor Manuel, et al. Plan de gestión mediante la guía del PMBOK para la planificación estratégica del sistema de gestión de la seguridad informática (SGSI) NTC ISO 27001: 2013 para la Clínica Medical Duarte.

GÓMEZ VIEITES, Á. *Seguridad informática, básico.* s.l. : Ecoe Ediciones. págs. Pp. 15 – 55 (2010).

GUERRA ERASO, José Daniel, et al. Software para el diagnóstico y evaluación de la seguridad de la información empresarial basado en la norma ISO/IEC 27001 de 2013. 2016

GUERRERA BRAVO Gema y MERA Evelyn. "evaluación y tratamiento del análisis de riesgos de la facultad de ciencias informáticas" (2018).

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. *tecnología de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información (sgsi) requisitos. ntc-iso 27001.* Bogotá D.C: Icontec, 2006. pág. p 37.

JOSEY, Andrew. *togaf® versión 9.1-guía de bolsillo.* s.l. : van haren, (1970).

LADINO, martha isabel, VILLA, paula andrea y LÓPEZ, ana maría. *fundamentos de iso 27001 y su aplicación en las empresas.* s.l. : scientia et technica, 2011. págs. p. 334-339. vol. vol. 17.

MINTIC, Guía para la preparación de las TIC para la continuidad del negocio, Ministerio de las Tecnologías de la Información y las Comunicaciones, Seguridad y privacidad de la información, Guía N° 10. (2010).

OLIVARI TAVERA, Juan Mauricio y RAMÍREZ COLL, Carlos Elías. Plan de continuidad del negocio. 2013. Tesis de Licenciatura. Universidad Piloto de Colombia.

PICO, Hugo Vecino. Normas ISO y marcos de referencia para gobernanza de las TIC, revisión.

PITTA PICÓN, Shirley Tatiana, et al. Diseño de un plan de contingencia informático basado en las normas ISO/IEC 22301 e ISO/IEC 27031 para la Ferretería Cesar SAS en la ciudad de Valledupar.

RODRÍGUEZ Z. JOSELYNE E. & SÁNCHEZ M. DIANA F. Plan de sensibilización, comunicación y capacitación para minimizar los riesgos informáticos en la facultad de ciencias informáticas. (tesis de pregrado). Universidad Laica Eloy Alfaro de Manabí, manta, Ecuador (2019).

SÁNCHEZ GUERRA, Lidia. Implementación de un Sistema de Gestión de Continuidad de Negocio alineado con la ISO 22301 y la ISO 27031. (2017).

TRUJILLO LÓPEZ, marcelo. *planeación estratégica de tecnologías informáticas y sistemas de información.* Manizales: universidad de caldas, (2007).

URIBE PUPIALES, Daniel David. Propuesta de un plan de continuidad de tecnologías de información para la Dirección de Tecnologías de Información y Comunicación del Ministerio del Deporte. 2018.

VILLA, Cayambe y PAUL, Oscar. Plan de seguridad informática aplicando la norma ISO 27001, para la protección de activos en la asociación CONFERIB. 2020.

ANEXOS

1. Matriz de valoración activos de información CDA.
https://1drv.ms/x/s!AlPAoo_Bc1uGgfls9evX7NjG9izkog?e=amMeTE

RESUMEN ANALÍTICO ESPECIALIZADO

Fecha de Realización:	22/10/2021
Programa:	Especialización en seguridad informática
Línea de Investigación:	Proyecto aplicado
Título:	Plan de continuidad del negocio referente a la gestión de la seguridad de la información para el proceso de la dirección de tecnologías e información de la empresa CDA basado en el estándar 27031
Autor(es):	Fabio Fernando Zuñiga Lopez
Palabras Claves:	Continuidad del negocio, estándar ISO/IEC 27000, Norma ISO 270031, BIA, Metodologías para la Gestión del Riesgo
Descripción:	La empresa CDA es una empresa industrial y comercial del estado EICE desarrollo del objeto social y para que el CDA continúe con los proyectos contenidos en los diferentes planes de acción, se requiere mantener una política de actualización y apropiación de tecnología de la información y telecomunicaciones que le permita ser cada vez más competitivo ofreciendo servicios de una manera óptima, ágil, segura y confiable, teniendo en cuenta esto el CDA requiere implementar diseñar, estructurar y llegar a implementar un plan de continuidad del negocio. Este proyecto está enfocado en presentarle la organización una propuesta de plan de continuidad del negocio, para que sea implementada inicialmente al área de TI., para esto es necesario establecer un plan de acción y así evitar una falta de disponibilidad que ocasione inconformidad en los usuarios y poner en tela de juicio la calidad del servicio, adicional a esto prevenir las pérdidas económicas por cada minuto que se deje de prestar el servicio, este plan está basado a través de la norma ISO/IEC 27031 que ofrece una guía para la preparación en la continuidad del negocio y recuperación de desastres, apoyado del estándar ISO/IEC 27001 que

	tiene un conjunto de estándares internacionales sobre la seguridad de la información
Fuentes bibliográficas destacadas: CRESPO-MARTÍNEZ, Esteban; CORDERO-TORRES, Geovanna. Estudio comparativo entre las metodologías CRAMM Y MAGERIT para la gestión de riesgo de ti en las MPYMES. UDA AKADEM, 2016, no 1, p. 38-47. MINTIC, Guía para la preparación de las TIC para la continuidad del negocio, Ministerio de las Tecnologías de la Información y las Comunicaciones, Seguridad y privacidad de la información, Guía N° 10. (2010). CORREA SALAZAR, RENZO GIANCARLO., Diseño de un plan de continuidad para los servicios críticos del área de Tecnología de la Información de la empresa JJC Contratistas Generales S.A. basado principalmente en la norma ISO/IEC 27031:2011. Obtenido de 10.19083/tesis/625692. (2021) GARCÍA MORA, Yury Andrea. Plan de Continuidad de Negocio frente a pandemia de COVID-19. 2020. Tesis Doctoral. INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. tecnología de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información (SGSI) requisitos. NTC-ISO 27001. Bogotá D.C: Icontec, 2006. pág. p 37.	
Contenido del documento:	Este informe se compone inicialmente de una definición del problema donde se presentan los antecedentes y la formulación del problema, seguido se presenta una justificación del porque se plantea esta propuesta, posterior a esto se plantean los objetivos tanto general como específicos, luego se pone en contexto de los temas que se abordaron a través del marco teórico y el marco conceptual y unos antecedentes donde también fue implementado un plan de continuidad , posteriormente se presenta el marco legal en el cual se sustenta este trabajo y su diseño metodológico, con esto se comienza el desarrollo de los objetivos planteados y por último se presentan las conclusiones obtenidas del desarrollo del trabajo y las recomendaciones a la empresa
Marco Metodológico:	Este proyecto aplicado se desarrolló bajo

	procesos de observación en cada área de la empresa y a partir de esto un análisis estadístico para manejar los datos cuantitativos y cualitativos de los activos de información, articulado a un enfoque experimental y descriptivo, alineado a la ISO/IEC 27031: 2011
Conceptos adquiridos:	Después del desarrollo del trabajo de grado se logró obtener los conceptos sobre la estructuración de un plan de continuidad del negocio basado a través de la norma ISO/IEC 27031 que ofrece una guía para la preparación en la continuidad del negocio y recuperación de desastres.
Conclusiones:	El plan de continuidad diseñado para el CDA describe una guía de cómo debe actuar la compañía rápidamente para restablecer los servicios en caso de que se presente una falla y como mantener las operaciones durante la misma sin que se afecten los activos de la información o los recursos tecnológicos de la empresa. Se logró identificar todos los activos del proceso de la dirección de tecnologías, utilizando la metodología de análisis de riesgos Magerit, posteriormente se realizó el reconocimiento y la clasificación de los activos, los cuales son importantes para la continuidad de las actividades de la empresa, el análisis de riesgo nos permitió identificar las amenazas a las cuales se encuentra expuesta la compañía, implementando un plan de despliegue para la prevención y recuperación de estas y finalmente realizar una valoración de los activos de mayor importancia estableciendo la criticidad y los riesgos a los que se encuentran expuestos con el fin de darles la prioridad para la implementación de un plan de continuidad. Se logro una comprensión del funcionamiento integral del proceso, permitiendo establecer estrategias con las cuales se logra disminuir las probabilidades de que la empresa se encuentre en un estado de contingencia.