DISEÑO DE UN PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LAS NORMAS ISO/IEC 22301 E ISO/IEC 27031 PARA LA FERRETERÍA CESAR S.A.S EN LA CIUDAD DE VALLEDUPAR

SHIRLEY TATIANA PITTA PICÓN

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD VALLEDUPAR
2018

DISEÑO DE UN PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LAS NORMAS ISO/IEC 22301 E ISO / IEC 27031 PARA LA FERRETERÍA CESAR S.A.S EN LA CIUDAD DE VALLEDUPAR

SHIRLEY TATIANA PITTA PICÓN

Propuesta de grado para optar por el título de Especialista en Seguridad Informática

Director
Ing. JULIO ALBERTO VARGAS FERNÁNDEZ

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD VALLEDUPAR
2018

Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Abierta y a Distancia UNAD, para optar al título de Especialista en Seguridad Informática

_____

Firma del jurado

_____

Firma del jurado

Valledupar, junio de 2018

DEDICACIÓN

Dedico este proyecto a Dios por permitir alcanzar esta meta. A mis padres y hermanos por su ayuda incondicional. A mi esposo e hija por el tiempo valioso que deje de compartir con ellos.

SHIRLEY PITTA.

AGRADECIMIENTOS

Agradezco a todos los tutores y asesores de la UNAD que aportaron tiempo y apoyo en la culminación de este proyecto.

A todos los empleados de la Ferretería Cesar y en especial al gerente Germán Tapias por toda la disposición y apoyo en el diseño e implementación de este proyecto. Y a los ingenieros Cesar Acosta y Amilkar Sierra por su tiempo y colaboración.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

La Ferretería Cesar es una mediana empresa ubicada en la ciudad de Valledupar, líder en la comercialización de materiales para la construcción cuya actividad económica principal está soportada sobre una infraestructura tecnológica. La alta dirección es consciente de que están expuestos a algunos riesgos inherentes al uso de las tecnologías de la información y comunicaciones en sus procesos comerciales, por esto están interesados en implementar estrategias preventivas que aseguren la disponibilidad y confidencialidad de sus activos de información, y además contar con los procedimientos de recuperación que permitan la continuidad de las tareas críticas de la empresa.

Se propone diseñar un plan de contingencia informático que permita identificar los riesgos a los que están expuestos y establecer estrategias basados en las normas internacionales ISO 22301 y 27031, las cuales proveen las técnicas y directrices para establecer sistemas de gestión de continuidad de negocio y recuperación de los servicios de TIC. Al finalizar el proyecto la empresa contará con un plan que contenga el análisis y la gestión de riesgos de la situación actual de la empresa, la definición de los procedimientos para la recuperación en caso de incidentes, los roles y responsabilidades del recurso humano de la empresa y una guía para el mantenimiento y pruebas del plan de contingencia.

INTRODUCCIÓN

En la actualidad, las tecnologías de la información (TI) se han convertido en herramientas fundamentales para el desarrollo de las de todas las empresas sin importar su tamaño y actividad económica. El uso de ellas ha permitido agilizar procesos, ampliar mercados, obtener nuevos clientes; incluso en muchos casos existe tanta dependencia que si éstas no estuvieran disponibles sus procesos de negocio fracasarían y tendrían pérdidas económicas muy grandes. En las TI también se incluyen los recursos para el almacenamiento de información sensible e importante para las empresas, en las que se requiere un alto grado de confidencialidad e integridad.

Dada la importancia de las tecnologías de la información para procesos fundamentales de las empresas se requiere implementar estrategias que aseguren su disponibilidad, confidencialidad e integridad ante los riesgos inherentes a su uso, por ejemplo, la pérdida de la información, alteración de datos, interrupción de los servicios informáticos, entre otros, que pueden afectar considerablemente la reputación de la empresa y/o generar pérdidas económicas significativas.

La Ferretería Cesar es una empresa cuya actividad económica principal está soportada sobre una infraestructura tecnológica que debe asegurar y proteger. Además de implementar estrategias que ayuden a recuperarse en caso de una eventualidad que afecte la continuidad de sus operaciones, de allí su interés por implementar un plan de contingencia informático que provea las estrategias preventivas y de recuperación que aseguren la continuidad de las tareas críticas de la empresa.

1. TITULO

DISEÑO DE UN PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LAS NORMAS ISO/IEC 22301 E ISO/IEC 27031: 2011 PARA LA FERRETERÍA CESAR S.A.S EN LA CIUDAD DE VALLEDUPAR

2. PLANTEAMIENTO DEL PROBLEMA

La Ferretería Cesar es una empresa comercializadora de materiales para la construcción, abrió sus puertas hace 53 años en la ciudad de Valledupar, su amplia experiencia y buen servicio ha permitido que hoy sea una de las empresas líderes en el sector a nivel local y regional. Todo el proceso comercial de esta empresa está soportado sobre una infraestructura tecnológica, que desde su implementación le ha permitido ampliar su mercado, prestar un servicio más oportuno y ágil, controlar el inventario, evitar errores de cálculos durante el proceso de venta; además de proveer el espacio para almacenar la información sensible de la empresa como las listas de proveedores y clientes, cuentas por cobrar, cuentas por pagar e información contable. Sin embargo, el uso de esta infraestructura tecnológica ha generado una amplia dependencia entre ella y la actividad principal del negocio, una falla técnica o la parálisis de las operaciones normales de los servicios tecnológicos y de información, pueden llegar a impactar negativamente a los ingresos y reputación de la empresa.

Durante su operación diaria la empresa ha tenido que enfrentarse a fallas tecnológicas como por ejemplo el daño en el disco duro del servidor de aplicaciones, que generó una parálisis de más de cuatro horas y pérdida de la información de la actividad comercial de diez días. En otra ocasión, la propagación de un virus informático que dañó los ejecutables de acceso al programa de inventario y facturación, dejando así sin servicio a la empresa por más de dos horas. En estos casos la empresa ha tenido pérdidas económicas significativas, ya que por la falta del servicio tecnológico no se pueden realizar las ventas causando además la insatisfacción en los clientes, afectando la imagen y la calidad del servicio.

Por lo tanto, es importante que la empresa defina acciones y procedimientos a seguir en caso de fallos en los recursos tecnológicos e implementar medidas preventivas que conlleven a que los servicios tecnológicos estén siempre disponibles, confiables y solo sean accedidos por personas autorizadas. Por consiguiente, se propone el diseño de un plan de contingencia informático que contribuya a la empresa a recuperarse rápidamente ante fallos parciales o totales en los servicios tecnológicos y de información, restaurándolos servicios y aplicaciones que soportan las actividades criticas de negocio.

2.1 FORMULACIÓN DEL PROBLEMA

¿Cómo un plan de contingencia informático para la Ferretería Cesar ubicada en la ciudad de Valledupar, permitirá restaurar los servicios informáticos en caso de una eventualidad, y garantizar la continuidad de las actividades críticas de negocio?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Asegurar la continuidad de los servicios de la Ferretería Cesar frente a la posible ocurrencia de un incidente de seguridad que comprometa total o parcialmente la prestación de los servicios informáticos, mediante el diseño de un plan de contingencia informático.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los riesgos que pueden afectar el normal funcionamiento de los procesos informáticos de la empresa con el fin de hacer una valoración de los mismos, utilizando la metodología Magerit.

- Establecer las estrategias preventivas que permitan disminuir la probabilidad de ocurrencia de un estado de contingencia.

- Diseñar los procedimientos de recuperación que pueden asegurar la continuidad de los servicios informáticos en caso de una interrupción, alineados con el estándar ISO / IEC 27031: 2011 e ISO/IEC 22301:2012.

- Sensibilizar al personal para promover el buen uso y manejo del plan de contingencia informático, a través de una capacitación.

- Elaborar un plan de contingencias que asegure la continuidad de las tareas críticas, acorde a la infraestructura y necesidades de la empresa alineado al estándar ISO / IEC 27031: 2011 e ISO/IEC 22301:2012.

4. JUSTIFICACIÓN

La Ferretería Cesar siendo una empresa de reconocida trayectoria comercial en el ámbito local y regional, que cuenta con una infraestructura tecnológica para controlar todos los procesos que soportan su actividad económica principal, esta imperiosamente abocada a diseñar un plan de contingencia informático que permita identificar los riegos y contar con un procedimiento estructurado para asegurar la continuidad de los servicios informáticos en caso de una eventualidad que afecte su infraestructura tecnológica instalada.

Con la implementación de un plan de contingencia se podrán identificar y mitigar los riesgos a los que está expuesta la empresa, y se contará con las actividades planificadas de recuperación que permitan superar eficazmente cualquier crisis ocasionada por un incidente informático. Por consiguiente, se contará con acciones encaminadas a disminuir el nivel de improvisación, fortaleciendo la capacidad operativa y de respuesta e impidiendo que pequeñas situaciones terminen por convertirse en problemas mayores que impacten la estabilidad de la empresa.

Por todo lo anterior, se evidencia la importancia y beneficios que obtendría la Ferretería Cesar con el diseño de un plan de contingencia informático, que se constituiría como una inversión que generará un aumento en la satisfacción de los clientes por la calidad de los servicios prestados, de los empleados por contar con procedimientos documentados que le permitan reaccionar eficazmente ante eventos adversos y de los directivos que tendrán la confianza que las actividades críticas de la empresa están respaldadas por un plan de contingencia acorde a sus necesidades.

4.1 ALCANCE Y DELIMITACIÓN DEL PROYECTO

El presente proyecto se desarrollará en las instalaciones de la FERRETERÍA CESAR, ubicada en el municipio de Valledupar – Colombia. El desarrollo de las actividades se llevará a cabo durante el segundo semestre del año2017.

El alcance del diseño del Plan de Contingencia abarcará los elementos de infraestructura tecnológica, sistemas de información, personal y servicios, involucrados en los procesos críticos para la continuidad del negocio de la Ferretería Cesar. En el desarrollo del mismo se realizará el análisis de riesgos, procedimientos encaminados a la minimización de riesgos, la gestión para la reanudación rápida y eficiente de los servicios informáticos en caso de alguna eventualidad y la capacitación del personal.

5. MARCO DE REFERENCIA

5.1 ANTECEDENTES

En Bogotá – Colombia en el año 2007 en la Universidad de la Salle se elaboró tesis titulada “Plan de Contingencia para el Archivo de la Universidad de la Salle como parte de la Implantación del Sistema Integrado de Conservación”. Elaborada por Diana León López El trabajo de grado está dirigido a los profesionales de Sistemas de Información y en general a los responsables de archivos y bibliotecas, con el fin de que consideren la importancia de Un Plan de Contingencia en una determinada Unidad de Información y de esta manera estar preparados y capacitados a la hora en que se presente una emergencia reduciendo radicalmente sus efectos y consecuencias[1]

En Cuenca - Ecuador para el año 2011 en la Universidad de Cuenca se desarrolló tesis titulada “Diseño de un plan de contingencias de Tics para la empresa eléctrica CENTRO SUR”. Elaborada por Andrea Granda. Donde se utilizó la metodología Magerit que proporciona una guía para la identificación de los activos, amenazas y salvaguardas o controles de seguridad, que impacten a la continuidad del negocio, en conjunto con los controles de seguridad de la norma ISO 27001[2].

En Bogotá – Colombia en el año 2012 en la Universidad EAN se elaboró tesis titulada “Propuesta de mejoramiento y contingencia de sistemas informáticos en la empresa ‘T’”. El trabajo de grado presenta el desarrollo de un proceso de consultoría en una compañía de su interés, que llamarón “T”, detectan las problemáticas de TI y generan las estrategias orientadas a promover la mejora del área y de los servicios informáticos para beneficio de la organización; los resultados obtenidos son representados en una propuesta de mejoramiento y un plan de contingencia de TIbasada en guías de buenas prácticas de TI y en su propia experiencia. Tesis elaborada por Maritza Yohana Ramírez Robayo, Edwin Alberto Londoño Rúa, Jairo Andrés Gómez Gómez, para optar título de Especialistas en Gerencia Informática[3]

En la ciudad de Valledupar - Colombia para el año 2013 en la Universidad Popular del Cesar, se elaboró tesis de grado titulada:“Diseño de un plan de contingencia y

[1]LEÓN LÓPEZ, Diana Rocío. Plan de Contingencia para el archivo de la Universidad de la Salle como parte de la implantación del sistema integrado de Conservación. Trabajo de grado profesional en Sistemas de Información, bibliotecología y archivística. Bogotá, Colombia. Universidad La Salle. Facultad de sistemas de Información y Documentación. 2007. 186p.

[2]GRANDA, Andrea. Diseño de un plan de contingencias de Tics para la empresa eléctrica CENTROSUR. Trabajo de grado maestría en gerencia de sistemas de información. Cuenca, Ecuador. Universidad de Cuenca. Facultad de Ingeniería. 2011. 237p.

[3]RAMÍREZ ROBAYO, Maritza Yohana, LONDOÑO RÚA, Edwin Alberto y GÓMEZ GÓMEZ, Jairo Andrés. Propuesta de Mejoramiento y Contingencia de Sistemas Informáticos en la Empresa “T”. Trabajo de Grado. Especialización en Gerencia Informática. Bogotá, Colombia. Universidad EAN. Facultad de ingeniería. 2012. 165p.

recuperación ante desastres en el centro de cómputo de la Universidad Popular del Cesar", esta tesis buscaba aportar a La Universidad Popular del Cesar un instrumento a través del cual pudiera mejorar la seguridad informática física y lógica, además; aportó una guía para que la institución tuviera pautas sobre qué debe hacer y cómo debe actuar frente a una ocurrencia de un desastre y poder reanudar sus actividades laborales luego de la misma. Fue elaborada por Cindy Guzmán Trujillo y Zaidy Pacheco Palmiery para optar título de Ingenieras de Sistemas[4].

Todas estas tesis ayudan a comprender la metodología a utilizar, métodos de recolección de información, metas que se deben cumplir, normas internacionales de buenas prácticas que se deben considerar para los planes de contingencias, tiempo estimado que se empleará en cada fase del desarrollo del plan de contingencia, entre otros aportes de vital importancia en el desarrollo de este proyecto.

5.2 MARCO CONTEXTUAL

5.2.1 Reseña Histórica de La Ferretería Cesar. En abril de 1968, Daniel Tapias Pico sostenía a su familia de su actividad como taxista en San Gil – Colombia. La familia comenzó a pasar por una dificultad económica y uno de sus hijos de nombre Mauro Antonio le da la idea de vender el taxi y trasladarse a Valledupar, ciudad que fue designada como capital del naciente Departamento del Cesaren 1967. Es así como esta familia santandereana se traslada a Valledupar y con la venta del taxi abren un negocio de ferretería al cual llamaron La FERRETERÍA CESAR, ubicada en un sector conocido como "El Boliche", rodeado de cantinas y bares. Inician actividades en el año de 1968, como persona natural cuyo objeto social era la compra venta y distribución de materiales para la construcción y artículos de ferretería en general; con un capital social de $11.000.000 de pesos, y con un mínimo número de empleados.

Diez años más tarde (1978), se trasladó a la primera etapa de la construcción de su propiedad, situada en la Calle 20 No. 11-06 del Barrio La Graja, hoy en día sector totalmente comercial, con énfasis en Ferreterías y Almacenes de Materiales de Construcción.

El 14 de mayo de 1982, por escritura pública No 138 otorgada en la notaria única de Codazzi Cesar, inscrita en la Cámara de Comercio de Valledupar, el 23 de noviembre de 1982, bajo el No 1620, del libro IX, se constituyó la sociedad comercial denominada FERRETERÍA CESAR LIMITADA; cuyo objeto social es la

[4] GUZMÁN, Cindy y PACHECO, Zaidy. Diseño de un plan de contingencia y recuperación ante desastres en el centro de cómputo de la Universidad Popular del Cesar. Trabajo de Grado (Ingeniero de Sistemas).Valledupar, Colombia. Universidad Popular del Cesar. Facultad de ingeniería.2013. 186p.

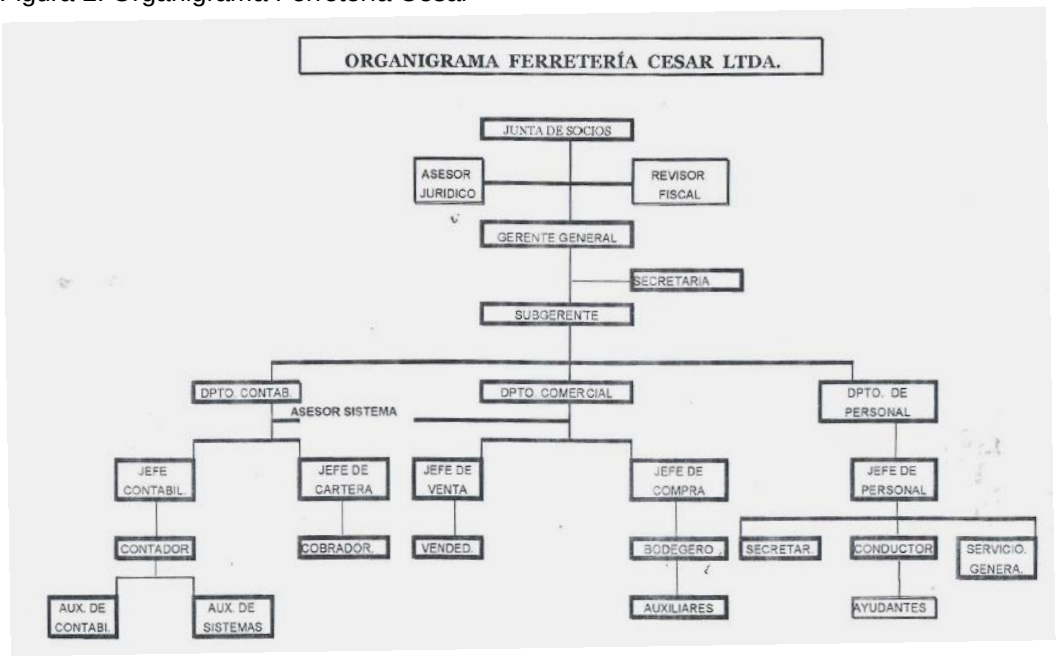
compraventa de bienes raíces urbanos y rurales, semovientes, compra venta de vehículos, celebrar actos y contratos de comercio lícito, venta de materiales de construcción. El capital social: ciento cuarenta y un millones novecientos mil pesos M/cte., ($141.900.000) representado en catorce mil cientos noventa (14.190) cuotas de un valor nominal de diez mil pesos ($10.000).

Cuando celebraron los primeros 20 años de existencia, Ferretería Cesar hizo entrega a la comunidad del Barrio Villa Miriam una Escuela para educación primaria, que hoy en día atiende a 1.200 niños, en dos jornadas y sólo pidió a cambio que le permitieran llevar el nombre de “Concentración Escolar Daniel Tapias Pico”, en memoria del fundador de La Ferretería Cesar, quien falleció de un infarto el 17 de octubre de 1982.
Ferretería Cesar cuenta en la actualidad con unas modernas instalaciones en un área aproximada de 4.000 metros, divididos en un edificio de tres (3) plantas (ver Figura 1) y tres (3) bodegas externas. Es una de las empresas líderes en el sector, con un portafolio de aproximadamente 11.000 ítems, siendo distribuidores mayoristas del 90% de este portafolio, cubriendo los departamentos del Cesar, Guajira y Magdalena.

Figura 1. Instalaciones Ferretería Cesar

Fuente: Ferretería Cesar

Figura 2. Organigrama Ferretería Cesar



Fuente: Ferretería Cesar

5.2.1.1 Actividad económica. La actividad económica principal de la Ferretería Cesar es la compra y venta de materiales para la construcción y ferretería en general.

5.2.1.2 Descripción general de los activos informáticos. La Ferretería Cesar cuenta con dos servidores en uno de ellos se encuentra el Sistema de Inventario, Facturación y Compras “ZAFIRO”, el sistema de contabilidad y nomina llamado “HELISA”, el sistema de inventario y facturación “SIFFOX” que utilizaron desde el año 2007 al 2016. En un segundo servidor se encuentra el sistema de inventario y facturación “Sifec” que utilizaron hasta el año 2006 y el sistema de contabilidad “LINKER” que utilizaron hasta el año 2008.

Cuentan con 19 computadores y 5 portátiles, ubicados en las diferentes oficinas de la empresa, están interconectados por una red LAN que permite el acceso a Internet y a los servidores de aplicaciones. Además, tienen una red inalámbrica que brinda acceso a internet a los equipos móviles de sus clientes. Tienen contratado un servicio de hosting donde está alojada la página Web y un servicio de correo de cuentas corporativas.

5.3 MARCO TEÓRICO

5.3.1 Planes de contingencia informático. Un plan de contingencia informático es un conjunto de estrategias preventivas, estrategias de recuperación y procedimientos que buscan prevenir incidentes informáticos y/o restaurar de una forma ordenada, ágil la infraestructura tecnológica que soporta los procesos críticos de negocio de una organización en caso de una contingencia.

El desarrollo de un plan de contingencia informático lo componen varias fases: análisis de riesgos, identificación de estrategias preventivas y de recuperación, documentación del plan de contingencia, realización de pruebas, implementación y mejoramiento.

Durante la fase de análisis de riesgo se identifican las vulnerabilidades y los riesgos a los que está expuesto la organización en estudio, esto dará el escenario para el establecimiento de estrategias preventivas y de recuperación. Una vez que se han establecido las estrategias acordes al presupuesto y la infraestructura de la organización se procede a la documentación del plan de contingencia.

Las pruebas del plan de contingencia buscan mejorar el plan y se realiza cuando se diseña el plan para medir la efectividad del plan planteado, y luego de implementarse cada cierto tiempo para la mejora continua del mismo. La realización de las pruebas del plan de contingencia se puede realizar en forma de escritorio, que consiste en crear un escenario hipotético y a través de preguntas describir las acciones que se llevarían a cabo. Otra manera es realizar una prueba controlada, la cual consiste en crear una contingencia controlada y que le personal realice las actividades del plan hasta superar la contingencia.

La fase de implementación y mejoramiento del plan de contingencia consiste en la capacitación continua al personal, el análisis de las pruebas realizadas al plan de contingencias que darán como resultado recomendaciones que lleven a la mejora continua del plan.

5.3.2 Estándar ISO / IEC 27031: 2011. Este estándar agrupa las técnicas y directrices a seguir para que una organización pueda recuperar sus servicios de TIC ante un incidente y soportar sus operaciones de negocio de forma planificada. Además, proporciona un marco de métodos para generar capacidad de prevenir incidentes, es decir proteger a las TIC de cualquier amenaza sea física, ambiental, humana. Detectar incidentes oportunamente, para tomar medidas y así minimizar el impacto que puede causar una amenaza, responder de la mejor manera ante un incidente, implementar estrategias que le permitan recuperarse de manera oportuna y elementos para que se encuentre en un continuo mejoramiento.

La preparación TIC para la Continuidad del Negocio (IRBC, por sus siglas en inglés *Readiness for Business Continuity*), consta de las fases de planificación, implementación y operación, seguimiento y revisión, y mejoramiento[5].

5.3.2.1 Fase de planificación. Durante esta fase se deben designar las personas que se harán responsables por implementar y mantener el IRBC y personas competentes para ejecutar tareas que se le sean asignadas dentro del IRBC.

Luego, se deberá determinar el número de servicios TIC, documentar e identificar cuáles de ellos son los servicios críticos. Una vez identificados se deben revisar las capacidades actuales de continuidad valorando los riesgos de interrupción del servicio y planteando alternativas que mejoren la capacidad de recuperación del servicio TIC. Una vez finalizado este análisis de riesgo se deberá identificar la brecha entre las capacidades del IRBC y los requisitos de continuidad del negocio. Plantear las estrategias del IRBC enfocado a la prevención de incidentes, detección respuesta recuperación y restauración de los servicios TIC, estas estrategias deben ser aterrizadas de acuerdo al prepuesto de la organización, disponibilidad de recursos, costo-beneficio, obligaciones regulatorias. Se deben planear estrategias enfocadas a la disponibilidad de las instalaciones, la reanudación de los servicios tecnológicos dentro de los objetivos de los tiempos de respuesta, asegurar la confidencialidad, la integridad y la disponibilidad de los datos, los procesos necesarios para asegurar la viabilidad de las estrategias y las estrategias orientadas a todos los servicios tecnológicos que sean soportado por los proveedores externos.

Una vez se han planteado las estrategias del IRBC se deben formalizar ante la alta dirección, para que en común acuerdo se seleccionen las estrategias IRBC, luego se aprueben y formalicen garantizando que las opciones se han entendido y soportan los requisitos generales de la continuidad del negocio.

Finalmente se debe planificar las capacidades de mejoramiento del IRBC y los criterios de desempeño IRBC.

5.3.2.2 Fase de implementación y operación. Esta fase no se puede llevar a cabo sin la aprobación y formalización de las estrategias planteadas para el IRBC, ya que estas son las bases para poner en marcha la implementación y operación del IRBC. Esta fase se puede dividir en 5 actividades que son:

[5] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Directrices para la preparación de la tecnología de la información y las comunicaciones para la continuidad de negocio. NTC-ISO27031:2011. Bogotá D.C: El Instituto, 2016. 42 p.

La primera actividad es realizar un proceso de concientización con el personal, indicando que ellos son pieza fundamental para la alcanzar los objetivos del IRBC.

La alta dirección deberá mantener una educación continua en este aspecto, además de asegurar que las personas que se le asignaron responsabilidades dentro del IRBC sean competentes. Luego, se debe implementar las estrategias diseñadas para la infraestructura, tecnología y datos, también documentar claramente los procesos del IRBC garantizando que el personal competente es capaz de comprenderlo y ejecutarlo. Además de asegurar que los proveedores críticos tienen la capacidad de soportar los servicios del IRBC.

La segunda actividad consiste en establecer respuesta a cada incidente TIC con una acción apropiada dentro del IRBC. Esto con la finalidad que se pueda tomar el control en un incidente.

La tercera actividad determinar el contenido del plan. Para realizar una buena documentación el estándar establece que el plan debe contener los siguientes elementos:

- El propósito y alcance: debe ser claro y conciso, decir si se deben referenciar otros planes dentro de la organización y como acceder a ellos, además de establecer objetivos sobre qué servicios críticos se va a recuperar y la escala estimada de tiempo en que se recuperarán. También se deberían incorporar listas de chequeos de incidentes para una posterior revisión.

- Roles y responsabilidades: se debe documentar los roles y las responsabilidades de las personas que toman decisiones dentro del plan.

- Invocación del plan: se debe documentar claramente en que situaciones se invoca el plan de respuesta y recuperación de TIC e incluir una descripción clara de por ejemplo los puntos de encuentro, como movilizar los equipos y/o individuos asignados. Como también en que circunstancia no es necesario una respuesta IRBC sino más bien manejada por el personal de soporte.

- Dueño y Responsable del mantenimiento y documentación del plan de respuesta y recuperación de TIC: La alta dirección debe asignar una persona que se hará responsable las actividades de revisión, actualización del plan. En caso que el plan sea actualizado, se debe emplear un sistema de control de versiones y de notificaciones sobre los cambios realizados en el plan a todo el personal.

- Detalles de contactos: es apropiado contener el registro de contacto de todas las personas y/o entidades que sean pieza clave dentro del plan.

Al redactar la documentación del plan de respuesta y recuperación TIC se debe tener en cuenta que debe ser una redacción sencilla que cualquier persona pueda entender, debe ser flexible y lo más importante proporcionar las bases para manejar los aspectos graves que considere la organización referente a las TIC. Documentar la estrategia, el servicio crítico, la línea de tiempo de recuperación, los equipos de recuperación y las responsabilidades. También, deben incluir:

- Objetivos del plan

- Alcance: en este se debe definir la criticidad de los servicios, un resumen de la tecnología que soporta los servicios críticos, un resumen de los departamentos y/o personas que gestiona dicha tecnología y un resumen de la documentación fundamenta para la tecnología.

- Requisitos de disponibilidad de servicios y tecnología.

- Requisitos de seguridad de la información incluyendo los requisitos para su confidencialidad, integridad y disponibilidad.

- Procedimientos de recuperación de la tecnología, es decir una descripción del procedimiento y actividades a seguir para restaurar los servicios TIC.

- Apéndice, debe incluir el inventario de los sistemas de información, aplicaciones, base de datos, acuerdos a nivel de servicios y contratos.

- Proveedores TIC.

La cuarta actividad es la concientización, competencia y programa de pruebas, es decir establecer un programa para asegurar que regularmente se promueve la concientización del IRBC, se evalúa y se mejora.

La quinta y última actividad de esta fase es el control de la documentación del IRBC, es decir establecer controles para proveer su almacenamiento, revisiones, actualizaciones, control de cambio y de versión, control de aprobación y distribución.

5.3.2.3 Fase de seguimiento y revisión. Durante esta fase se planifica el mantenimiento del IRBC, la auditoría interna del IRBC, la revisión por parte de la dirección y la medición de los criterios de desempeño.

Respecto al mantenimiento del IRBC, la idea es establecer un proceso para el seguimiento, detección y análisis de nuevas amenazas que afecten la seguridad

de las TIC, diseñar un programa de pruebas ejercicios que permitan medir si las estrategias acordadas pueden minimizar el impacto al negocio y si los procedimientos son válidos para retornar al negocio a la normalidad. El programa de pruebas debe definir la frecuencia, alcance y formato de cada ejercicio por ejemplo la recuperación de la base de datos; lo que se busca es demostrar que las estrategias cumplen con los requisitos de negocio, que los servicios críticos se pueden mantener y recuperar dentro de los objetivos que se acordaron para la recuperación, además permite que el personal se familiarice con los procedimientos de recuperación y así asegurar que tiene un conocimiento adecuado de los planes y procedimientos a seguir dentro del IRBC. Cuando se vaya a realizar un ejercicio de prueba, este deberá planificarse asegurando que se cuentan con datos de respaldos, realizarse en horarios no hábiles, elaborar actas del ejercicio, interrogar a los participantes para recolectar información y una posterior retroalimentación. Al finalizar el ejercicio se debe analizar los resultados y hallazgos frente a los objetivos del ejercicio.

Para el plan de auditoría interna del IRBC se debe definir la frecuencia en que se va a realizar dicha auditoria. El personal que sea asignado para realizarla debe tener un amplio conocimiento acerca del plan y en el caso que la auditoría interna identifique falencia deberá reportar los resultados a los directores para la toma de acciones correctivas.

En cuanto a la revisión por parte de la dirección debe realizarse de forma anual, lo que se busca es que se tenga en cuenta las revisiones de las auditorías internas y las autoevaluaciones y valorar mejoras y/o cambios a la gestión del IRBC. Estas revisiones deben registrarse para un mejor control de los resultados de cada revisión.

Para finalizar esta fase se deben definir unos criterios de desempeño cuantitativo y cualitativo sobre la preparación de las TIC para hacer seguimiento y medir la preparación de TIC de la organización. Como método de recolección se pueden realizar encuestas, talleres de retroalimentación y/o reuniones

5.3.2.4 Fase de mejoramiento. Durante esta fase la organización debe tomar acciones correctivas sobre cualquier falla encontrada ya sea en los servicios de TIC y/o en los elementos del IRBC. Una vez que se identifique la falla deberá ser documentada determinando cuales fueron las causas de la falla y determinar las acciones correctivas a tomar. Además, la organización también puede llevar a cabo acciones preventivas una vez que ha identificado una potencial falla, estas también deben ser documentadas para llevar un registro y control de las acciones tomadas que contribuyen al mejoramiento del IRBC.

5.3.3 Estándar ISO/IEC 22301:2012. Este estándar define los requisitos para diseñar un sistema de gestión de continuidad de negocio (BCMS) apropiado a las necesidades de la organización, es aplicable a cualquier organización sin importar su tamaño y/o actividad. Se basa en el modelo planear – hacer – verificar – actuar (PHVA) con la finalidad de diseñarlo, implementarlo, revisarlo y mejorarlo. [6]

Para la implementación de este estándar primero hay que colocar en contexto a la organización, es decir, identificar y documentar los procesos de la organización y el impacto relacionado con un incidente perjudicial, definir los factores que dan lugar al riesgo, definir el propósito y el alcance del BCMS. Es importante que la alta gerencia se encuentre comprometida con el BCMS ya que es uno de los actores principales para establecer las políticas de continuidad de negocio, designar a las personas responsables para la implementación y mantenimiento del BCMS, además de establecer y comunicar las políticas de continuidad de negocio, velando porque estas últimas sean adecuadas para la organización y que estén siempre disponible, ampliamente comunicadas y revisadas dentro de la organización.

Una vez se ha colocado en contexto a la organización se procede a planificar el BCMS, durante esta actividad se establecen las acciones para direccionar el riesgo y se establecen los objetivos de continuidad de negocio y cuáles son los planes para alcanzar dichos objetivos, determinar que competencias deben cumplir el personal responsable del BCMS, determinar la necesidad de comunicar interna y externamente sobre el BCMS. Respecto a la comunicación se debe ser claro sobre qué, cuándo y a quienes comunicarse. También, se debe crear la información documentada requerida asegurando que tenga una identificación y descripción, es decir el título, fecha de elaboración y/o actualización, personas que intervinieron, etc. Esta información documentada deberá estar siempre disponible para su uso y en constante revisión para garantizar que sea apropiada, deberá tener un control de cambios o de versiones y debe estar adecuadamente protegida por la organización.

El BCMS debe incluir un proceso formal y documentado para el análisis del impacto de negocio y de valoración del riesgo. El análisis de impacto del negocio debe identificar las actividades que apoyan la prestación de bienes y servicios evaluando el impacto vs el tiempo de no realizar estas actividades; como resultado de esta evaluación se debe establecer los plazos prioritarios para la reanudación de las actividades a un mínimo especifico aceptable. La valoración del riesgo debe identificar los riesgos para que posteriormente sea analizado y evaluado, identificando los tratamientos acordes a los objetivos de continuidad de negocio. Luego, se debe determinar y seleccionar las estrategias apropiadas para proteger las actividades prioritarias, como las estrategias que permitan estabilizar, reanudar

[6] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistemas de gestión de continuidad de negocio. NTC-ISO22301:2012. Bogotá D.C: El Instituto, 2012. 28p

y recuperar dichas actividades priorizadas en una contingencia, además de las estrategias que permitan mitigar y/o responder a los impactos. Todas estas estrategias deben incluir un tiempo de prioridad para la reanudación de actividades y los recursos que se requieren por ejemplo humano, hardware, software, sitios, etc. También se deben listar estrategias para la protección y mitigación del riesgo, que permitan reducir la probabilidad de interrupción de las actividades de negocio y otras que acorten el tiempo de interrupción o limiten el impacto de la interrupción. Además, se deberá estructurar las repuestas a los incidentes estableciendo los procedimientos para manejarlos y los medios de comunicación a las partes interesadas y los procedimientos de recuperación.

La organización debe realizar ejercicios y pruebas de los procedimientos de continuidad de negocio, evaluando su desempeño. Además, debe realizar auditorías internas con la finalidad de proporcionar información si el BCMS está eficazmente implementado, si cumple con los requisitos de la norma y los requisitos propios de la organización. La alta gerencia también debe revisar su BCMS para asegurar la idoneidad y tomar decisiones para la mejora continua del BCMS.

5.3.4 Metodología de Análisis y Gestión de Riesgo MAGERIT. La metodología MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Esta metodología contempla diferentes actividades:

Determinar los activos relevantes de la empresa: Un activo es una parte fundamental para el sistema de información que en el caso que llegase a fallar produciría un efecto negativo en el funcionamiento de la empresa. En la metodología MAGERIT existen diferentes tipos:

- Los servicios que son prestados por el sistema. Como por ejemplo el correo electrónico, el almacenamiento de archivos gestión de identidades y/o privilegios, servicios al público en general, servicios internos, internet, entre otros.

- Datos e información, que pueden estar almacenado en archivos digitales, archivos físicos, copias de respaldo, datos de control de acceso y/o configuración, código fuente.

- Claves criptográficas, utilizadas para la protección de la información protección de las comunicaciones.

- Aplicaciones informáticas, ya sean desarrollos propios, desarrollos a la medida o estándares.

- Equipamiento informático, es todo hardware que soporta las aplicaciones informáticas, grandes y medianos servidores, equipos de mesa/portátiles, equipos móviles, equipos virtuales, equipos que soportan la red, periférico, entre otros.

- Personal o recurso humano, todas las personas relacionadas con el sistema de información; usuarios externos y/o internos, administradores, proveedores, contratista, etc.

- Redes de comunicaciones, incluye hasta los servicios contratados a terceros. Red telefónica, red digital, ADSL, telefonía móvil, internet, etc.

- Los soportes de información, son los dispositivos que permiten el almacenamiento de información como son los DVD, CD, discos, tarjetas de memoria, tarjetas inteligentes, memorias USB, etc.

- El equipamiento auxiliar, como son las fuentes de alimentación, sistemas de alimentación interrumpida, generadores eléctricos, equipos de climatización, cableado, equipos de destrucción, cajas fuertes y todo aquel equipo que sirva de soporte a los sistemas de información.

- Las instalaciones. Son los lugares donde se hospedan los sistemas de información y comunicaciones.

Luego los activos deben ser valorados de acuerdo a las dimensiones de seguridad:

- Confidencialidad, es decir valorar la gravedad que los datos sean conocidos por personas no autorizadas.

- Integridad de los datos, es decir valorar la importancia que los datos sean alterados de forma voluntaria o intencional.

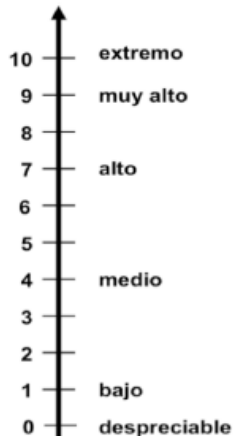
- Disponibilidad, valorar el daño que causaría que el activo no estuviera disponible cuando se requiera.

- Autenticidad, valorar la importancia que se identifique la fuente de donde proceden los datos o quien acceda a ellos.

- Trazabilidad, valorar la importancia que quede constancia del uso o acceso de los datos y/o servicios.

Es muy importante que los criterios de valoración sean homogéneos y se utilice una misma escala para todas las dimensiones. Magerit nos presenta un ejemplo de una escala detallada como muestra la Figura 3.

Figura 3. Criterios de Valoración Magerit



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Fuente: Libro II catálogo de elementos metodología Magerit

5.3.5.1 Determinar las amenazas a los que están expuestos los activos. Las amenazas a los que están expuestos los activos pueden ser:

- De origen natural: son todos aquellos eventos naturales que pueden presentarse, como por ejemplo fenómenos climáticos, fenómenos sísmicos, fenómenos de origen volcánico fenómeno meteorológico, inundaciones, contaminación.

- Del entorno: son los eventos industriales que pueden ocurrir con intervención del ser humano, por ejemplo, un incendio accidental o deliberado, daños ocasionados por el agua, corte del suministro eléctrico, fallas de climatización, fallos en los servicios de comunicación, daños o fallas en el Hardware.

- Defectos de las aplicaciones,

  - Originadas por personas de manera accidental, errores en el uso, inadecuado registro de log, errores de configuración, deficiencias en la organización, etc.

  - Originadas por personas de manera deliberada, por ejemplo, para escalar privilegios, suplantar la identidad de otra persona, manipular registros de datos, uso no previsto de las tecnologías de la información, difundir software dañino, destruir información, entre otras.

Al igual que los activos las amenazas también deben ser valoradas, estás se hacen en base a su degradación y probabilidad de ocurrencia. Esto con la

finalidad de medir que tanto daño puede causar su ocurrencia y que tan probable puede ser que ocurra.

5.3.5.2 Estimar los impactos y riesgos potenciales. El impacto potencial consiste en calcular el daño que puede causar una amenaza materializada a un activo y el riesgo potencial al que se enfrenta la empresa en función del impacto y la probabilidad de materialización de una amenaza.

5.3.5.3 Estimar las salvaguardas de los activos. Son medidas que se toman para proteger los activos de las amenazas. Las cuales pueden reducir la probabilidad de ocurrencia o limitar el daño que pueda causar la materialización de la amenaza. Existen diferentes tipos de salvaguardas de acuerdo a su protección:

- [PR] prevención
- [DR] disuasión
- [EL] eliminación
- [IM] minimización del impacto
- [CR] corrección
- [RC] recuperación
- [MN] monitorización
- [DC] detección
- [AW] concienciación
- [AD] administración

Las salvaguardas deberán ser medidas de acuerdo a la eficacia de su protección, dando como resultado el grado de eficacia real frente al riesgo.

5.3.5.4 Estimar los impactos y riesgos residuales. En esta fase se vuelven a realizar los cálculos del riesgo usando el impacto residual y la probabilidad de residual de ocurrencia. Se denomina residual porque se han extendido unas salvaguardas al sistema que harán que éste quede en una situación de posible impacto y riesgo.

5.3.5.5 Se consolidarán los resultados obtenidos y se realiza la documentación. La documentación final debe contener un modelo de valor donde se detalla los activos de la empresa valorados de acuerdo a las dimensiones de seguridad, el mapa de riesgos donde se detalla las amenazas sobre cada activo valoradas por su impacto y probabilidad de ocurrencia, la declaración de aplicabilidad donde se detallan las medidas que se consideran apropiados para salvaguardar el sistema, la calificación de las salvaguardas existentes de acuerdo a su eficacia, el informe de insuficiencias y vulnerabilidades

donde se detalla las salvaguardas necesarias pero que no están implementadas o que son ineficaces, también se realiza un informe sobre el estado del riesgo donde se encuentra el detalle del impacto y riesgo potencial y residual por cada amenaza.

5.3.5.6 Gestión del riesgo. Esta fase parte de las valoraciones anteriores y califica cada riesgo para determinar si es crítico, grave, es apreciable o asumible. Se realiza un estudio cuantitativo y cualitativo de costo/beneficio para determinar inversiones las medidas a tomar referente al riesgo al que se afronta.

5.4 MARCO CONCEPTUAL

5.4.1 Sistema de Información en la empresa. Conjunto de recursos técnicos, humanos y económicos, interrelacionados dinámicamente, y organizados en torno al objetivo de satisfacer las necesidades de información de una organización empresarial para la gestión correcta adopción de decisiones. [7]
Riesgo.

Es la probabilidad de que algo ocurra y afecte, perjudique o haga algún daño a algo o alguien.

Amenaza: son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o perdidas inmateriales en sus activos.[8]

Vulnerabilidad: es la posibilidad de ocurrencia de materialización de una amenaza.

Contingencia: es una alteración de la continuidad que impacta en forma relevante el normal desarrollo de un servicio considerado crítico, teniendo su origen en la falla de un componente o la interrupción de una tarea, sin estar necesariamente prevista[9].

Plan de Continuidad de Negocio: es un conjunto de procedimientos que se deben realizar para el restablecimiento de los procesos críticos de negocio después de una interrupción. Estos planes incluyen un perfil de las personas que

[7]DE PABLOS HEREDERO, Carmen, et al. Informática y comunicaciones en la empresa. Madrid España: ESIC Editorial, 2004. 316 p.
[8]MOLINER, Francisco. Grupos A y B de informática bloque especifico temario Volumen II. Sevilla, España: Editorial MAD, 2011. 203 p.
[9]DEPOSITO CENTRAL DE VALORES. Plan de Contingencia del DCV Fundamentos y Metodología Aplicada. [En línea]. Agosto 2008. [Revisado: agosto 2017]. Disponible en internet: https://www.contacto.dcv.cl/portalweb/Servicios/ Portal/ empresa/procedimientos/download/PlandeContingenciade0DCV2008.pdf

incorporan el comité encargado de realizar las tareas de recuperación, mantenimiento, comunicaciones y formatos requeridos para la documentación de los procesos.

Plan de Contingencia de las Tecnologías de la información y Comunicaciones: consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el Plan de Continuidad de Negocio de la compañía[10].

5.5 MARCO LEGAL

Decreto 1377 De 2013. REGLAMENTA PARCIALMENTE LA LEY 1581 DE 2012. Tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información.

Ley estatutaria 1581 de 2012PROTECCIÓN DE DATOS PERSONALES. En esta ley determina los principios que deben seguirse en todo Tratamiento de Datos Personales en toda la base de datos. Habla sobre los aspectos de Legalidad, Finalidad, Libertad, Veracidad o calidad de la información, transparencia, seguridad, acceso y circulación restringida, confidencialidad.

Ley 1273 del 5 de enero de 2009. DELITOS INFORMÁTICOS. Esta ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales. Sancionando delitos que atente contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y De los atentados informáticos y otras infracciones.

Ley Estatutaria 1266 De 2008. HÁBEAS DATA Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 603 de 2000. **DERECHOS DE AUTOR**. Esta ley se refiere a la protección de los derechos de autor en Colombia. Regulando la legalidad del software. Todas las

[10]DÍAZ SAMPEDRO, Manuel. Contingencia TIC vs Continuidad de negocio [en línea], 30 de septiembre de 2011 [Revisado agosto 2017]. Disponible en internet: https://www.incibe.es/protege-tu-empresa/blog/contingencia-vs-continuidad

empresas deben poseer las licencias que demuestren la legalidad de los programas que utilizan.

6. MARCO METODOLÓGICO

6.1 METODOLOGÍA DE INVESTIGACIÓN

6.1.1 Tipo de investigación. El enfoque de investigación de este proyecto es CUANTITATIVO, ya que durante su desarrollo se realizará una medición de los riesgos y amenazas que pueden afectar el normal funcionamiento de los procesos informáticos de la empresa.

Además, es una investigación tipo exploratoria, porque se requiere de recolección de datos para hacer el diagnostico. También es descriptiva, ya que en ella se describen las estrategias y los procedimientos para reanudar los servicios informáticos, los riesgos operativos y recursos tecnológicos. Y por último explicativa porque en su etapa final se construye un documento teórico explicando eventos que pueden presentarse y medidas que se deben tomar.

6.1.2 Población y muestra. La población son todos los empleados de la Ferretería Cesar que para el desarrollo de sus labores se apoyen en el uso de las Tecnologías de la Información y Comunicaciones.

La muestra serán algunos empleados de diferentes áreas que tenga la mayor experiencia en las labores de su área.

6.1.3 Instrumentos de recolección de información. Para la recolección de la información se utilizarán las técnicas de:

- Entrevistas: se aplicarán al gerente y los jefes de las áreas de sistema, contabilidad, ventas, cartera, compra y despacho.

- Cuestionarios y Listas chequeos: se realizarán con la finalidad de recoger información sobre los conocimientos generales de los empleados sobre los planes de contingencia e identificar los procesos críticos de cada área.

- Observación directa.

6.2 METODOLOGÍA DE DESARROLLO

La metodología aplicada para el desarrollo del proyecto son las recomendadas por el Instituto Nacional de Estadística e Informática del Perú (INEI), el instituto

nacional de Ciberseguridad de España, alineándola con el estándar internacional ISO / IEC 27031: 2011e ISO/IEC 22301:2012.

La metodología consta de varias fases y las actividades a desarrollar en cada fase que son las siguientes:

6.2.1 Fase 1. Identificación de Riesgos. Durante esta fase se identificarán los riesgos que pueden afectar el normal funcionamiento de los procesos informático de la empresa con el fin de hacer una valoración de los mismos.

De acuerdo a la metodología Magerit, se realizarán las siguientes actividades:

- Determinar los activos relevantes de la empresa
- Determinar las amenazas a los que están expuestos los activos
- Estimar los impactos potenciales y residuales
- Estimar las salvaguardas de los activos
- Se consolidarán los resultados obtenidos.

Durante esta fase también se analizarán los procesos de la empresa para identificar los procesos críticos de negocio y determinar el tiempo objetivo de recuperación.

6.2.2 Fase 2: Identificación de soluciones y Estrategias. Durante esta fase se van a establecer las estrategias preventivas que permitan disminuir la probabilidad de ocurrencia de un estado de contingencia. Se identificarán las alternativas de respuestas y de recuperación en caso de una emergencia de acuerdo al estándar ISO / IEC 27031 e ISO/IEC 22301.

6.2.3 Fase 3: Documentación del proceso. Durante esta fase se diseñarán los procedimientos de recuperación que pueden asegurar la continuidad de los servicios informáticos en caso de una interrupción. Se elaborará el documento que contiene el plan de contingencia informático, en él estará consolidado todo el análisis y documentación que se ha recogido en las fases anteriores y las soluciones a las contingencias.

6.2.4 Fase 4: Implementación, socialización y evaluación del plan de contingencia. Durante esta fase se evaluará el plan de contingencia informático realizando una prueba controlada con la finalidad de garantizar que se entrega un plan de contingencia acorde a la infraestructura de la empresa y de acuerdo a los estándares internacionales. Además, se socializará con la gerencia y se realizará sensibilización al personal para promover el buen uso y manejo del plan de contingencia informático.

6.3 PRODUCTO RESULTADO A ENTREGAR

Como resultado de este proyecto se entregará un documento que contiene el Plan de Contingencia Informático. Este plan contempla el análisis y la gestión de riesgos de la situación actual de la empresa, la definición de los procedimientos para la recuperación en caso de incidentes, la definición de roles y responsabilidades del recurso humano de la empresa, definición de las pruebas del plan y la guía para el mantenimiento del plan de contingencia. Además, se realizará la respectiva socialización y capacitación a todos los involucrados en el plan.

7. DESARROLLO DEL PROYECTO

De acuerdo a la metodología de desarrollo de este proyecto la primera fase es la identificación de los riesgos utilizando la metodología Magerit. Durante esta fase se determinan los activos relevantes de la empresa, se determinan las amenazas, se estiman los impactos y riesgos potenciales, se estiman las salvaguardas, se estiman los impactos y riesgo residuales. El análisis de riesgo ayudará a la toma de decisiones y es base para el despliegue de las estrategias que aseguren la continuidad de las actividades de negocio.

Pero antes de realizar el análisis de riesgo se procedió a identificar los procesos críticos de negocio que están soportados por las TIC, y la prioridad de recuperación en caso de una indisponibilidad total de los activos que soportan a estos procesos. Con la finalidad de centrar el análisis riesgo en los activos que son de importancia para la continuidad de las actividades de negocio.

En común acuerdo con la gerencia se identificaron 5 procesos críticos de negocio que son: la gestión de venta, la gestión de cartera, la gestión de compra, gestión contable y la gestión administrativa. Cada uno de estos procesos se describe en los cuadros 14, 15, 16, 17 y 18 del Anexo B. A estos procesos se les evaluó el impacto financiero que ocasionaría un evento catastrófico que impidiera que el proceso crítico esté disponible. Una vez analizado los procesos se estableció el tiempo objetivo de recuperación y la prioridad de recuperación para cada uno de los procesos críticos de negocio. Dando como resultado los descritos en el cuadro 1.

Cuadro 1. Procesos críticos de negocio con prioridad de recuperación

Proceso crítico de Negocio	**Prioridad de Recuperación**	**Tiempo objetivo de recuperación [RTO]**
Gestión de Ventas	1	Menor a 4 Horas
Gestión de Cartera	2	Menor a 8 Horas
Gestión de Compras	3	Menor a 8 Horas
Contabilidad	4	Menor a 24 Horas
Gestión Administrativa	5	Menor a 24 Horas

Fuente: autor.

Para la empresa el proceso más crítico es el de gestión de ventas, el estudio arrojó que con una parálisis mayor a 4 horas la empresa puede llegar a perder ingresos por más de 20 millones de pesos, la empresa considera catastrófico una parálisis por más de 8 horas.

El tiempo objetivo de recuperación RTO oscila entre 4 y 24 horas, durante este tiempo se debe establecer las estrategias de continuidad para los procesos que son considerados como prioritarios para la empresa. En base a estos procesos y prioridad de recuperación se diseñará el plan de contingencia informático.

El análisis de los procesos críticos de negocio se logró identificar los activos que soportan las operaciones críticas, los cuales se listan en el cuadro 2.

Cuadro 2. Activos que soportan los procesos críticos de negocio

Activo	Descripción	Tiempo objetivo de recuperación	Impacto Financiero	Dimensión de seguridad	Valoración del Activo
[HW_PC] Equipos de informática personal	Un equipo que haga parte de la gestión de ventas, cartera o compras. Su disponibilidad es alta.	4 Horas	Pérdidas de 2.5 Millones por equipo.	Confidencialidad	Medio
				Integridad	Alto
				Autenticidad	Bajo
				Disponibilidad	Alto
				Trazabilidad	Bajo
[HW_PRINT] Impresoras	Una impresora que haga parte de la gestión de ventas. Su disponibilidad es alta.	4 Horas	Pérdidas de 2.5 Millones por impresora.	Confidencialidad	Bajo
				Integridad	Bajo
				Autenticidad	Bajo
				Disponibilidad	Alto
				Trazabilidad	Bajo
[HW_HOST1] Servidor de aplicaciones y archivos	Su disponibilidad es de gran impacto. Es esencial en todos los procesos críticos de negocio.	4 Horas	Pérdidas de 20 Millones de pesos.	Confidencialidad	Alto
				Integridad	Medio
				Autenticidad	Bajo
				Disponibilidad	Alto
				Trazabilidad	Bajo
[SW_ZAFIRO] Sistema de Inventario, Facturación y Compras	Su disponibilidad es de gran impacto. Es esencial para la gestión de venta, cartera y compras	4 Horas	Pérdidas de 20 Millones de pesos.	Confidencialidad	Medio
				Integridad	Alto
				Autenticidad	Bajo
				Disponibilidad	Alto
				Trazabilidad	Bajo
[COM_PSTN] Red Telefónica	Su disponibilidad es de gran impacto. Es necesaria para las posibles ventas, compras y cobro.	8 Horas	Pérdidas de 3 Millones de pesos	Confidencialidad	Alto
				Integridad	Bajo
				Autenticidad	Bajo
				Disponibilidad	Alto
				Trazabilidad	Bajo

Cuadro 2. (Continuación)

Activo	Descripción	Tiempo objetivo de recuperación	Impacto Financiero	Dimensión de seguridad	Valoración del Activo
[COM_LAN] Red LAN	Su disponibilidad es de gran impacto. Es esencial para todos los procesos críticos.	4 Horas	Pérdidas de hasta 80 millones de pesos.	Confidencialidad	Alto
				Integridad	Alto
				Autenticidad	Bajo
				Disponibilidad	Alto
				Trazabilidad	Bajo
[COM_INTERNET] Red de acceso a Internet	El acceso a internet es esencial en las fechas de liquidación de impuesto, fines de mes y quincena para reporte a la policía.	6 Horas	Ocasionaría el pago de sanciones por reportes extemporáneos	Confidencialidad	Alto
				Integridad	Medio
				Autenticidad	Bajo
				Disponibilidad	Alto
				Trazabilidad	Bajo
[S_WWW] Servicios de hosting	La página web es externa, no se hacen pedidos en línea, pero promocionan productos. Útil para publicidad.	24 Horas	Pérdidas de posibles ventas generadas por la publicidad.	Confidencialidad	Bajo
				Integridad	Bajo
				Autenticidad	Bajo
				Disponibilidad	Medio
				Trazabilidad	Bajo
[S_EMAIL] servicio de email corporativos	Los correos corporativos son esenciales para la gestión de venta.	4 Horas	Generaría pérdidas de hasta 5 millones de pesos. Por invitaciones a cotizar.	Confidencialidad	Alto
				Integridad	Medio
				Autenticidad	Medio
				Disponibilidad	Alto
				Trazabilidad	Bajo

Fuente: autor

7.1 ANÁLISIS DE RIESGO UTILIZANDO LA METODOLOGÍA MAGERIT

7.1.1 Identificación de los activos. A través de entrevistas, encuestas, listas de chequeo y visitas a la Ferretería Cesar se logró identificar los activos relevantes de la empresa y se clasificaron de acuerdo a la metodología Magerit, dando como resultado el listado del cuadro 3

Cuadro 3. Activos de información de la Ferretería Cesar

Nombre del Activo	Descripción	Código y nombre del grupo de activo MAGERIT
[HW_HOST1]	Servidor 1, es el servidor de 3 sistemas de información que se usan en la actualidad y además es el servidor de archivos.	[HW] Equipos Informáticos
[HW_HOST2]	Servidor 2, contiene archivos históricos de la empresa y las aplicaciones de software que se usaron antes del año 2008.	[HW] Equipos Informáticos
[HW_PC]	Equipos de informática personal, existen 25	[HW] Equipos Informáticos
[HW_PRINT]	10 impresoras	[HW] Equipos Informáticos
[COM_PSTN]	1 Red Telefónica	[COM] Redes de comunicaciones
[COM_WIFI]	1 Red Inalámbrica	[COM] Redes de comunicaciones
[COM_LAN]	1 Red LAN	[COM] Redes de comunicaciones
[COM_INTERNET]	1 Red de acceso a Internet	[COM] Redes de comunicaciones
[SW_ZAFIRO]	Sistema de inventario, facturación compras y cartera “ZAFIRO”. Es el sistema donde actualmente se registra toda la información concerniente a la venta, compra, manejo de inventario, costos, cartera.	[SW] Aplicaciones (Software)
[SW_HELISA]	Sistema de contabilidad y nomina “HELISA”. Es el sistema en que se registra toda la información	[SW] Aplicaciones (Software)

Cuadro 3. (Continuación)

Nombre del Activo	Descripción	Código y nombre del grupo de activo MAGERIT
	referente a la nómina y la contabilidad de la empresa	
[SW_SIFFOX]	Sistema de Inventario, Facturación y Compras “SIFFOX”. Es el sistema donde se registró toda la información concerniente a la venta, compra, manejo de inventario, costos, cartera hasta el año 2016.	[SW] Aplicaciones (Software)
[SW_OTROS]	En este se incluyen los siguientes sistemas: El sistema de contabilidad “SisConPlus” donde se registró las transacciones contables de la empresa. Hasta el año 2015. El Sistema de contabilidad “LINKER” donde se registró todas las transacciones contables de la empresa hasta el año 2008. Sistema de Inventario “SIFEC”. Es el sistema donde se registraba toda la información concerniente a la venta, compra, manejo de inventario, costos, cartera hasta el año 2006. Las aplicaciones Ofimáticas.	[SW] Aplicaciones (Software)
[OS_WIN_2003]	Sistema Operativo Windows 2003 Server instalado en el Servidor 2	[SW] Aplicaciones (Software)
[OS_WIN_2012]	Sistema Operativo Windows 2012 Server R2 instalado en el Servidor 1	[SW] Aplicaciones (Software)
[S_WWW]	Servicios de hosting prestado por un tercero que aloja la página web	[S] Servicios

Cuadro 3. (Continuación)

Nombre del Activo	Descripción	Código y nombre del grupo de activo MAGERIT
	referente a la nómina y la contabilidad de la empresa	
[S_EMAIL]	Servicio contratado para el servicio de email corporativos	[S] Servicios
[AUX_AC]	Aires acondicionados	[AUX] Equipamiento Auxiliar
[AUX_UPS]	Sistemas de alimentación ininterrumpida	[AUX] Equipamiento Auxiliar
[AUX_SAFE]	1 Caja Fuerte	[AUX] Equipamiento Auxiliar
[AUX_GEN]	1 Generador Eléctrico	[AUX] Equipamiento Auxiliar
[AUX_CAB]	Cableado	[AUX] Equipamiento Auxiliar
[AUX_SISVIG]	Sistema de Vigilancia	[AUX] Equipamiento Auxiliar
[P_UI]	47 Usuarios Internos	[P] Personal
[P_ADM]	1 Administrador de Sistema	[P] Personal
[L_EDIFICIO]	Edificio	[L]Instalaciones

Fuente: autor

7.1.2 Valoración de los activos. Una vez que se han identificado los activos de información se procede a evaluar el perjuicio para la empresa si el activo se ve dañado de acuerdo a los criterios definidos en la tabla 1, se evalúa en cada dimensión de seguridad: disponibilidad [D], integridad de datos [I], confidencial de datos [C], autenticidad de los usuarios y de la información [A], trazabilidad de los servicios y de los datos [T].

Tabla 1. Criterios de valoración para los activos

Valor			Criterio
10 -9	Muy Alto	MA	Daño Extremadamente grave
6 -8	Alto	A	Daño Grave
3 – 5	Medio	M	Daño Importante
1 – 2	Bajo	B	Daño Menor
0	Despreciable	MB	Irrelevante a efectos prácticos

Fuente: MAGERIT. Libro III Metodología. Versión 3. [En línea], [consultado el 22 de septiembre de 2017]. Disponible en internet: https://www.ccn-cert.cni.es/documentos-publicos/1793-magent

Cuadro 4. Valoración de activos de acuerdo a las dimensiones de seguridad

Código grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de seguridad	Criterio
[pc]	[HW_PC]	Equipos de informática personal	Confidencialidad	5
			Integridad	6
			Autenticidad	0
			Disponibilidad	6
			Trazabilidad	0
[print]	[HW_PRINT]	Impresoras	Confidencialidad	0
			Integridad	0
			Autenticidad	0
			Disponibilidad	6
			Trazabilidad	0
[host]	[HW_HOST1]	Servidor de aplicaciones y archivos	Confidencialidad	8
			Integridad	5
			Autenticidad	0
			Disponibilidad	9
			Trazabilidad	0
	[HW_HOST2]	Servidor de aplicaciones antiguo	Confidencialidad	8
			Integridad	5
			Autenticidad	0
			Disponibilidad	9
			Trazabilidad	0
[PSTN]	[COM_PSTN]	Red Telefónica	Confidencialidad	8
			Integridad	2
			Autenticidad	0
			Disponibilidad	0

Cuadro 4. (Continuación)

Código grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de seguridad	Criterio
			Trazabilidad	0
[wifi]	[COM_WIFI]	Red Inalámbrica	Confidencialidad	5
			Integridad	2
			Autenticidad	0
			Disponibilidad	5
			Trazabilidad	0
[LAN]	[COM_LAN]	Red LAN	Confidencialidad	8
			Integridad	8
			Autenticidad	0
			Disponibilidad	9
			Trazabilidad	0
[Internet]	[COM_INTERNET]	Red de acceso a Internet	Confidencialidad	7
			Integridad	6
			Autenticidad	0
			Disponibilidad	7
			Trazabilidad	0
[app]	[SW_ZAFIRO]	Sistema de inventario, facturación compras y cartera “ZAFIRO”	Confidencialidad	7
			Integridad	8
			Autenticidad	0
			Disponibilidad	9
			Trazabilidad	0
	[SW_HELISA]	Información contable, nomina	Confidencialidad	8
			Integridad	8
			Autenticidad	8
			Disponibilidad	8
			Trazabilidad	0
	[SW_SIFFOX]	Sistema de Inventario, Facturación y Compras “SIFFOX”	Confidencialidad	7
			Integridad	7
			Autenticidad	7
			Disponibilidad	7
			Trazabilidad	0
	[SW_OTROS]	“SisConPlus”, “LINKER”, “SIFEC”	Confidencialidad	5
			Integridad	6
			Autenticidad	5
			Disponibilidad	5
			Trazabilidad	0

Cuadro 4. (Continuación)

Código grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de seguridad	Criterio
[OS]	[OS_WIN_2003]	Sistema Operativo	Confidencialidad	2
			Integridad	5
			Autenticidad	5
			Disponibilidad	5
			Trazabilidad	0
	[OS_WIN_2012]	Sistema Operativo	Confidencialidad	5
			Integridad	8
			Autenticidad	0
			Disponibilidad	8
			Trazabilidad	0
	[OS_WIN_7_8_10]	Sistema Operativo Windows 7, 8 y Windows 10	Confidencialidad	7
			Integridad	5
			Autenticidad	5
			Disponibilidad	5
			Trazabilidad	0
[email]	[S_EMAIL]	servicio de email corporativos	Confidencialidad	6
			Integridad	6
			Autenticidad	4
			Disponibilidad	5
			Trazabilidad	0
[S]	[S_WWW]	Servicios de hosting prestado por un tercero que aloja la página web	Confidencialidad	0
			Integridad	0
			Autenticidad	0
			Disponibilidad	2
			Trazabilidad	0
[AC]	[AUX_AC]	Aires acondicionados	Confidencialidad	0
			Integridad	0
			Autenticidad	0
			Disponibilidad	5
			Trazabilidad	0
[Ups]	[AUX_UPS]	Sistemas de alimentación ininterrumpida	Confidencialidad	0
			Integridad	0
			Autenticidad	0
			Disponibilidad	5
			Trazabilidad	0
[safe]	[AUX_SAFE]	Caja Fuerte	Confidencialidad	2
			Integridad	0

Cuadro 4. (Continuación)

Código grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de seguridad	Criterio
			Autenticidad	0
			Disponibilidad	5
			Trazabilidad	0
[gen]	[AUX_GEN]	Generador Eléctrico	Confidencialidad	0
			Integridad	0
			Autenticidad	0
			Disponibilidad	5
			Trazabilidad	0
[wire]	[AUX_CAB]	Cableado	Confidencialidad	0
			Integridad	0
			Autenticidad	0
			Disponibilidad	8
			Trazabilidad	0
	[AUX_SISVIG]	Sistema de Vigilancia	Confidencialidad	6
			Integridad	6
			Autenticidad	0
			Disponibilidad	5
			Trazabilidad	0
[ui]	[P_UI]	Usuarios Internos	Confidencialidad	8
			Integridad	8
			Autenticidad	0
			Disponibilidad	5
			Trazabilidad	0
[adm]	[P_ADM]	Administrador de Sistema	Confidencialidad	7
			Integridad	5
			Autenticidad	0
			Disponibilidad	8
			Trazabilidad	0
[local]	[L_EDIFICIO]	Edificio	Confidencialidad	0
			Integridad	0
			Autenticidad	0
			Disponibilidad	9
			Trazabilidad	0

Fuente: autor

7.1.3 Caracterización de las amenazas. Siguiendo la metodología Magerit en su versión 3, una vez que son valorados los activos de información se procede a identificar las amenazas ([N] Desastres Naturales, [L] De origen Industrial, [E] Errores y fallos no intencionados, [A] Ataques intencionados) a los que están expuestos cada activo, de acuerdo al catálogo de amenazas establecidas en la metodología:

Dando como resultado las descritas en el cuadro 5.

Cuadro 5. Identificación de las Amenazas

Activos	Amenazas	
[HW] Equipos Informáticos		
[HW_HOST1] Servidor de Aplicaciones	[N.1] [N.2] [N*] [I.2] [I.5] [I.7] [I*] [A.11] [A.18]	Fuego Daños por agua Desastres Naturales Daños por agua Avería de origen físico o lógico Condiciones inadecuadas de temperatura Desastres Industriales Acceso no autorizado
[HW_HOST2] Servidor de Aplicaciones y Archivos	[N.1] [N.2] [N*] [I.2] [I.5] [I.7] [I.*] [E.24] [A.11]	Fuego Daños por agua Desastres Naturales Daños por agua Avería de origen físico o lógico Condiciones inadecuadas de temperatura Desastres Industriales Caída del sistema por agotamiento de recursos Acceso no autorizado
[HW_PC] Equipos de informática personal	[N.1] [N.2] [N*] [I.2] [I.5] [I.7] [I.*] [E.24] [A.7] [A.25]	Fuego Daños por agua Desastres Naturales Daños por agua Avería de origen físico o lógico Condiciones inadecuadas de temperatura Desastres Industriales Caída del sistema por agotamiento de recursos Uso no previsto Robo

Cuadro 5. (Continuación)

Activos	Amenazas	
[HW_PRINT] Impresoras	[N.1] [N.2] [N*] [I.2] [I.5] [I.7]	Fuego Daños por agua Desastres Naturales Daños por agua Avería de origen físico o lógico Condiciones inadecuadas de temperatura
[COM] Redes de comunicaciones		
[COM_WIFI] Red Inalámbrica	[I.8] [A.7]	Fallos de servicios de telecomunicaciones Uso no previsto
[COM_LAN] Red LAN	[I.8] [A.11]	Fallos de servicios de telecomunicaciones Acceso no autorizado
[COM_INTERNET] Red de acceso a Internet	[I.8] [A.7]	Fallos de servicios de telecomunicaciones Uso no previsto
[SW] Aplicaciones (Software)		
[SW_ZAFIRO]Sistema de Inventario, Facturación y Compras	[I.5] [E.1] [E.8] [E.20] [E.21] [A.5] [A.11]	Avería de origen físico o lógico Errores de los usuarios Difusión de software dañino Vulnerabilidades de los programas (Software) Errores Mantenimiento / actualización de programas (software) Suplantación de identidad Acceso no autorizado
[SW_HELISA] Sistema de Información contable, nomina	[I.5] [E.1] [E.8] [E.20] [E.21] [A.5] [A.11]	Avería de origen físico o lógico Errores de los usuarios Difusión de software dañino Vulnerabilidades de los programas (Software) Errores Mantenimiento / actualización de programas (software) Suplantación de identidad Acceso no autorizado
[SW_SIFFOX]Sistema de Inventario, Facturación y Compras “SIFFOX”	[E.18] [A.5] [A.11]	Destrucción de información Suplantación de identidad Acceso no autorizado
[SW_OTROS]“SisConPlus”, “LINKER”, “SIFEC”	[I.5] [E.18] [A.5] [A.11]	Avería de origen físico o lógico Destrucción de información Suplantación de identidad Acceso no autorizado

Cuadro 5. (Continuación)

Activos	Amenazas	
[OS_WIN_2003] Sistema Operativo	[I.5] [E.2] [E.8] [E.21] [A.11]	Avería de origen físico o lógico Errores del administrador Difusión de software dañino Errores Mantenimiento / actualización de programas (software) Acceso no autorizado
[OS_WIN_2012] Sistema Operativo	[I.5] [E.2] [E.8] [E.21] [A.11]	Avería de origen físico o lógico Errores del administrador Difusión de software dañino Errores Mantenimiento / actualización de programas (software) Acceso no autorizado
[OS_WIN_7_8_10]Sistema Operativo	[I.5] [E.1] [E.8] [E.21] [A.5] [A.11]	Avería de origen físico o lógico Errores de los usuarios Difusión de software dañino Errores Mantenimiento / actualización de programas (software) Suplantación de identidad Acceso no autorizado
[S] Servicios		
[S_WWW] Servicios de hosting	[E.24] [A.24]	Caída del sistema por agotamiento de recursos Denegación del servicio
[S_EMAIL] servicio de email corporativos	[E.1] [E.24] [A.5] [A.11]	Errores de usuarios Caída del sistema por agotamiento de recursos Suplantación de la identidad del usuario Acceso no autorizado
[AUX] Equipamiento Auxiliar		
[AUX_AC] Aires acondicionados	[I.3]	Contaminación medioambiental
[AUX_UPS] Sistemas de alimentación ininterrumpida	[I.3]	Contaminación medioambiental
[AUX_SAFE] Caja Fuerte	[I.3] [A.25]	Contaminación medioambiental Robo
[AUX_GEN] Generador Eléctrico	[I.3]	Contaminación medioambiental
[AUX_CAB] Cableado	[I.3]	Contaminación medioambiental
[AUX_SISVIG] Sistema de Vigilancia	[I.3] [A.11] [A.26]	Contaminación medioambiental Acceso no autorizado Ataque Destructivo

Cuadro 5. (Continuación)

Activos	Amenazas	
[P] Personal		
[P_UI] Usuarios Internos	[E.19] [E.28] [A.29] [A.30]	Fuga de Información Indisponibilidad del personal Extorsión Ingeniería social (picaresca)
Cuadro 4. (Continuación)		
[P_ADM] Administrador de Sistema	[E.19] [E.28] [A.29] [A.30]	Fuga de Información Indisponibilidad del personal Extorsión Ingeniería social (picaresca)
[L]Instalaciones		
[L_EDIFICIO]EDIFICIO	[I.1] [N.2] [N*] [A.11] [A.26]	Fuego Daños por agua Desastres Naturales Acceso no autorizado Ataque Destructivo

Fuente: autor

Una vez se han identificado las amenazas de cada activo se procede a valorar cada amenaza. La valoración consiste en determinar la probabilidad de ocurrencia de la materialización de la amenaza y la degradación que causaría en cada dimensión de seguridad (Confidencialidad [C], Integridad [I], Autenticidad [A], Disponibilidad [D], Trazabilidad [T]). De acuerdo a la escala de la tabla 2 se realiza la valoración de las amenazas, descritas en el cuadro 6.

Tabla 2. Criterios de valoración de las amenazas

Criterio	Niveles de Degradación[N]	Probabilidad de Ocurrencia [P]	Impacto [I]
MB	Muy Bajo	Muy raro	Muy Bajo
B	Bajo	Poco Probable	Bajo
M	Medio	Posible	Medio
A	Alto	Probable	Alto
MA	Muy Alto	Prácticamente Seguro	Muy Alto

Fuente: MAGERIT. Libro III Metodología. Versión 3. [En línea], [consultado el 22 de septiembre de 2017]. Disponible en internet: https://www.ccn-cert.cni.es/documentos-publicos/1793-magent

En el anexo D se registraron gráficamente evidencias de amenazas y vulnerabilidades encontradas.

Cuadro 6. Valoración de Amenazas

Activo	**Amenaza**		**Dimensiones**				
		[P]	**{D}**	**{I}**	**{C}**	**{A}**	**{T}**
[HW_HOST1] Servidor de Aplicaciones y Archivos	[N.1] Fuego	B	MA				
	[N.2] Daños por agua	MB	MA				
	[N*] Desastres Naturales	B	MA				
	[I.2] Daños por agua	A	MA				
	[I.5] Avería de origen físico o lógico	M	A				
	[I.7] Condiciones inadecuadas de temperatura	A	MA				
	[I.*] Desastres Industriales	M	MA				
	[A.11] Acceso no autorizado	M		M	A		
[HW_HOST2] Servidor de Aplicaciones y Archivos	[N.1] Fuego	B	MA				
	[N.2] Daños por agua	MB	MA				
	[N*] Desastres Naturales	B	MA				
	[I.2] Daños por agua	A	MA				
	[I.5] Avería de origen físico o lógico	M	A				
	[I.7] Condiciones inadecuadas de temperatura	A	MA				
	[I.*] Desastres Industriales	M	MA				
	[E.24] Caída del sistema por agotamiento de recursos	B	MA				
	[A.11] Acceso no autorizado	M		M	A		

Cuadro 6. (Continuación)

Activo	Amenaza		Dimensiones				
		[P]	{D}	{I}	{C}	{A}	{T}
[HW_PC] Equipos de informática personal	[N.1] Fuego	B	MA				
	[N.2] Daños por agua	MB	MA				
	[N*] Desastres Naturales	B	MA				
	[I.2] Daños por agua	A	MA				
	[I.5] Avería de origen físico o lógico	M	A				
	[I.7] Condiciones inadecuadas de temperatura	M	M				
	[I.*] Desastres Industriales	M	MA				
	[E.24] Caída del sistema por agotamiento de recursos	B	MA				
	[A.7] Uso no previsto	B	M	M	B		
	[A.25] Robo	MB	M		B		
[HW_PRINT] Impresoras	[N.1] Fuego	B	MA				
	[N.2] Daños por agua	MB	MA				
	[N*] Desastres Naturales	B	MA				
	[I.2] Daños por agua	A	M				
	[I.5] Avería de origen físico o lógico	M	A				
	[I.7] Condiciones inadecuadas de temperatura	M	M				
[COM_PSTN] Red Telefónica	[I.8] Fallos de servicios de telecomunicaciones	M	MA				
	[E.19] Fugas de Información	B			MA		
	[A.7] Uso no previsto	B	M	M	M		
[COM_WIFI] Red Inalámbrica	[I.8] Fallos de servicios de	M	MA				

Cuadro 6. (Continuación)

Activo	Amenaza		Dimensiones				
		[P]	{D}	{I}	{C}	{A}	{T}
	telecomunicaciones						
	[A.7] Uso no previsto	B	M	MB	M		
[COM_LAN] Red LAN	[I.8] Fallos de servicios de telecomunicaciones	M	MA				
	[A.11] Acceso no autorizado	M		M	A		
[COM_INTERNET] Red de acceso a Internet	[I.8] Fallos de servicios de telecomunicaciones	M	MA				
	[A.7] Uso no previsto	B	M	B	M		
[SW_ZAFIRO] Sistema de Inventario, Facturación y Compras	[I.5] Avería de origen físico o lógico	M	A				
	[E.1] Errores de los usuarios	M	A	A	A		
	[E.8] Difusión de software dañino	A	MA	MA	M		
	[E.20] Vulnerabilidades de los programas (Software)	M	M	M	M		
	[E.21] Errores Mantenimiento / actualización de programas (software)	M	M	M			
	[A.5] Suplantación de identidad	M		M	M	M	
	[A.11] Acceso no autorizado	M		A	A		
[SW_HELISA] Sistema de Información contable, nomina	[I.5] Avería de origen físico o lógico	M	A				
	[E.1] Errores de los usuarios	M	M	A	A		
	[E.8] Difusión de software dañino	A	MA	A	A		
	[E.20] Vulnerabilidades de los programas (Software)	M	M	M	M		

Cuadro 6. (Continuación)

Activo	Amenaza		Dimensiones				
		[P]	{D}	{I}	{C}	{A}	{T}
	[E.21] Errores Mantenimiento / actualización de programas (software)	M	M	M			
	[A.5] Suplantación de identidad	M		B	M	M	
	[A.11] Acceso no autorizado	M		A	A		
[SW_SIFFOX] Sistema de Inventario, Facturación y Compras “SIFFOX”	[E.18] Destrucción de información	MA	M				
	[A.5] Suplantación de identidad	M		M	M	M	
	[A.11] Acceso no autorizado	M		A	A		
[SW_OTROS] “SisConPlus”, “LINKER”, “SIFEC”	[I.5] Avería de origen físico o lógico	M	A				
	[E.18] Destrucción de información	MA	M				
	[A.5] Suplantación de identidad	M		B	M	M	
	[A.11] Acceso no autorizado	M		A	A		
[OS_WIN_2003] Sistema Operativo	[I.5] Avería de origen físico o lógico	M	A				
	[E.2] Errores del administrador	B	A	A	M		
	[E.8] Difusión de software dañino	A	MA	MA	B		
	[E.21] Errores Mantenimiento / actualización de programas (software)	M	M	M			
	[A.11] Acceso no autorizado	M		A	A		
[OS_WIN_2012] Sistema Operativo	[I.5] Avería de origen físico o lógico	M	A				
	[E.2] Errores del administrador	B	A	A	M		
	[E.8] Difusión de software dañino	A	MA	MA	MA		
	[E.21] Errores Mantenimiento / actualización de programas (software)	M	M	M			

Cuadro 6. (Continuación)

Activo	**Amenaza**		**Dimensiones**				
		[P]	**{D}**	**{I}**	**{C}**	**{A}**	**{T}**
	[A.11] Acceso no autorizado	M		A	A		
[OS_WIN_7_8_10]Sistema Operativo	[I.5] Avería de origen físico o lógico	M	A				
	[E.1] Errores de los usuarios	M	M	A	B		
	[E.8] Difusión de software dañino	A	MA	M	B		
	[E.21] Errores Mantenimiento / actualización de programas (software)	M	M	M			
	[A.5] Suplantación de identidad	M		M	M	M	
	[A.11] Acceso no autorizado	M		A	A		
[S_WWW] Servicios de hosting	[E.24] Caída del sistema por agotamiento de recursos	B	MA				
[S_EMAIL] servicio de email corporativos	[E.1] Errores de los usuarios	M	A	MA	MA		
	[E.24] Caída del sistema por agotamiento de recursos	B	MA				
	[A.5] Suplantación de identidad	M		B	M	M	
	[A.11] Acceso no autorizado	M		A	A		
[AUX_AC] Aires acondicionados	[I.3] Contaminación medioambiental	A	M				
[AUX_UPS] Sistemas de alimentación ininterrumpida	[I.3] Contaminación medioambiental	A	M				
[AUX_SAFE] Caja Fuerte	[I.3] Contaminación medioambiental	A	B				
	[A.25] Robo	MB	M		M		
[AUX_GEN] Generador Eléctrico	[I.3] Contaminación medioambiental	A	M				
[AUX_CAB] Cableado	[I.3] Contaminación medioambiental	A	M				
[AUX_SISVIG] Sistema de Vigilancia	[I.3] Contaminación medioambiental	A	B				
	[A.11] Acceso no autorizado	M		A	A		

Cuadro 6. (Continuación)

Activo	Amenaza		Dimensiones				
		[P]	{D}	{I}	{C}	{A}	{T}
	[A.26] Ataque Destructivo	MB	M				
[P_UI] Usuarios Internos	[E.19] Fugas de Información	B			MA		
	[E.28] Indisponibilidad del personal	B	B				
	[A.29] Extorsión	MB	B	B	M		
	[A.30] Ingeniería social (picaresca)	B	A	A	MA		
[P_ADM] Administrador de Sistema	[E.19] Fugas de Información	B			MA		
	[E.28] Indisponibilidad del personal	B	B				
	[A.29] Extorsión	MB	A	A	A		
	[A.30] Ingeniería social (picaresca)	B	M	M	A		
[L_EDIFICIO] Edificio	[N.1] Fuego	B	MA				
	[N.2] Daños por agua	MB	MA				
	[N*] Desastres Naturales	B	MA				
	[A.26] Ataque Destructivo	MB	M				

Fuente: autor

A continuación, se presenta las consideraciones que se tuvieron en cuenta para la estimación de los resultados anteriores.

Cuadro 7. Explicación de la estimación de la valoración de amenazas

Amenazas	Explicación de la estimación
[I.1] Fuego	En caso de ocurrir un incendio el nivel de degradación sería muy alto y afectaría su disponibilidad. El centro de datos cuenta con un sistema de detección de incendios y extintor. Existen extintores estratégicamente bien ubicados. En las áreas de cartera y gestión de compras no cuentan con sistema de detección de incendios. La empresa comercializa productos inflamables. Históricamente no se ha presentado ningún incendio en la empresa.
[N.2] Daños por agua	El centro de datos se encuentra ubicado en el segundo piso del edificio, no existen ventanas al exterior del edificio. Las fuertes lluvias que se presentan en la ciudad no han ocasionado inundaciones. Sin embargo, en caso de ocurrir una inundación afectaría de manera muy alta la disponibilidad de los activos.
[N*] Desastres Naturales	Históricamente en la ciudad no se han presentado terremotos, derrumbes, inundaciones o cualquier otro tipo de desastre natural. Sin embargo, no se puede garantizar que no llegue a ocurrir. En caso de materializarse esta amenaza la degradación sería muy alta. La empresa cuenta con planes de emergencia y recuperación de desastre.
[I.2] Daños por agua	Es probable que pueda ocurrir un incidente debido a que los empleados tienen constantemente vasos de agua en sus puestos de trabajo. Por otra parte, el centro de datos queda en frente de los baños de la empresa y en caso de una fuga podrían resultar afectados. En el techo de la sala de ventas pasa el ducto del aire acondicionado y los equipos de cómputos están ubicados debajo de ese ducto, generalmente hay gotas de agua en los escritorios.
[I.3] Contaminación medioambiental	Existe una gran acumulación de polvo en todo el equipamiento auxiliar. Ver imágenes en el anexo C.
[I.5] Avería de origen físico o lógico	Es posible que se pueda dañar un disco duro, ocurrir un fallo en la tarjeta madre del equipo, un error en el sistema operativo o en un software de importancia para la empresa. En caso del daño de alguna de pieza de un equipo o de su sistema operativo el nivel de degradación seria alto afectando la disponibilidad del mismo.
[I.7] Condiciones inadecuadas de temperatura	El centro de datos tiene un inadecuado sistema de climatización, ver imagen en el anexo C. Algunos equipos de informática personal están adecuadamente climatizados, sin embargo, existen algunos que no tiene una adecuada ventilación y están expuestos a altas temperaturas.

Cuadro 7. (Continuación)

Amenazas	Explicación de la estimación
[I.8] Fallos de servicios de telecomunicaciones	Es posible que pueda existir destrucción de los medios de comunicación por la inapropiada organización del cableado y la exposición del mismo en varias áreas de la empresa, la ubicación de los módems inalámbricos no es apropiada.
[I.*] Desastres Industriales	El centro de datos está ubicado en una bodega donde hay productos inflamables. Existen equipos con UPS dañadas y otros que no cuentan con una. Algunos reguladores no funcionan y hay equipos conectados directamente a la fuente de alimentación.
[E.1] Errores de los usuarios	Pueden ocurrir errores involuntarios por parte de los usuarios de los sistemas de información y de algunos servicios. Muchas veces por desconocimiento en el uso de los sistemas de información y/o herramientas ofimáticas, opciones del sistema operativo. Los empleados no realizan copias de sus archivos. En ocasiones hacen envíos a correos electrónicos al destinatario erróneo.
[E.2] Errores del administrador	El administrador del sistema está muy bien capacitado. Sin embargo, existen muchos procesos de instalación y configuración que no están documentados. Los sistemas operativos tienen puertos abiertos que son innecesarios y sus servicios configurados con puertos por defectos.
[E.8] Difusión de software dañino	Es una amenaza que puede degradar de manera muy alta los sistemas de información y los sistemas operativos de la empresa. Tiene una probabilidad de ocurrencia muy probable ya que en la empresa existe mucho intercambio de información a través de correos electrónicos, memorias USB, a través de carpetas compartidas. Aunque la empresa cuenta con software antivirus en todos los equipos clientes y servidores, hay muchas utilidades de los antivirus que están deshabilitadas, no hay restricciones para las descargas e instalación de software. Se han presentado varios casos de infección.
[E.18] Destrucción de información	Los antiguos sistemas de información se acceden mediante una unidad de red, estos sistemas fueron desarrollados en Visual Fox Pro y su base de datos se encuentra en la misma carpeta del ejecutable, así que toda la carpeta es compartida. La eliminación de cualquier archivo afectaría el funcionamiento de los mismos. En una ocasión fue eliminada una tabla accidentalmente. Los empleados colocan en las carpetas compartidas del servidor, archivos que son importantes para sus funciones sin ninguna copia de los mismos.
[E.19] Fugas de Información	Es poco probable la probabilidad de ocurrencia de esta amenaza, sin embargo, en caso de fuga de información puede llegar hacer muy alta colocando en riesgo la confidencialidad. En una ocasión hubo un robo de material porque se fugó información de la forma en que un cliente hacia los pedidos a crédito, se tomaron controles al respecto.

Cuadro 7. (Continuación)

Amenazas	Explicación de la estimación
[E.20] Vulnerabilidades de los programas (Software)	Esta amenaza generalmente se presenta cuando se coloca en producción un nuevo módulo que en muchos casos tienen errores de codificación que han afectado la integridad de la información y otras veces la disponibilidad del sistema de información. Hay muchos equipos en que los sistemas operativos no tienen activo la opción de actualizaciones automáticas, para la corrección de vulnerabilidades.
[E.21] Errores Mantenimiento / actualización de programas (software)	Hay muchos equipos en que los sistemas operativos no tienen activo la opción de actualizaciones automáticas, para la corrección de vulnerabilidades. El sistema Zafiro trabaja con ejecutables locales en cada equipo y muchas veces no tienen la misma versión, ocasionando errores que ya están corregidos en versiones posteriores.
[E.24] Caída del sistema por agotamiento de recursos	Anteriormente a este análisis se presentaba caída del sistema, pero se adquirió un nuevo servidor (servidor 1), se repotenció el servidor anterior (servidor 2) y los equipos clientes han sido remplazados paulatinamente.
[E.28] Indisponibilidad del personal	El ausentismo laboral es bajo.
[A.5] Suplantación de identidad	En ocasiones el personal interno comparte las claves de acceso a los sistemas de información y/o claves de los sistemas operativos. El personal acostumbra a levantarse de su sitio de trabajo dejando las sesiones de los programas abiertos.
[A.7] Uso no previsto	No hay restricciones en los equipos clientes para la instalación de programas de software que pueden generar conflicto con las aplicaciones y/o servicios de negocio instaladas, afectando la disponibilidad de las mismas. La red telefónica puede ser usada para fines personales al igual que el servicio de internet.
[A.11] Acceso no autorizado	El centro de datos está ubicado en una zona donde transita mucho personal interno, la puerta y la cerradura que tiene instalado puede ser violada con facilidad. Desde la oficina de contabilidad hay una ventana sin ningún tipo de seguridad donde se puede acceder al centro de datos. Las contraseñas de acceso a los sistemas operativos de los servidores no son robustas. Algunos equipos de informática personal no tienen asignadas claves de acceso para el sistema operativo. El personal no bloquea el escritorio de su equipo cuando se ausenta de su puesto de trabajo y generalmente dejan las sesiones abiertas de los programas.
[A.18] Destrucción de información	El servidor de aplicaciones tiene una carpeta compartida que está creada como unidad de red en los equipos clientes. Muchos usuarios la utilizan para guardar información de vital importancia para la empresa y han ocurrido casos en que la información ha sido borrada y no hay registros de quien la eliminó. Esta unidad compartida

Cuadro 7. (Continuación)

Amenazas	Explicación de la estimación
	Los correos personales son utilizados para realizar labores misionales de la empresa.
[A.25] Robo	La empresa no ha registrado casos de robos por lo tal motivo se estima una probabilidad de ocurrencia poco probable. La empresa cuenta con pólizas de seguros contra robos, tiene instaladas cámaras de seguridad.
[A.26] Ataque Destructivo	La empresa se encuentra ubicada en un sector donde los índices de vandalismo son altos, sin embargo, el sector es constantemente monitoreado por la fuerza pública. Debido a esto se estima una probabilidad de ocurrencia muy rara.
[A.29] Extorsión	No se han presentado casos de extorsión. Sin embargo, es importante crear concienciación que existe la amenaza.
[A.30] Ingeniería social (picaresca)	No se han registrado abusos de la buena fe de las personas. Sin embargo, se debe capacitar personal sobre la confidencialidad de la información.

Fuente: autor.

7.1.4 Estimar las salvaguardas de los activos. Para estimar las salvaguardas se tuvo en cuenta el catálogo de salvaguardas propuesta por la metodología Magerit en el libro II catálogo de elementos. Para medir la eficacia y la madurez de las salvaguardas se empleó los criterios descritos en la Tabla 3.

Tabla 3. Eficacia y madurez de las Salvaguardas

Eficacia	Nivel	Madurez	Descripción
0%	L0	Inexistente	La salvaguarda no existe.
10%	L1	Inicial/ad hoc	La salvaguarda existe o está definida, pero en un estado donde no es utilizada o se utiliza esporádicamente.
30 %	L2	Reproducible, pero intuitivo	La salvaguarda existe o está definida, se utiliza pero está en un estado de ajuste, está en desarrollo o está sin documentación
60 %	L3	Proceso definido	La salvaguarda está en funcionamiento. Pero puede ser mejorada.

Tabla 3. (Continuación)

Eficacia	Nivel	Madurez	Descripción
80%	L4	Gestionado y medible	La salvaguarda está en funcionamiento se obtiene indicadores de ella.
100%	L5	Optimizado	La salvaguarda está en funcionamiento se obtiene indicadores de ella y está en un continuo mejoramiento.

Fuente: MAGERIT. Libro III Metodología. Versión 3. [En línea], [consultado el 22 de septiembre de 2017]. Disponible en internet: https://www.ccn-cert.cni.es/documentos-publicos/1793-magent

Cuadro 8. Caracterización y valoración de las salvaguardas

Salvaguarda	Amenaza mitigada	Nivel	Descripción del Control / Salvaguarda
Protecciones Generales			
[H.IA] Identificación y autenticación	[A.11] Acceso no autorizado	L0	a) Política para la construcción de contraseñas seguras.
[H.tools.AV] Herramienta contra código dañino	[E.8] Difusión de software dañino	L3 L0	a) Revisión periódica de la habilitación de todas las herramientas de software antivirus. b) Política para la limitación de instalación de software no autorizado.
Protección de los Datos / Información			
[D.A] Copias de seguridad de los datos	[I.1] Fuego [N.2] Daños por agua [N*] Desastres Naturales [I.2] Daños por agua [I.5] Avería de origen físico o lógico [A.18] Destrucción de información [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (Software)	L0 L0	a) Los usuarios deben realizar sus propias copias de seguridad de los datos almacenados en sus equipos. b) Las copias de seguridad deben ser resguardada en lugares lejos de canalizaciones de energía y agua.
Protección de los servicios			
[S.www] Protección de servicios y aplicaciones web	[E.24] Caída del sistema por agotamiento de recursos	L1	a) Documentar los datos de contactos de soporte para un evento de dificultad
[S.SC] Se aplican perfiles de seguridad	[A.7] Uso no previsto [A.18] Destrucción de información	L0 L2	a) Política para la creación de perfiles de usuarios en todos los sistemas operativos. b) Política de mínimo permiso asignado a los perfiles de usuarios.

Cuadro 8. (Continuación)

Salvaguarda	Amenaza mitigada	Nivel	Descripción del Control / Salvaguarda
[S.email] Protección del correo electrónico	[E.24] Caída del sistema por agotamiento de recursos [E.1] Errores de los usuarios	L1 L0	a) Documentar los datos de contactos de soporte para un evento de dificultad b) Política para el almacenamiento de los contactos en los correos electrónico con una identificación inequívoca.
[S.dir] Protección del directorio	[A.18] Destrucción de información	L0	a) La carpeta compartida de los sistemas de información antiguo debe ser restringido el permiso de eliminación.
Protección de las aplicaciones (software)			
[SW.A] Copias de seguridad (backup)	[I.1] Fuego [N.2] Daños por agua [N*] Desastres Naturales [I.2] Daños por agua [I.5] Avería de origen físico o lógico [A.18] Destrucción de información [E.1] Errores de los usuarios [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (Software)	L5 L5 L3	a) Copias de seguridad de la base de datos de las aplicaciones críticas de la empresa. Con una frecuencia diaria. b) Mantener copias de seguridad fuera y dentro del edificio. c) Localizar las copias de seguridad dentro del edificio en un lugar seguro y lejos de canalizaciones de energía o agua.
[SW.CM] Cambios (actualizaciones y mantenimiento)	[E.20] Vulnerabilidades de los programas (Software) [E.19] Fugas de Información	L2 L0 L0 L0	a) Activar las actualizaciones automáticas de los sistemas operativos y aplicaciones de ofimática b) Llevar un registro de las actualizaciones de las aplicaciones críticas de negocio. c) Establecer una revisión periódica de las actualizaciones software. d) Firmar acuerdos de confidencialidad con los

Cuadro 8. (Continuación)

Salvaguarda	Amenaza mitigada	Nivel	Descripción del Control / Salvaguarda
			proveedores de software que requieran del envío de copias de la base de datos de la empresa.
[SW.start] Puesta en producción	[E.20] Vulnerabilidades de los programas (Software)	L0	a) Crear un ambiente de pruebas para que antes de colocar módulos en producción sea probado su comportamiento.
[SW] Protección de las Aplicaciones Informáticas	[E.1] Errores de los usuarios [E.8] Difusión de software dañino [E.21] Errores Mantenimiento / actualización de programas (software) [E.2] Errores del administrador [A.5] Suplantación de identidad	L1 L0 L3 L0 L3 L0 L0 L3	a) La instalación de programas sea gestionada solo por las personas del área de sistemas. b) Establecer procedimientos para la gestión y solicitudes de la instalación de programas que requieran los usuarios internos. c) Revisar que las aplicaciones instaladas cuenten con su licencia de uso. d) Llevar un inventario de las aplicaciones instaladas, su distribución, uso y responsable del uso. e) Notificación a proveedores de software sobre errores de las aplicaciones originado por errores del usuario para que tomen medidas que ayuden a minimizar este tipo de errores. f) Análisis de vulnerabilidades de los sistemas operativos de los servidores g) Documentar proceso de actualización de las aplicaciones críticas, lista de chequeo para verificar el versionamiento de las aplicaciones críticas en todos los equipos. h) Registro de log del inicio de sesión en las aplicaciones
Protección de los equipos (hardware)			
[HW] Protección de los Equipos Informáticos	[A.25]Robo [I.1] Fuego	L2 L1	a) Inventario de los equipos informáticos y redes b) Relación de los equipos informáticos asignado,

Cuadro 8. (Continuación)

Salvaguarda	Amenaza mitigada	Nivel	Descripción del Control / Salvaguarda
	[E.24] Caída del sistema por agotamiento de recursos	L0 L2	su distribución y responsable de uso. c) Rack ignifugo para proteger servidor d) Registro de incidentes por fallas hardware
[HW.CM] Cambios (actualizaciones y mantenimiento)	[I.3] Contaminación medioambiental [I.5] Avería de origen físico o lógico	L3 L1	e) Realizar mantenimiento periódico a los equipos de computo f) Llevar un registro del mantenimiento de equipos.
[HW.op] Operación	[A.11] Acceso no autorizado [A.7] Uso no previsto	L0	a) Documentación para el buen uso de los equipos.
Protección de las comunicaciones			
[COM.internet] Internet uso de acceso	[A.7] Uso no previsto [E.8] Difusión de software dañino	L0	a) Documentación para el buen uso del internet
[COM.DS] Segregación de las redes en dominios	[E.8] Difusión de software dañino [A.11] Acceso no autorizado [A.7] Uso no previsto	L0	a) Segregar las redes de acuerdo a cada una de las dependencias para asegurar la confidencialidad de la información.
[COM] Protección de las Comunicaciones	[I.8] Fallos de servicios de telecomunicaciones	L3 L5	a) Cableado organizado y asegurado b) Cables de energía separados de los cables de comunicaciones
Protección a los elementos auxiliares			
[AUX.AC] Climatización	[I.7]Condiciones inadecuadas de temperatura	L1	a) El centro de datos con un sistema de refrigeración adecuada
Cuadro 8. (Continuación)			b)
[AUX.power]Suministro eléctrico	[I*]Desastres Industriales [I.5]Avería de origen físico o lógico	L1	a) Realizar mantenimiento periódico al cableado eléctrico
[AUX] Elementos Auxiliares	[I.3]Contaminación	L3	a) Realizar mantenimiento periódico al cableado de

Cuadro 8. (Continuación)

Salvaguarda	Amenaza mitigada	Nivel	Descripción del Control / Salvaguarda
	medioambiental [I.5]Avería de origen físico o lógico		datos, generador eléctrico, aires acondicionados, sistema de vigilancia.
Seguridad física – Protección de las instalaciones			
[L.AC] Control de los accesos físicos	[A.11]Acceso no autorizado	L3	a) Asegurar el centro de datos de tal manera que solo sea accedida por el personal autorizado.
[L] Protección de las Instalaciones	[I.1] Fuego [I.*] Desastres Industriales	L2 L3 L4	a) Centro de datos ubicado en una zona aislada de productos inflamables b) Los productos altamente inflamables ubicarlos en la bodega externa. c) Detectores de incendios en todas las áreas donde hay equipos de cómputos.
Salvaguardas relativas al personal			
[PS] Gestión del Personal	[I.2] Daños por agua [I.5] Avería de origen físico o lógico [E.19]Fuga de Información [A.11]Acceso no autorizado [A.7]Uso no previsto [A.29]Extorsión [A.30]Ingeniería social (picaresca)	L0 L0 L0 L3 L0 L0	a) Prohibiciones para fumar, consumir alimentos y bebidas en los puestos de trabajo. b) Política de puesto de trabajo despejado y pantalla limpia c) Implementar sanciones cuando un empleado viole las políticas de seguridad de la información d) Informar a los empleados, clientes, contratistas o usuarios terceras partes los cambios de personal o de acciones operativas e) Durante la fase de contratación revisar los antecedentes (procuraduría, contraloría, policía nacional) de los aspirantes. f) Cláusulas de confidencialidad de la información en los contratos.
[PS.AT] Formación y concienciación	[E.1] Errores de los usuarios [E.2]Errores del administrador	L0	a) Capacitar periódicamente al personal sobre seguridad de la información

Cuadro 8. (Continuación)

Salvaguarda	Amenaza mitigada	Nivel	Descripción del Control / Salvaguarda
	[A.5] Suplantación de identidad [A.11]Acceso no autorizado [A.7]Uso no previsto [E.19]Fuga de Información [A.29]Extorsión [A.30]Ingeniería social (picaresca)	L2 L0	b) Notificar incidentes de seguridad de la información al administrador del sistema c) Capacitación formal al inicio y durante el empleo en los aplicativos críticos de negocio
Salvaguardas de tipo organizativo			
[G.plan] Planificación de la seguridad	[A.11]Acceso no autorizado [A.7]Uso no previsto [E.19]Fuga de Información [A.29]Extorsión [A.30]Ingeniería social (picaresca)	L0 L0 L0	a) Documento sobre políticas de seguridad b) Socialización periódica con los empleados sobre las políticas de seguridad c) Plan de contingencia informático
Continuidad de operaciones			
[BC.DRP] Plan de Recuperación de Desastres (DRP)	[I.1]Fuego [N.2]Daños por agua [N*]Desastres Naturales [L*]Desastres Industriales	L5	a) Plan de prevención y recuperación de desastre.

Fuente: autor

7.1.5 Estimación de los impactos y riesgos potencial. Esta tarea es conocida también como la estimación del riesgo, aquí se estima el impacto potencial al que se está expuesto todo el sistema sin las salvaguardas identificadas.

El impacto es igual al valor del activo por el nivel de degradación que causaría la materialización de la amenaza.

Impacto = Valor del activo x Nivel de Degradación

El riesgo es igual al impacto por la probabilidad de ocurrencia de una amenaza.

Riesgo = Impacto x Probabilidad de Ocurrencia

En esta investigación el análisis del impacto y riesgo se realiza utilizando la técnica cualitativa de análisis mediante tablas de doble entrada, los criterios de valoración son los descritos en los cuadros 9 y 10.

Cuadro 9. Valoración del Impacto

Impacto		Degradación				
		MB	B	M	A	MA
Valor	MA	M	M	MA	MA	MA
	A	B	M	A	A	A
	M	MB	B	M	M	M
	B	MB	MB	B	M	M
	MB	MB	MB	MB	B	M

Fuente: MAGERIT. Libro III Metodología. Versión 3. [En línea], [consultado el 22 de septiembre de 2017]. Disponible en internet: https://www.ccn-cert.cni.es/documentos-publicos/1793-magent

Cuadro 10. Criterios de estimación del Riesgo

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: MAGERIT. Libro III Metodología . Versión 3. [En línea], [consultado el 22 de septiembre de 2017]. Disponible en internet: https://www.ccn-cert.cni.es/documentos-publicos/1793-magent

Teniendo en cuenta las siguientes convenciones se proceden a estimar el riesgo potencial y a los que están expuestos los activos.

[D] = Dimensión de seguridad

[V] = Valor del activo

[N] = Nivel de degradación

[P] = Probabilidad de ocurrencia

[I] = Impacto

[R] = Riesgo

[NR] = Nivel de riesgo

[S] = Efectividad de las salvaguardas

{D} = Disponibilidad

{I} = Integridad de datos

{C} = Confidencial de datos

{A} = Autenticidad de los usuarios y de la información

{T}= Trazabilidad de los servicios y de los datos

Ténganse en cuenta que para el cálculo del impacto y riesgo se utilizan las tablas de doble entrada de los cuadros 9 y 10. Además:

Impacto = Valor del activo x Nivel de Degradación

[I] = [V] x [N]

Riesgo = Impacto x Probabilidad de Ocurrencia

[R] = [I] x [P]

Los resultados de la estimación están relacionados en el cuadro 11

Cuadro 11. Estimación de los impactos y riesgos Potenciales

Activo	**Amenaza**	**[D]**	**[V]**	**[N]**	**[P]**	**RIESGO POTENCIAL**		
						[I]	**[R]**	**[NR]**
[HW_HOST1] Servidor de Aplicaciones y Archivos	[N.1] Fuego	{D}	MA	MA	B	MA	MA	Extremo
	[N.2] Daños por agua	{D}	MA	MA	MB	MA	A	Intolerable
	[N*] Desastres Naturales	{D}	MA	MA	B	MA	MA	**Extremo**
	[I.2] Daños por agua	{D}	MA	MA	A	MA	MA	**Extremo**
	[I.5] Avería de origen físico o lógico	{D}	MA	A	M	MA	MA	**Extremo**
	[I.7] Condiciones inadecuadas de temperatura	{D}	MA	MA	A	MA	MA	**Extremo**
	[I.*] Desastres Industriales	{D}	MA	MA	M	MA	MA	**Extremo**
	[A.11] Acceso no autorizado	{I}	M	M	M	M	M	**Tolerable**
		{C}	A	A	M	A	A	**Intolerable**
[HW_HOST2] Servidor de Aplicaciones y Archivos	[N.1] Fuego	{D}	MA	MA	B	MA	MA	**Extremo**
	[N.2] Daños por agua	{D}	MA	MA	MB	MA	A	**Intolerable**
	[N*] Desastres Naturales	{D}	MA	MA	B	MA	MA	**Extremo**
	[I.2] Daños por agua	{D}	MA	MA	A	MA	MA	**Extremo**
	[I.5] Avería de origen físico o lógico	{D}	MA	A	M	MA	MA	**Extremo**
	[I.7] Condiciones inadecuadas de temperatura	{D}	MA	MA	A	MA	MA	**Extremo**
	[I.*] Desastres Industriales	{D}	MA	MA	M	MA	MA	**Extremo**
	[E.24] Caída del sistema por agotamiento de recursos	{D}	MA	MA	B	MA	MA	**Extremo**
	[A.11] Acceso no autorizado	{I}	M	M	M	M	M	**Tolerable**
		{C}	A	A	M	A	A	**Intolerable**

Cuadro 11. (Continuación)

Activo	Amenaza	[D]	[V]	[N]	[P]	RIESGO POTENCIAL		
						[I]	[R]	[NR]
[HW_PC] Equipos de informática personal	[N.1] Fuego	{D}	A	MA	B	A	A	Intolerable
	[N.2] Daños por agua	{D}	A	MA	MB	A	M	Tolerable
	[N*] Desastres Naturales	{D}	A	MA	B	A	A	Intolerable
	[I.2] Daños por agua	{D}	A	MA	A	A	MA	Extremo
	[I.5] Avería de origen físico o lógico	{D}	A	A	M	A	A	Intolerable
	[I.7] Condiciones inadecuadas de temperatura	{D}	A	M	M	A	A	Intolerable
	[I.*] Desastres Industriales	{D}	A	MA	M	A	A	Intolerable
	[E.24] Caída del sistema por agotamiento de recursos	{D}	A	MA	B	A	A	Intolerable
	[A.7] Uso no previsto	{D}	A	M	B	A	A	Intolerable
		{I}	A	M	B	A	A	Intolerable
		{C}	M	B	B	B	B	Aceptable
	[A.25] Robo	{D}	A	M	MB	A	M	Tolerable
		{C}	M	B	MB	B	MB	Aceptable
[HW_PRINT] Impresoras	[N.1] Fuego	{D}	M	MA	B	M	M	Tolerable
	[N.2] Daños por agua	{D}	M	MA	MB	M	B	Aceptable
	[N*] Desastres Naturales	{D}	M	MA	B	M	M	Tolerable
	[I.2] Daños por agua	{D}	M	M	A	M	A	Intolerable
	[I.5] Avería de origen físico o lógico	{D}	M	A	M	M	M	Tolerable
	[I.7] Condiciones inadecuadas de temperatura	{D}	M	M	M	M	M	Tolerable
[COM_PSTN] Red Telefónica	[I.8] Fallos de servicios de telecomunicaciones	{D}	A	MA	M	A	A	Intolerable
	[E.19] Fugas de Información	{C}	A	MA	B	A	A	Intolerable
	[A.7] Uso no	{D}	A	M	B	A	A	Intolerable

Cuadro 11. (Continuación)

Activo	Amenaza	[D]	[V]	[N]	[P]	RIESGO POTENCIAL		
						[I]	[R]	[NR]
	previsto	{I}	B	M	B	B	B	Aceptable
		{C}	A	M	B	A	A	Intolerable
[COM_WIFI] Red Inalámbrica	[I.8] Fallos de servicios de telecomunicaciones	{D}	M	MA	M	M	M	Tolerable
	[A.7] Uso no previsto	{D}	M	M	B	M	M	Tolerable
		{I}	B	MB	B	MB	MB	Aceptable
		{C}	M	M	B	M	M	Tolerable
[COM_LAN] Red LAN	[I.8] Fallos de servicios de telecomunicaciones	{D}	MA	MA	M	MA	MA	Extremo
	[A.11] Acceso no autorizado	{I}	A	M	M	A	A	Intolerable
		{C}	A	A	M	A	A	Intolerable
[COM_INTERNET] Red de acceso a Internet	[I.8] Fallos de servicios de telecomunicaciones	{D}	A	MA	M	A	A	Intolerable
	[A.7] Uso no previsto	{D}	A	M	B	A	A	Intolerable
		{I}	M	B	B	B	B	Aceptable
		{C}	A	M	B	A	A	Intolerable
[SW_ZAFIRO] Sistema de Inventario, Facturación y Compras	[I.5] Avería de origen físico o lógico	{D}	MA	A	M	MA	MA	Extremo
	[E.1] Errores de los usuarios	{D}	MA	A	M	MA	MA	Extremo
		{I}	A	A	A	A	MA	Extremo
		{C}	A	A	M	A	A	Intolerable
	[E.8] Difusión de software dañino	{D}	MA	MA	A	MA	MA	Extremo
		{I}	A	MA	A	A	MA	Extremo
		{C}	A	M	A	A	MA	Extremo
	[E.20] Vulnerabilidades de los programas (Software)	{D}	MA	M	M	MA	MA	Extremo
		{I}	A	M	M	A	A	Intolerable
		{C}	A	M	M	A	A	Intolerable
	[E.21] Errores Mantenimiento / actualización de programas (software)	{D}	MA	M	M	MA	MA	Extremo
		{I}	A	M	M	A	A	Intolerable
	[A.5] Suplantación de identidad	{I}	A	M	M	A	A	Intolerable
		{C}	A	M	M	A	A	Intolerable
		{A}	MA	M	M	MA	MA	Extremo
	[A.11] Acceso no autorizado	{I}	A	A	M	A	A	Intolerable
		{C}	A	A	M	A	A	Intolerable

Cuadro 11. (Continuación)

Activo	Amenaza	[D]	[V]	[N]	[P]	RIESGO POTENCIAL		
						[I]	[R]	[NR]
[SW_HELISA] Sistema de Información contable, nomina	[I.5] Avería de origen físico o lógico	{D}	A	A	M	A	A	Intolerable
	[E.1] Errores de los usuarios	{D}	A	M	M	A	A	Intolerable
		{I}	A	A	M	A	A	Intolerable
		{C}	A	A	M	A	A	Intolerable
	[E.8] Difusión de software dañino	{D}	A	MA	A	A	MA	Extremo
		{I}	A	A	A	A	MA	Extremo
		{C}	A	A	A	A	MA	Extremo
	[E.20] Vulnerabilidades de los programas (Software)	{D}	A	M	M	A	A	Intolerable
		{I}	A	M	M	A	A	Intolerable
		{C}	A	M	M	A	A	Intolerable
	[E.21] Errores Mantenimiento / actualización de programas (software)	{D}	A	M	M	A	A	Intolerable
		{I}	A	M	M	A	A	Intolerable
	[A.5] Suplantación de identidad	{I}	A	B	M	M	M	Tolerable
		{C}	A	M	M	A	A	Intolerable
		{A}	A	M	M	A	A	Intolerable
	[A.11] Acceso no autorizado	{I}	A	A	M	A	A	Intolerable
		{C}	A	A	M	A	A	Intolerable
[SW_SIFFOX] Sistema de Inventario, Facturación y Compras “SIFFOX”	[E.18] Destrucción de información	{D}	A	M	MA	A	MA	Extremo
	[A.5] Suplantación de identidad	{I}	A	M	M	A	A	Intolerable
		{C}	A	M	M	A	A	Intolerable
		{A}	A	M	M	A	A	Intolerable
	[A.11] Acceso no autorizado	{I}	A	A	M	A	A	Intolerable
		{C}	A	A	M	A	A	Intolerable
[SW_OTROS] “SisConPlus”, “LINKER”, “SIFEC”	[I.5] Avería de origen físico o lógico	{D}	M	A	M	M	M	Tolerable
	[E.18] Destrucción de información	{D}	M	M	MA	M	A	Intolerable
	[A.5] Suplantación de identidad	{I}	A	B	M	M	M	Tolerable
		{C}	M	M	M	M	M	Tolerable
		{A}	M	M	M	M	M	Tolerable
	[A.11] Acceso no autorizado	{I}	A	A	M	A	A	Intolerable
		{C}	M	A	M	M	M	Tolerable
[OS_WIN_2003] Sistema Operativo	[I.5] Avería de origen físico o lógico	{D}	M	A	M	M	M	Tolerable

Cuadro 11. (Continuación)

Activo	Amenaza	[D]	[V]	[N]	[P]	RIESGO POTENCIAL		
						[I]	[R]	[NR]
	[E.2] Errores del administrador	{D}	M	A	B	M	M	Tolerable
		{I}	M	A	B	M	M	Tolerable
		{C}	B	M	B	B	B	Aceptable
	[E.8] Difusión de software dañino	{D}	M	MA	A	M	A	Intolerable
		{I}	M	MA	A	M	A	Intolerable
		{C}	B	B	A	MB	B	Aceptable
	[E.21] Errores Mantenimiento / actualización de programas (software)	{D}	M	M	M	M	M	Tolerable
		{I}	M	M	M	M	M	Tolerable
	[A.11] Acceso no autorizado	{I}	M	A	M	M	M	Tolerable
		{C}	B	A	M	M	M	Tolerable
[OS_WIN_2012] Sistema Operativo	[I.5] Avería de origen físico o lógico	{D}	A	A	M	A	A	Intolerable
	[E.2] Errores del administrador	{D}	A	A	B	A	A	Intolerable
		{I}	A	A	B	A	A	Intolerable
		{C}	M	M	B	M	M	Tolerable
	[E.8] Difusión de software dañino	{D}	A	MA	A	A	MA	Extremo
		{I}	A	MA	A	A	MA	Extremo
		{C}	M	MA	A	M	A	Intolerable
	[E.21] Errores Mantenimiento / actualización de programas (software)	{D}	A	M	M	A	A	Intolerable
		{I}	A	M	M	A	A	Intolerable
	[A.11] Acceso no autorizado	{I}	A	A	M	A	A	Intolerable
		{C}	M	A	M	M	M	Tolerable
[OS_WIN_7_8_10]Sistema Operativo	[I.5] Avería de origen físico o lógico	{D}	M	A	M	M	M	Tolerable
	[E.1] Errores de los usuarios	{D}	M	M	M	M	M	Tolerable
		{I}	M	A	M	M	M	Tolerable
		{C}	A	B	M	M	M	Tolerable
	[E.8] Difusión de software dañino	{D}	M	MA	A	M	A	Intolerable
		{I}	M	M	A	M	A	Intolerable
		{C}	A	B	A	M	A	Intolerable

Cuadro 11. (Continuación)

Activo	Amenaza	[D]	[V]	[N]	[P]	RIESGO POTENCIAL		
						[I]	[R]	[NR]
	[E.21] Errores Mantenimiento / actualización de programas (software)	{D}	M	M	M	M	M	Tolerable
		{I}	M	M	M	M	M	Tolerable
	[A.5] Suplantación de identidad	{I}	M	M	M	M	M	Tolerable
		{C}	A	M	M	A	A	Intolerable
		{A}	M	M	M	M	M	Tolerable
	[A.11] Acceso no autorizado	{I}	M	A	M	M	M	Tolerable
		{C}	A	A	M	A	A	Intolerable
[S_WWW] Servicios de hosting	[E.24] Caída del sistema por agotamiento de recursos	{D}	B	MA	B	M	M	Tolerable
[S_EMAIL] servicio de email corporativos	[E.1] Errores de los usuarios	{D}	M	A	M	M	M	Tolerable
		{I}	A	MA	M	A	A	Intolerable
		{C}	A	MA	M	A	A	Intolerable
	[E.24] Caída del sistema por agotamiento de recursos	{D}	M	MA	B	M	M	Tolerable
	[A.5] Suplantación de identidad	{I}	A	B	M	M	M	Tolerable
		{C}	A	M	M	A	A	Intolerable
		{A}	M	M	M	M	M	Tolerable
	[A.11] Acceso no autorizado	{I}	A	A	M	A	A	Intolerable
		{C}	A	A	M	A	A	Intolerable
[AUX_AC] Aires acondicionados	[I.3] Contaminación medioambiental	{D}	M	M	A	M	A	Intolerable
[AUX_UPS] Sistemas de alimentación ininterrumpida	[I.3] Contaminación medioambiental	{D}	M	M	A	M	A	Intolerable
[AUX_SAFE] Caja Fuerte	[I.3] Contaminación medioambiental	{D}	M	B	A	B	M	Tolerable
	[A.25] Robo	{D}	M	M	MB	M	B	Aceptable
		{C}	B	M	MB	B	MB	Aceptable
[AUX_GEN] Generador Eléctrico	[I.3] Contaminación medioambiental	{D}	M	M	A	M	A	Intolerable
[AUX_CAB] Cableado	[I.3] Contaminación medioambiental	{D}	A	M	A	A	MA	Extremo
[AUX_SISVIG] Sistema de Vigilancia	[I.3] Contaminación medioambiental	{D}	M	B	A	B	M	Tolerable
	[A.11] Acceso no	{I}	A	A	M	A	A	Intolerable

Cuadro 11. (Continuación)

Activo	Amenaza	[D]	[V]	[N]	[P]	RIESGO POTENCIAL		
						[I]	[R]	[NR]
	autorizado	{C}	A	A	M	A	A	Intolerable
	[A.26] Ataque Destructivo	{D}	M	M	MB	M	B	Aceptable
[P_UI] Usuarios Internos	[E.19] Fugas de Información	{C}	A	MA	B	A	A	Intolerable
	[E.28] Indisponibilidad del personal	{D}	M	B	B	B	B	Aceptable
	[A.29] Extorsión	{D}	M	B	MB	B	MB	Aceptable
		{I}	A	B	MB	M	B	Aceptable
		{C}	A	M	MB	A	M	Tolerable
	[A.30] Ingeniería social (picaresca)	{D}	M	A	B	M	M	Tolerable
		{I}	M	A	B	M	M	Tolerable
		{C}	A	MA	B	A	A	Intolerable
[P_ADM] Administrador de Sistema	[E.19] Fugas de Información	{C}	A	MA	B	A	A	Intolerable
	[E.28] Indisponibilidad del personal	{D}	A	B	B	M	M	Tolerable
	[A.29] Extorsión	{D}	A	A	MB	A	M	Tolerable
		{I}	M	A	MB	M	B	Aceptable
		{C}	A	A	MB	A	M	Tolerable
	[A.30] Ingeniería social (picaresca)	{D}	A	M	B	A	A	Intolerable
		{I}	M	M	B	M	M	Tolerable
		{C}	A	A	B	A	A	Intolerable
[L_EDIFICIO] Edificio	[N.1] Fuego	{D}	MA	MA	B	MA	MA	Extremo
	[N.2] Daños por agua	{D}	MA	MA	MB	MA	A	Intolerable
	[N*] Desastres Naturales	{D}	MA	MA	B	MA	MA	Extremo
	[A.26] Ataque Destructivo	{D}	MA	M	MB	MA	A	Intolerable

Fuente: autor

7.1.6 Estimación de los impactos y riesgos residual. La estimación del impacto y riesgo residual se calcula de la misma forma como se calcula el impacto y riesgo potencial, pero teniendo en cuenta las salvaguardas identificadas, su nivel de implementación y la eficacia que tienen actualmente en el sistema. El valor de los activos no cambia, con la implementación de la salvaguarda puede cambiar el nivel de degradación que causaría en el sistema la amenaza o su probabilidad de ocurrencia, y de acuerdo esto se calcula el nuevo impacto y riesgo. El resultado de cálculo se describe en el cuadro 12.

Cuadro 12. Estimación de los impactos y riesgos Residuales

Activo	**Amenaza**	**[D]**	**[V]**	**[S]**	**[N]**	**[P]**	**RIESGO RESIDUAL**		
							[I]	**[R]**	**[NR]**
[HW_HOST1] Servidor de Aplicaciones y Archivos	[N.1] Fuego	{D}	MA	60%	M	B	MA	MA	Extremo
	[N.2] Daños por agua	{D}	MA	60%	M	MB	MA	A	Intolerable
	[N*] Desastres Naturales	{D}	MA	60%	M	B	MA	MA	Extremo
	[I.2] Daños por agua	{D}	MA	20%	MA	A	MA	MA	Extremo
	[I.5] Avería de origen físico o lógico	{D}	MA	40%	M	B	MA	MA	Extremo
	[I.7] Condiciones inadecuadas de temperatura	{D}	MA	10%	A	B	MA	MA	Extremo
	[I.*] Desastres Industriales	{D}	MA	80%	B	A	M	A	Intolerable
[HW_HOST1] Servidor de Aplicaciones y Archivos	[A.11] Acceso no autorizado	{I}	M	60%	M	M	M	M	Tolerable
		{C}	A	60%	M	M	A	A	Intolerable
[HW_HOST2] Servidor de Aplicaciones y Archivos	[N.1] Fuego	{D}	MA	60%	M	B	MA	MA	Extremo
	[N.2] Daños por agua	{D}	MA	60%	M	MB	MA	A	Intolerable
	[N*] Desastres Naturales	{D}	MA	60%	M	B	MA	MA	Extremo
	[I.2] Daños por agua	{D}	MA	20%	MA	A	MA	MA	Extremo
	[I.5] Avería de origen físico o lógico	{D}	MA	40%	M	B	MA	MA	Extremo
	[I.7] Condiciones inadecuadas de temperatura	{D}	MA	10%	A	B	MA	MA	Extremo

Cuadro 12. (Continuación)

Activo	Amenaza	[D]	[V]	[S]	[N]	[P]	RIESGO RESIDUAL		
							[I]	[R]	[NR]
	[I.*] Desastres Industriales	{D}	MA	80%	B	A	M	A	Intolerable
	[E.24] Caída del sistema por agotamiento de recursos	{D}	MA	60%	B	MB	M	B	Aceptable
	[A.11] Acceso no autorizado	{I}	M	60%	B	M	B	B	Aceptable
		{C}	A	60%	M	M	A	A	Intolerable
[HW_PC] Equipos de informática personal	[N.1] Fuego	{D}	A	60%	M	B	A	A	Intolerable
	[N.2] Daños por agua	{D}	A	60%	M	MB	A	M	Tolerable
	[N*] Desastres Naturales	{D}	A	60%	M	B	A	A	Intolerable
	[I.2] Daños por agua	{D}	A	20%	MA	A	A	MA	Extremo
	[I.5] Avería de origen físico o lógico	{D}	A	40%	M	B	A	A	Intolerable
	[I.7] Condiciones inadecuadas de temperatura	{D}	A	80%	B	MB	M	B	Aceptable
	[I.*] Desastres Industriales	{D}	A	80%	B	B	M	M	Tolerable
	[E.24] Caída del sistema por agotamiento de recursos	{D}	A	60%	MB	MB	B	MB	Aceptable
	[A.7] Uso no previsto	{D}	A	30%	M	B	A	A	Intolerable
		{I}	A	30%	M	B	A	A	Intolerable
		{C}	M	30%	B	B	B	B	Aceptable
	[A.25] Robo	{D}	A	80%	M	MB	A	M	Tolerable
		{C}	M	80%	B	MB	B	MB	Aceptable
[HW_PRINT] Impresoras	[N.1] Fuego	{D}	M	60%	M	B	M	M	Tolerable
	[N.2] Daños por agua	{D}	M	60%	M	MB	M	B	Aceptable
	[N*] Desastres Naturales	{D}	M	60%	M	B	M	M	Tolerable
	[I.2] Daños por agua	{D}	M	20%	MA	A	M	A	Intolerable
	[I.5] Avería de origen físico o lógico	{D}	M	40%	M	B	M	M	Tolerable
	[I.7] Condiciones inadecuadas de	{D}	M	80%	B	MB	B	MB	Aceptable

Cuadro 12. (Continuación)

Activo	Amenaza	[D]	[V]	[S]	[N]	[P]	RIESGO RESIDUAL		
							[I]	[R]	[NR]
	temperatura								
[COM_PSTN] Red Telefónica	[I.8] Fallos de servicios de telecomunicaciones	{D}	A	80%	B	MB	M	B	Aceptable
	[E.19] Fugas de Información	{C}	A	10%	MA	B	A	A	Intolerable
	[A.7] Uso no previsto	{D}	A	30%	M	B	A	A	Intolerable
		{I}	B	30%	B	B	MB	MB	Aceptable
		{C}	A	30%	M	B	A	A	Intolerable
[COM_WIFI] Red Inalámbrica	[I.8] Fallos de servicios de telecomunicaciones	{D}	M	80%	B	MB	B	MB	Aceptable
	[A.7] Uso no previsto	{D}	M	30%	M	M	M	M	Tolerable
		{I}	B	30%	MB	MB	MB	MB	Aceptable
		{C}	M	30%	M	M	M	M	Tolerable
[COM_LAN] Red LAN	[I.8] Fallos de servicios de telecomunicaciones	{D}	MA	80%	B	M	M	M	Tolerable
	[A.11] Acceso no autorizado	{I}	A	60%	B	M	M	M	Tolerable
		{C}	A	60%	M	M	A	A	Intolerable
[COM_INTERNET] Red de acceso a Internet	[I.8] Fallos de servicios de tele comunicaciones	{D}	A	80%	B	MB	M	B	Aceptable
	[A.7] Uso no previsto	{D}	A	30%	M	B	A	A	Intolerable
		{I}	M	30%	B	B	B	B	Aceptable
		{C}	A	30%	B	B	M	M	Tolerable
[SW_ZAFIRO] Sistema de Inventario, Facturación y Compras	[I.5] Avería de origen físico o lógico	{D}	MA	40%	M	B	MA	MA	Extremo
	[E.1] Errores de los usuarios	{D}	MA	30%	M	B	MA	MA	Extremo
		{I}	A	30%	M	A	A	MA	Extremo
		{C}	A	30%	M	B	A	A	Intolerable
	[E.8] Difusión de software dañino	{D}	MA	70%	A	MB	MA	A	Intolerable
		{I}	A	70%	A	MB	A	M	Tolerable
		{C}	A	70%	M	MB	A	M	Tolerable
	[E.20] Vulnerabilidades de los programas (Software)	{D}	MA	50%	M	M	MA	MA	Extremo
		{I}	A	50%	M	M	A	A	Intolerable
		{C}	A	50%	M	M	A	A	Intolerable

Cuadro 12. (Continuación)

Activo	Amenaza	[D]	[V]	[S]	[N]	[P]	RIESGO RESIDUAL		
							[I]	[R]	[NR]
	[E.21] Errores Mantenimiento / actualización de programas (software)	{D}	MA	40%	M	M	MA	MA	Extremo
		{I}	A	40%	M	M	A	A	Intolerable
	[A.5] Suplantación de identidad	{I}	A	40%	M	B	A	A	Intolerable
		{C}	A	40%	M	B	A	A	Intolerable
		{A}	MA	40%	M	M	MA	MA	Extremo
	[A.11] Acceso no autorizado	{I}	A	60%	M	M	A	A	Intolerable
		{C}	A	60%	M	M	A	A	Intolerable
[SW_HELISA] Sistema de Información contable, nomina	[I.5] Avería de origen físico o lógico	{D}	A	40%	M	B	A	A	Intolerable
	[E.1] Errores de los usuarios	{D}	A	30%	M	B	A	A	Intolerable
		{I}	A	30%	M	B	A	A	Intolerable
		{C}	A	30%	M	B	A	A	Intolerable
	[E.8] Difusión de software dañino	{D}	A	70%	A	B	A	A	Intolerable
		{I}	A	70%	A	B	A	A	Intolerable
		{C}	A	70%	A	B	A	A	Intolerable
	[E.20] Vulnerabilidades de los programas (Software)	{D}	A	50%	M	M	A	A	Intolerable
		{I}	A	50%	M	M	A	A	Intolerable
		{C}	A	50%	B	M	M	M	Tolerable
	[E.21] Errores Mantenimiento / actualización de programas (software)	{D}	A	40%	B	M	M	M	Tolerable
		{I}	A	40%	B	M	M	M	Tolerable
	[A.5] Suplantación de identidad	{I}	A	40%	B	M	M	M	Tolerable
		{C}	A	40%	M	M	A	A	Intolerable
		{A}	A	40%	M	M	A	A	Intolerable
	[A.11] Acceso no autorizado	{I}	A	60%	M	M	A	A	Intolerable
		{C}	A	60%	M	M	A	A	Intolerable
[SW_SIFFOX] Sistema de Inventario, Facturación y Compras “SIFFOX”	[E.18] Destrucción de información	{D}	A	0%	A	MA	A	MA	Extremo

Cuadro 12. (Continuación)

Activo	Amenaza	[D]	[V]	[S]	[N]	[P]	RIESGO RESIDUAL		
							[I]	[R]	[NR]
	[A.5] Suplantación de identidad	{I}	A	40%	M	M	A	A	Intolerable
		{C}	A	40%	M	M	A	A	Intolerable
		{A}	A	40%	M	M	A	A	Intolerable
	[A.11] Acceso no autorizado	{I}	A	60%	M	M	A	A	Intolerable
		{C}	A	60%	M	M	A	A	Intolerable
[SW_OTROS] “SisConPlus”, “LINKER”, “SIFEC”	[I.5] Avería de origen físico o lógico	{D}	M	40%	M	B	M	M	Tolerable
	[E.18] Destrucción de información	{D}	M	0%	M	MA	M	A	Intolerable
	[A.5] Suplantación de identidad	{I}	A	40%	B	M	M	M	Tolerable
		{C}	M	40%	M	M	M	M	Tolerable
		{A}	M	40%	M	M	M	M	Tolerable
	[A.11] Acceso no autorizado	{I}	A	60%	M	M	A	A	Intolerable
		{C}	M	60%	M	M	M	M	Tolerable
[OS_WIN_2003] Sistema Operativo	[I.5] Avería de origen físico o lógico	{D}	M	40%	M	B	M	M	Tolerable
	[E.2] Errores del administrador	{D}	M	10%	A	B	M	M	Tolerable
		{I}	M	10%	A	B	M	M	Tolerable
		{C}	B	10%	B	B	MB	MB	Aceptable
	[E.8] Difusión de software dañino	{D}	M	70%	A	B	M	M	Tolerable
		{I}	M	70%	A	B	M	M	Tolerable
		{C}	B	70%	B	B	MB	MB	Aceptable
	[E.21] Errores Mantenimiento / actualización de programas (software)	{D}	M	40%	M	M	M	M	Tolerable
		{I}	M	40%	M	M	M	M	Tolerable
	[A.11] Acceso no autorizado	{I}	M	60%	M	M	M	M	Tolerable
		{C}	B	60%	M	M	B	B	Aceptable
[OS_WIN_2012] Sistema Operativo	[I.5] Avería de origen físico o lógico	{D}	A	40%	M	B	A	A	Intolerable
	[E.2] Errores del administrador	{D}	A	10%	A	B	A	A	Intolerable
		{I}	A	10%	A	B	A	A	Intolerable
		{C}	M	10%	B	B	B	B	Aceptable

Cuadro 12. (Continuación)

Activo	Amenaza	[D]	[V]	[S]	[N]	[P]	RIESGO RESIDUAL		
							[I]	[R]	[NR]
	[E.8] Difusión de software dañino	{D}	A	70%	A	B	A	A	Intolerable
		{I}	A	70%	A	B	A	A	Intolerable
		{C}	M	70%	A	B	M	M	Tolerable
	[E.21] Errores Mantenimiento / actualización de programas (software)	{D}	A	40%	M	M	A	A	Intolerable
		{I}	A	40%	M	M	A	A	Intolerable
	[A.11] Acceso no autorizado	{I}	A	60%	M	M	A	A	Intolerable
		{C}	M	60%	M	M	M	M	Tolerable
[OS_WIN_7_8_10]Sistema Operativo	[I.5] Avería de origen físico o lógico	{D}	M	40%	M	B	M	M	Tolerable
	[E.1] Errores de los usuarios	{D}	M	30%	B	B	B	B	Aceptable
		{I}	M	30%	A	B	M	M	Tolerable
		{C}	A	30%	B	B	M	M	Tolerable
	[E.8] Difusión de software dañino	{D}	M	70%	A	B	M	M	Tolerable
		{I}	M	70%	M	B	M	M	Tolerable
		{C}	A	70%	B	B	M	M	Tolerable
	[E.21] Errores Mantenimiento / actualización de programas (software)	{D}	M	40%	M	M	M	M	Tolerable
		{I}	M	40%	M	M	M	M	Tolerable
	[A.5] Suplantación de identidad	{I}	M	40%	M	M	M	M	Tolerable
		{C}	A	40%	M	M	A	A	Intolerable
		{A}	M	40%	M	M	M	M	Tolerable
	[A.11] Acceso no autorizado	{I}	M	60%	M	M	M	M	Tolerable
		{C}	A	60%	M	M	A	A	Intolerable
[S_WWW] Servicios de hosting	[E.24] Caída del sistema por agotamiento de recursos	{D}	B	60%	MA	M	M	M	Tolerable
[S_EMAIL] servicio de email corporativos	[E.1] Errores de los usuarios	{D}	M	30%	A	B	M	M	Tolerable
		{I}	A	30%	A	B	A	A	Intolerable
		{C}	A	30%	A	B	A	A	Intolerable
	[E.24] Caída del sistema por agotamiento de recursos	{D}	M	60%	MA	M	M	M	Tolerable
	[A.5] Suplantación de identidad	{I}	A	40%	B	M	M	M	Tolerable
		{C}	A	40%	M	M	A	A	Intolerable
		{A}	M	40%	M	M	M	M	Tolerable
	[A.11] Acceso no	{I}	A	60%	M	M	A	A	Intolerable

Cuadro 12. (Continuación)

Activo	Amenaza	[D]	[V]	[S]	[N]	[P]	RIESGO RESIDUAL		
							[I]	[R]	[NR]
	autorizado	{C}	A	60%	M	M	A	A	Intolerable
[AUX_AC] Aires acondicionados	[I.3] Contaminación medioambiental	{D}	M	60%	MA	M	M	M	Tolerable
[AUX_UPS] Sistemas de alimentación ininterrumpida	[I.3] Contaminación medioambiental	{D}	M	60%	MA	M	M	M	Tolerable
[AUX_SAFE] Caja Fuerte	[I.3] Contaminación medioambiental	{D}	M	60%	MA	M	M	M	Tolerable
	[A.25] Robo	{D}	M	80%	B	MB	B	MB	Aceptable
		{C}	B	80%	B	MB	MB	MB	Aceptable
[AUX_GEN] Generador Eléctrico	[I.3] Contaminación medioambiental	{D}	M	60%	MA	M	M	M	Tolerable
[AUX_CAB] Cableado	[I.3] Contaminación medioambiental	{D}	A	60%	MA	A	A	MA	Extremo
[AUX_SISVIG] Sistema de Vigilancia	[I.3] Contaminación medioambiental	{D}	M	60%	MA	B	M	M	Tolerable
	[A.11] Acceso no autorizado	{I}	A	60%	M	M	A	A	Intolerable
		{C}	A	60%	M	M	A	A	Intolerable
	[A.26] Ataque Destructivo	{D}	M	80%	M	MB	M	B	Aceptable
[P_UI] Usuarios Internos	[E.19] Fugas de Información	{C}	A	10%	MA	B	A	A	Intolerable
	[E.28] Indisponibilidad del personal	{D}	M	0%	B	B	B	B	Aceptable
	[A.29] Extorsión	{D}	M	10%	B	MB	B	MB	Aceptable
		{I}	A	10%	B	MB	M	B	Aceptable
		{C}	A	10%	M	MB	A	M	Tolerable
	[A.30] Ingeniería social (picaresca)	{D}	M	10%	A	B	M	M	Tolerable
		{I}	M	10%	A	B	M	M	Tolerable
		{C}	A	10%	A	B	A	A	Intolerable
[P_ADM] Administrador de Sistema	[E.19] Fugas de Información	{C}	A	10%	MA	B	A	A	Intolerable
	[E.28] Indisponibilidad del personal	{D}	A	0%	B	B	M	M	Tolerable
	[A.29] Extorsión	{D}	A	10%	M	MB	A	M	Tolerable
		{I}	M	10%	M	MB	M	B	Aceptable
		{C}	A	10%	M	MB	A	M	Tolerable
	[A.30] Ingeniería social (picaresca)	{D}	A	10%	M	B	A	A	Intolerable
		{I}	M	10%	M	B	M	M	Tolerable
		{C}	A	10%	A	B	A	A	Intolerable
[L_EDIFICIO] Edificio	[N.1] Fuego	{D}	MA	60%	M	B	MA	MA	Extremo
	[N.2] Daños por agua	{D}	MA	60%	M	MB	MA	A	Intolerable

Cuadro 12. (Continuación)

Activo	Amenaza	[D]	[V]	[S]	[N]	[P]	RIESGO RESIDUAL		
							[I]	[R]	[NR]
	[N*] Desastres Naturales	{D}	MA	60%	M	B	MA	MA	Extremo
	[A.26] Ataque Destructivo	{D}	MA	80%	B	MB	M	B	Aceptable

Fuente: autor

7.1.7 Análisis de resultados. El anterior análisis de riesgos permitió identificar los activos de información que se encuentran en riesgo extremo e intolerable, los cuales requieren de una alta prioridad para el despliegue de las estrategias de prevención y de recuperación del plan de contingencia informático, estos activos críticos para la continuidad del negocio y con un alto riesgo son:

- [HW_HOST1] Servidor de Aplicaciones y Archivos: es el servidor de los sistemas de información Zafiro, Helisa y Siffox. Esencial para el proceso de gestión administrativa, contable, de venta y compra.

- [HW_HOST2] Servidor 2 de Aplicaciones y Archivos: es el servidor que contiene archivos históricos de la empresa y las aplicaciones de software que se usaron antes del año 2008.
- [HW_PC] Equipos de informática personal: son los 25 computadores que están distribuidos en las diferentes áreas de la empresa.

- [AUX_CAB] Cableado: es el cableado de datos que permite la comunicación entre los diferentes nodos de la red.

- [SW_ZAFIRO] Sistema de inventario, facturación y compras Zafiro: es el sistema donde actualmente se registra toda la información concerniente a la venta, compra, manejo de inventario, costos y cartera.

- [SW_HELISA] Sistema de contabilidad y nomina Helisa: es el sistema en que se registra toda la información referente a la nómina y la contabilidad de la empresa.

- [HW_PRINT] Impresoras: las impresoras son uno de los elementos necesarios para el proceso de gestión de ventas.

- [COM_PSTN] Red Telefónica: es necesaria para las posibles ventas, compras y gestión de cartera.

- [COM_LAN]Red LAN: su disponibilidad es de gran impacto. Es esencial para todos los procesos críticos de negocio.

- [L_EDIFICIO] Edificio: este activo hace referencia a las instalaciones físicas de la Ferretería Cesar.

Se encontró que existen amenazas que pueden afectar a estos activos, principalmente las siguientes:

- [N*] Desastres Naturales: históricamente en la ciudad no se han presentado terremotos, derrumbes, inundaciones o cualquier otro tipo de desastre natural. Sin embargo, no se puede garantizar que no llegue a ocurrir.

- [I.1] Fuego: en la empresa no se ha registrado un incendio. Sin embargo, se comercializan productos inflamables los cuales son almacenados en un lugar contiguo al centro de datos, si llegase a ocurrir un incendio el nivel de degradación seria alto para los activos de información y afectarían su disponibilidad. Se evidenció que existen extintores estratégicamente bien ubicados yal centro de datos cuenta con un sistema de detección de incendios. Sin embargo, las áreas de cartera y gestión de compras no tienen instalados el sistema de detección de incendios.

- [I.2] Daños por agua: es probable que pueda ocurrir un incidente debido a que los empleados tienen constantemente vasos de agua en sus puestos de trabajo.

Por otra parte, el centro de datos queda en frente de los baños de la empresa y en caso de una fuga podrían resultar afectados. En el techo de la sala de ventas pasa el ducto del aire acondicionado y los equipos de cómputos están ubicados debajo de ese ducto, generalmente hay gotas de agua en los escritorios. Ver imágenes en el anexo C.

- [I.3] Contaminación medioambiental: existe una gran acumulación de polvo en todo el equipamiento auxiliar. El cual puede afectar el funcionamiento y contribuir a su deterioro. Ver imágenes en el anexo C.

- [I.7] Condiciones inadecuadas de temperatura: El centro de datos tiene un inadecuado sistema de climatización, ver imagen en el anexo C. Los equipos de informática personal ubicados en el área de despacho de bodega no tienen una adecuada ventilación y están expuestos a altas temperaturas.

- [I.5] Avería de origen físico o lógico: dada las condiciones inadecuadas de temperatura al que está expuesto el centro de datos y la contaminación medio

ambiental del equipamiento auxiliar, es posible que las piezas de los equipos puedan deteriorarse, generando así una avería importante. En la sala de venta y despacho de bodega existen algunas CPU que están ubicadas directamente en el suelo.

- [E.1] Errores de los usuarios: pueden ocurrir errores involuntarios por parte de los usuarios de los sistemas de información, muchas veces por desconocimiento en el uso de los sistemas de información, sistema operativo y/o herramientas ofimáticas.

- [E.18] Destrucción de información: los antiguos sistemas de información se acceden mediante una unidad de red, estos sistemas fueron desarrollados en Visual Fox Pro y su base de datos se encuentra en la misma carpeta del ejecutable, toda la carpeta esta compartida y con permisos de borrado. La eliminación de cualquier archivo afectaría el funcionamiento de los mismos. Los empleados colocan en esa carpeta compartida del servidor, archivos que son importantes para sus funciones sin ninguna copia de los mismos.

- [E.20] Vulnerabilidades de los programas (Software): esta amenaza generalmente se presenta cuando se coloca en producción una nueva funcionalidad del sistema de información, que puede presentar errores de codificación y afectar la integridad de la información o la disponibilidad del mismo.

- [E.21] Errores Mantenimiento / actualización de programas (software): algunos sistemas operativos no tienen activo la opción de actualizaciones automáticas, para la corrección de vulnerabilidades. El sistema Zafiro trabaja con ejecutables locales en cada equipo y muchas veces no tienen la misma versión, ocasionando errores que ya están corregidos en versiones posteriores.

- [A.5] Suplantación de identidad: En ocasiones el personal interno comparte las claves de acceso a los sistemas de información y/o claves de los sistemas operativos. El personal acostumbra a levantarse de su sitio de trabajo dejando las sesiones de los programas abiertos.

De acuerdo a todo lo anterior se recomienda cambiar la ubicación del centro de datos, lejos de cualquier instalación de agua y de los elementos de bodega que puedan ser inflamables o productos que puedan producir algún derrame de líquido. Adquirir un aire acondicionado para el centro de datos. Adquirir las UPS para los equipos de cómputo que hacen falta. Alzar en los escritorios o adquirir soportes para las CPU que están ubicada en el suelo. Establecer la prohibición de consumo de alimentos y de bebidas en los puestos de trabajo. Diseñar e implementar políticas de seguridad de información. Y en general implementar todas las estrategias de prevención relacionadas en el apartado 8.1.2 del plan de contingencia que ayudarán a mitigar los riesgos a los que está expuesta la empresa.

8. DISEÑO DEL PLAN DE CONTINGENCIA

Una vez finalizado el proceso de análisis de riesgo, se procedió a realizar el tratamiento de los mismos. Los riesgos considerados como extremo, intolerable y tolerable fueron tenidos en cuenta para el despliegue de las estrategias de prevención y recuperación del plan de contingencia. El análisis de impacto estableció cuales son los procesos críticos de negocio, la prioridad de recuperación y el tiempo objetivo de recuperación (RTO) en caso de desastres. El primer paso fue establecer los roles y responsabilidades que tendrán el comité encargado de implementar y mantener el plan, luego se estableció las estrategias y procedimientos que puedan asegurar la continuidad de los servicios informáticos en caso de interrupción, se realizaron pruebas y por último se brindaron charlas desensibilización al personal para el buen uso y manejo del plan de contingencia.

8.1 DOCUMENTACIÓN DEL PLAN DE CONTINGENCIA

8.1.1 Establecimiento de roles y responsabilidades. A continuación, se describen los roles y responsabilidades de los integrantes del comité encargado de implementar y mantener el plan de contingencia.

8.1.1.1 Coordinador de continuidad y recuperación. Es el encargado de dirigir todas las actividades del plan de contingencia. Sus responsabilidades incluyen:

- Mantener las copias del plan resguardada y de su distribución.
- Velar por la difusión y capacitación de los empleados
- Velar por la seguridad del personal que actúa en el área del evento.
- Monitorear el estado de recuperación durante la contingencia
- Responsable de delegar la responsabilidad de actualizar, mantener y probar el plan.

8.1.1.2 Coordinador TI. Es la persona encargada de coordinar todo el proceso de recuperación tecnológica, basado en las estrategias y procedimientos del plan de contingencia.

Sus responsabilidades son:

- Declarar el estado de contingencia y la activación del mismo.

- Programar las pruebas del plan y velar por la documentación de los resultados

- Coordinar el proceso de recuperación tecnológica

- Vigilar y colaborar con los proveedores de servicios externos para la superación del estado de contingencia.

- Mantener la comunicación con los líderes de comunicaciones y recuperación de procesos durante una contingencia.

- Evaluar las estrategias de recuperación.

- Comunicar al comité sobre posibles riesgos de aspectos tecnológicos que puedan afectar la continuidad de las actividades de negocio, para que sean tenidas en cuenta en el mejoramiento del plan de contingencia.

8.1.1.3 Líderes en comunicaciones y recuperación de procesos. Son los encargados de mantener la continua comunicación entre los usuarios finales de los procesos con el coordinador TI y el coordinador de contingencia y recuperación. Se sugiere que para cada proceso crítico de negocio se asigne una persona.

Sus responsabilidades son:

- Comunicar al coordinador de TI sobre incidencias tecnológicas en el proceso asignado.

- Mantener comunicación constante durante el estado de contingencia con el coordinador TI, el coordinador de contingencia y los usuarios finales.

- Velar por la realización de pruebas del plan de contingencia.

- Velar por el cumplimiento de las medidas preventivas implementadas en los procesos que tiene asignado.

- Revisar el impacto causado en el área durante un incidente.

- Realizar las actividades que le sean asignadas durante la declaración de contingencia.

- Advertir sobre riesgos que puedan afectar la continuidad de los procesos críticos de negocios y socializarlos con el comité.

8.1.2 Identificación de estrategias. A continuación, se establecen las estrategias de prevención que permitirán aminorar la probabilidad de ocurrencia de un estado de contingencia. Además, las acciones que se deben tomar con el objetivo de restablecer las operaciones de negocio una vez que ocurra alguna interrupción o falla en los procesos críticos de negocio soportados por las TIC.

8.1.2.1 Estrategias preventivas. El siguiente listado de estrategias se establece para las amenazas que ponen en un riesgo crítico los activos de información.

Estrategias preventivas para desastre naturales [N*], [I.1] Fuego, [I.2] Daños por agua, [I.3] Contaminación medioambiental

- El centro de datos debe ubicarse lejos de cualquier instalación de agua y de los elementos de bodega que puedan ser inflamables o productos que puedan producir algún derrame de líquido.

- Contar con una relación visible de teléfonos de emergencia que incluya a todas las entidades de emergencia, bomberos, policía nacional, defensa civil, cruz roja, ambulancias y personal de la Ferretería de Cesar.

- Realizar capacitaciones periódicas para planes de gestión de riesgo y desastre.

- Realizar capacitaciones a los empleados para el uso de extintores. Llevar un control con la fecha de vencimiento de los extintores.

- Realizar mantenimiento anual al cableado eléctrico y cableado de datos.

- Realizar simulacros cuatrimestrales para la evacuación de las instalaciones en caso de emergencia.

- Prohibir fumar en las instalaciones de la empresa, con su respectiva señalización.

Estrategias preventivas para [I.5] Avería de origen físico o lógico, [I.7] Condiciones inadecuadas de temperatura

- Adquirir un aire acondicionado para el centro de datos.

- Adquirir UPS para los equipos de cómputo que no tengan.

- Las CPU que estén sobre el suelo deben ser alzada en los escritorios o adquirir soportes para las mismas.

- Realizar copias de seguridad de la base de datos de las aplicaciones críticas de la empresa con una frecuencia diaria. Mantener copias de seguridad fuera y dentro del edificio. Localizar las copias de seguridad dentro del edificio en un lugar seguro y lejos de canalizaciones de energía o agua.

Estrategias para [E.1] Errores de los usuarios, [E.18] Destrucción de información, [E.20] Vulnerabilidades de los programas (Software), [E.21] Errores Mantenimiento */ actualización de programas (software), [A.5] Suplantación de identidad*

- Prohibición de consumir alimentos y bebidas en los puestos de trabajo.

- Elaborar políticas y capacitar al personal sobre:

- La construcción de contraseñas seguras.

- La limitación de instalación de software no autorizado.

- Procedimientos para la gestión y solicitudes de la instalación de programas

- La realización de sus propias copias de seguridad de los datos almacenados en sus equipos y el aseguramiento de las copias de seguridad.

- Notificación sobre incidentes informáticos para que se tomen las medidas necesarias que ayuden a minimizarlos.

- Buen uso del internet y de los equipos informáticos

- Seguridad de la información

- Cerrar las sesiones activas cuando se ausenta del puesto de trabajo.

- Capacitación formal al inicio y durante el empleo en los aplicativos críticos de negocio

- Incluir en cláusulas de confidencialidad de la información en los contratos.

- Durante la fase de contratación revisar los antecedentes (procuraduría, contraloría, policía nacional) de los aspirantes.

- Crear perfiles de usuarios en todos los sistemas operativos y de mínimo permiso asignado.

- Asignar contraseña para el inicio de sesión de todos los sistemas operativos.

- Instalación de herramientas de antimalware y antispyware de software libre.

- Habilitar el escaneo automático del disco extraíble en el software antivirus.

- Habilitar las actualizaciones automáticas en los equipos personales con sistema operativo Windows. En el caso de servidores se activa la opción que descargue la actualización pero que el jefe de sistema las revise la compatibilidad con las aplicaciones críticas.

- Restringir el permiso de eliminación a las carpetas compartidas de los sistemas de información antiguos.

- Llevar un registro de las actualizaciones de las aplicaciones críticas de negocio.

- Firmar acuerdos de confidencialidad con los proveedores de software que requieran del envío de copias de la base de datos de la empresa.

- Inventario de todos los activos de información y los aplicativos instalados en cada uno de ellos.

- Deshabilitar puertos y servicios no requeridos en los sistemas operativos.

- Segregar las redes de acuerdo a cada una de las dependencias para asegurar la confidencialidad de la información.

- Colocar un ticket de color a los computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Los servidores tendrán un ticket de color rojo, de color amarillo a los equipos que contengan información importante para la empresa y de color verde a los equipos de contenidos normales.

8.1.2.2 Estrategias de recuperación

- Cada líder de recuperación de proceso cuente con un listado de contactos telefónicos para casos de contingencia.

- Contar con facturas con membrete y número de resolución de autorización de la DIAN, para los casos en que se requiera activar la contingencia de facturación manual.

- Imprimir trimestralmente el listado de precio para usarlo en caso que se requiera activar la facturación manual.

- Habilitar en el software de inventario y facturación Zafiro una opción para el descargue de las facturas con talonario manual.

- Documentar procedimientos para:

  - La recuperación de la base de datos de los sistemas información
  - La recuperación del sistema operativo del servidor
  - La recuperación del servidor causado por daño de hardware.
  - La recuperación por la suspensión del servicio de internet.
  - La recuperación de los sistemas de información críticos
  - La recuperación por un incidente en la red de datos.
  - La recuperación de daño en equipos personales.
  - El reporte de incidentes informático

- Contar con copia de seguridad de los sistemas de información en caso de eventualidades con el servidor. Copia de seguridad de los archivos elaboradas por los empleados en los casos de equipos de informática personal.

- Contar con un equipo pre-configurado con los requisitos necesarios para el buen funcionamiento del programa Zafiro, para que en el caso de un daño en el hardware del servidor este sea colocado en funcionamiento, aunque no pueda atender a todos los equipos clientes.

- En caso de evacuación se debe evacuar a los equipos informáticos de acuerdo a su prioridad, primero los equipos identificados con color rojo, luego los amarillos y por último los de color verde.

- Conservar instaladores de los aplicativos críticos y sistema operativos en un estante en el centro de datos.

- Traslado a un sitio alterno, esta estrategia solo será aplicada en el evento que el personal no pueda acceder a las instalaciones de la Ferretería Cesar por causa de un evento catastrófico, permitiendo la continuidad de los procesos críticos desde un sitio alterno de operación. En ese caso el tiempo de recuperación estará supeditado a la magnitud del evento que causó la contingencia y el número de procesos que active dicha contingencia.

8.1.2.3. Estrategias para el mantenimiento y mejoramiento del plan de contingencia

- Realizar auditorías internas al plan de contingencia anualmente.

- La actualización del plan de contingencia puede realizarse una vez finalice la auditoría interna o en los siguientes casos:

  - Adquisición de nuevos aplicativos.
  - Cambio en la red de datos
  - Cambio de instalaciones
  - Tercerización de procesos
  - Cambio de proveedores de servicios críticos

- Realizar pruebas anuales del plan de contingencia e informar al comité del resultado de las mismas.

- Realizar capacitación semestral del plan de contingencia.

- Realizar jornadas de sensibilización trimestrales de las medidas preventivas del plan de contingencia.

8.1.3 Tratamiento de incidentes. Ante un incidente informático cualquier empleado puede notificar al coordinador TI a través de cualquier medio de comunicación disponible. El coordinador TI evaluará el incidente y verificará si este afecta solo a una persona o a toda un área, y determinará si declara un estado de contingencia. Si el incidente no requiere de la activación del plan de contingencia el coordinador de TI lo gestionará y estimará su tiempo de resolución. Una vez solucionado debe diligenciar el formato de reporte de incidente (Anexo D) correspondiente a la causa de la falla, solución del incidente y medidas preventivas. Los formatos de incidentes deben ser resguardados y revisados en las auditorías internas.

8.1.4 Comité del plan de contingencia. El comité de plan de contingencia quedó conformado de acuerdo al Anexo E. El formato cuenta con los datos de contacto, para notificar de manera oportuna cualquier novedad. En algunos casos se contemplan suplentes, es de aclarar que los suplentes tienen las mismas responsabilidades de los titulares y estarán a cargo en caso que el titular llegue a faltar.

8.1.5 Activación del plan de contingencia. En el caso que el coordinador TI declare el estado de contingencia, activará el árbol de llamadas para notificar a los miembros del comité y seleccionará los planes de respuesta y recuperación que considere pertinentes. En el caso que no pueda cumplir con el tiempo objetivo de recuperación debe informar al coordinador de contingencia para que se activen los procedimientos de contingencia manual. Cuando la contingencia sea ocasionada por un desastre de gran magnitud el comité debe reunirse y determinar cuáles procedimientos activar del plan de contingencia.

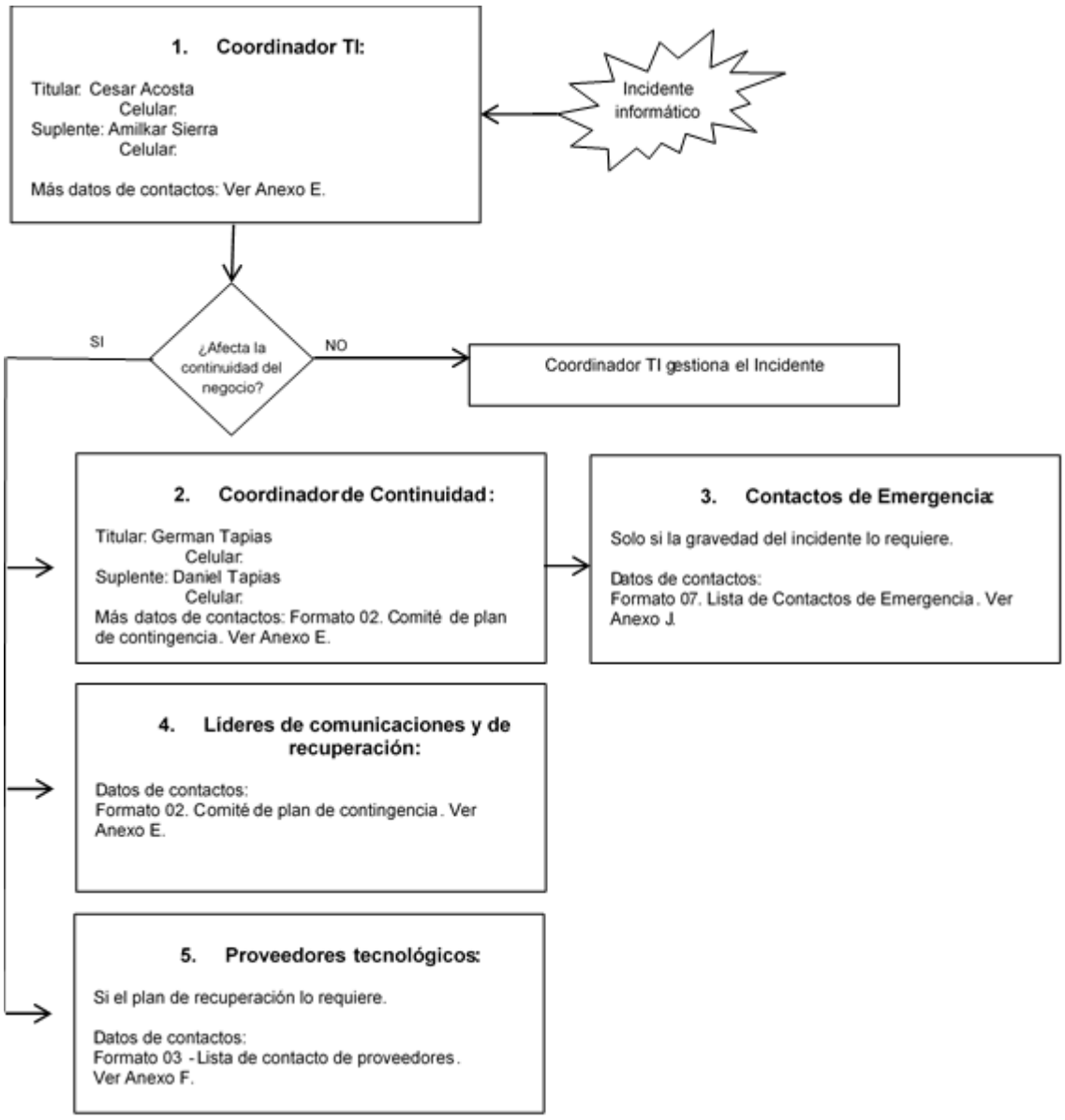
8.1.6 Árbol de llamadas o cascada telefónica. Cuando ocurre un incidente informático cualquier empleado puede notificar al Coordinador TI a través de cualquier medio de comunicación disponible (telefónico, correo electrónico, personal, etc.). Los datos de contactos se encuentran registrados en el formato "Lista de contacto del Comité Plan de Contingencia" (Ver anexo E). Dependiendo de la gravedad del incidente el Coordinador de TI determina si es necesaria la activación del plan de contingencia. En caso de ser necesaria la activación del plan, el coordinador TI notificará al coordinador de contingencia y a los líderes de comunicaciones y de recuperación.

El coordinador TI según el incidente determinará si debe contactar alguno de los proveedores de servicios informáticos contratado por la Ferretería Cesar. Para los datos de contacto remitirse al formato "Lista de Contacto de Proveedores" (Ver anexo F)

Si el incidente requiere del contacto de equipos de emergencia el coordinador de contingencia debe remitirse al formato "Lista de contacto de emergencia" (Ver anexo J).

En la figura 4 se representa gráficamente el árbol telefónico.

Figura 4. Árbol de llamadas o cascada telefónica



Fuente: autor

8.1.7 Lugar de reunión del comité. Las reuniones del comité de contingencia se realizarán en sala de juntas ubicada en el piso 1 de la Ferretería Cesar. Si no es posible acceder al sitio por la gravedad del incidente los miembros del comité determinarán el lugar de reunión.

8.1.8 Procedimientos contingencia por desastre natural, incendio o inundación.

Procedimiento contingencia por desastre natural, incendio o inundación

*Versión***:** 1.0 *Fecha de actualización***:** Octubre 2017

Objetivo: Ejecutar acciones que conlleven a una evacuación segura de las personas y bienes informáticos ante una contingencia ocasionada por un desastre natural, incendio o inundación.

Alcance: el procedimiento aplica para todas las personas que laboren en la empresa.

Acciones:

- Llevar a cabo todas las acciones requeridas por el plan de emergencia y desastres.

- Una vez que el personal está evacuado y en el punto de encuentro, se deberá coordinar con los brigadistas y el personal de emergencia la evacuación de los activos informáticos, en caso de ser posible.

- Los equipos informáticos deben ser evacuados de acuerdo a su prioridad, primero los equipos identificados con color rojo, luego los amarillos y por último los de color verde.

- Verificar el estado de los equipos, realizar el secado y limpieza de los mismos en caso de ser necesario.

- Una vez ha finalizado la contingencia, el coordinador TI debe realizar un reporte de los daños tecnológicos ocasionados por la contingencia.

- Luego de identificar los daños proceder a activar los planes de respuesta y recuperación que sean necesarios.

- En caso que las instalaciones no puedan ser accedidas por la magnitud catastrófica del evento se requerirá el traslado a un sitio alterno.

8.1.9 Procedimientos contingencia registro manual de las operaciones

Procedimiento contingencia registro manual de operaciones.
*Versión***:** 1.0 *Fecha de actualización***:** Octubre 2017
Objetivo: Ejecutar acciones que conlleven a la continuidad de las operaciones criticas de negocio.

Alcance: el procedimiento aplica en el caso que no se pueda reanudar la continuidad de las herramientas tecnológicas en un tiempo menor a 4 horas.

Acciones:

Facturación Manual:

- El líder del proceso de ventas debe informar a todo el personal la activación del procedimiento de facturación manual

- El líder del proceso de ventas deberá distribuir a cada vendedor las listas de precios impresas.

- El líder del proceso de ventas debe distribuir los 5 talonarios de facturación pre impreso.

- El jefe de bodegas registrará en el libro de entradas y salidas de bodega cada uno de los elementos que entren o salgan de la bodega, diligenciando toda la información que solicita el formato.

- El personal de caja debe registrar en libro de recaudo la información requerida por el formato.

- Las devoluciones de ventas deben ser registradas en libro de devoluciones de ventas.

- La contingencia manual termina cuando el coordinador TI indique la reanudación de las herramientas tecnológica que tuvieron falla.

- Una vez superada la contingencia todos los movimientos registrados, deben ser registrados en el programa ZAFIRO, a través de la opción de cargue de registro manuales.

Contabilización Manual:

- El líder del proceso de contabilidad debe informar al área de contabilidad que se pondrá en marcha la contabilización manual.

- En caso de contar con un computador que tenga Excel instalado, puede registrar los movimientos contables en el formato establecido por el programa Helisa para el registro de movimientos contables, para que luego pueda ser cargado a la contabilidad a través de la opción generación de documentos a través de archivos planos.

- Si no cuenta con un computador debe registrar los movimientos contables en el libro diario contable.

- Solicitar a la dirección la recarga del dongle para el acceso de internet y así puedan acceder a la página de la DIAN si es necesario.

- El líder del proceso de contabilidad informará al área cuando la contingencia haya sido superada, previa comunicación del coordinador TI.

- Una vez se ha superado la contingencia se debe registrar los movimientos manuales en el programa Helisa.

8.1.10 Procedimiento contingencia sitio alterno

*Fecha de actualización***:** Octubre 2017

*Versión***:** 1.0

Objetivo: Ejecutar acciones que conlleven a la continuidad de las operaciones criticas de negocio en un sitio alterno.

Alcance: el procedimiento aplica en el caso que no se pueda acceder a las instalaciones de la ferretería por un evento catastrófico y se requiera reanudar las operaciones desde un sitio alterno.

Acciones: *El Coordinador de continuidad y recuperación* debe realizar las siguientes acciones:

Activa la contingencia de sitio alterno una vez que se ha revisado que las instalaciones no pueden ser accedidas.

Define cual es el sitio alterno para mantener la continuidad de las operaciones de la empresa.

Convoca al personal y comunica al coordinador TI y los líderes de procesos y recuperación la activación del traslado a un sitio alterno.

Coordina el traslado del personal y del equipo informático.

8.1.10.1 El coordinador de TI. Realiza un chequeo del sitio y de acuerdo a las actividades de recuperación que se requiera en materia de TI, recomendará al coordinador de continuidad y recuperación si se activa el proceso de ventas manual.

- Realizar las adecuaciones en materia TI, activar los planes de respuesta y recuperación que sean necesarios.

- Comunicar a los al coordinador de continuidad y líderes cuando ya se encuentre listos los recursos TI.

El comité de contingencia

Evalúan cuando se puede realizar el desplazamiento a las instalaciones de la Ferretería.

Una vez se han desplazado al sitio original y se retornen las actividades a la normalidad se da por terminada la contingencia.

8.1.11 Procedimiento para la restauración de la base de datos ZAFIRO.

Procedimiento para la restauración de una copia de seguridad de la base de datos ZAFIRO.

*Fecha de actualización***:** Octubre 2017

*Versión***:** 1.0

Objetivo: Ejecutar acciones que conlleven a la restauración de una copia de seguridad de la base de datos ZAFIRO.

Alcance: el procedimiento aplica en el caso que se deba restaurar una copia de seguridad de la base de datos del programa ZAFIRO.

Acciones:

- El coordinador de TI, debe verificar que tiene instalado Oracle Server versión 11g y la instancia de base de datos “ZAFIRO”.

- Luego debe conectarse a la instancia con el usuario SYSTEM, a través del TOAD, SQL developer o SQL plus.

- Ejecutar las siguientes instrucciones para la creación del Tablespace ZGRAL:

CREATE TABLESPACE ZGRAL DATAFILE

'C:\app\FCESAR\oradata\ZAFIRO\ZGRAL.ORA' SIZE 100M AUTOEXTEND ON NEXT 50M MAXSIZE UNLIMITED LOGGING
ONLINE
PERMANENT
EXTENT MANAGEMENT LOCAL AUTOALLOCATE
BLOCKSIZE 8K
SEGMENT SPACE MANAGEMENT AUTO
FLASHBACK ON;

CREATE USER ZU_GRAL IDENTIFIED BY Z_FIRO_526_ DEFAULT TABLESPACE ZGRAL TEMPORARY TABLESPACE TEMP PROFILEDEFAULT ACCOUNT UNLOCK;

GRANT DBA TO ZU_GRAL WITH ADMIN OPTION;

ALTER USER ZU_GRAL DEFAULT ROLE ALL;

GRANT UNLIMITED TABLESPACE TO ZU_GRAL WITH ADMIN OPTION;

- Ubicarse en la ruta C:\app\FCESAR\admin\ZAFIRO\dpdump y crear un archivo .bat con la instrucción descrita a continuación:

- IMPDPZU_GRAL/Z_FIRO_526_@ZAFIRO
DUMPFILE=EXPDP_ZG_AUTOMATICA.DMPLOGFILE=IMP_ZG.log
REMAP_SCHEMA=ZU_GRAL:ZU_GRAL
REMAP_TABLESPACE=ZGRAL:ZGRAL

- “EXPDP_ZG_AUTOMATICA.DMP” es el nombre físico de la copia de la base de datos y debe ubicarse en la misma ruta del archivo .bat.

- Verificar en el archivo IMP_ZG.log que no haya errores. En caso de existir debe contactar al soporte técnico de la aplicación.

- Una vez recuperado el servicio de la base de datos, el coordinador de TI informará a los a los al coordinador de continuidad y líderes que ya se encuentre listos el servicio.

8.2 PLAN DE RESPUESTA Y RECUPERACIÓN SISTEMA DE INFORMACIÓN HELISA

Contingencia: **Sistema de información HELISA fuera de servicio**
*Versión***:** 1.0 *Fecha de actualización***:** Octubre 2017

Objetivo: Recuperar la continuidad del servicio del sistema de información Helisa.

Alcance: el procedimiento aplica para el escenario en que:
- Exista un daño físico o lógico en el servidor de aplicación
- Falle el servicio de base de datos del aplicativo

Recursos necesarios:
- Ultima copia de la Base de datos
- Contrato de soporte
- Administrador del servidor
- Coordinador TI
- Líder en comunicación y recuperación del proceso de ventas

Plan de Respuesta:

- El administrador del sistema debe hacer un diagnóstico para identificar la causa de la falla del servicio: inoperatividad de la base de datos o daño en el servidor de aplicaciones.

- En caso que se requiera de reinstalación de la aplicación Helisa o de la restauración de la copia de la base de datos, se debe contactar al soporte técnico de Helisa para realizar estas tareas, tal como lo indica el contrato de adquisición del software.

- De acuerdo al diagnóstico del servicio técnico de Helisa se puede decidir entre:

o Recuperar el servicio en el mismo servidor. De acuerdo a la falla, se puede llegar a reinstalar el motor de base de datos y restaurar la última copia de la base de datos o los procedimientos que sean necesario.

o Montar la última copia de la base de datos en el servidor alterno y re-direccionar los clientes al nuevo servidor.

- Si es una falla ocasionado por el daño del servidor físico o lógico, dependiendo del daño se decide entre:

o Recuperar el servidor arreglando la falla física o lógica y restaurar los servicios.

Ver el plan de repuesta y recuperación del Servidor 1.

o Montar la última copia de la base de datos en el servidor alterno y re-direccionar los clientes al nuevo servidor.

- Una vez se identifica la falla y el procedimiento a seguir se procede a comunicar al líder del proceso de contabilidad y nomina el tiempo estimado para arreglar la falla.

Exclusión: Si por algún motivo no está disponible el servidor alterno y no es posible recuperar el servicio en menos del tiempo objetivo de recuperación, puede proceder activar el plan de contabilización manual.

- Se verifica que el servidor opera adecuadamente.
- Se procede a restablecer el servicio.

Tiempo objetivo de recuperación: menos de 6 horas.

Plan de recuperación: En el evento que haya sido puesto en funcionamiento el servidor alterno o activado el procedimiento de contabilización manual, se procede a realizar los procedimientos requeridos para la normalización del servicio.

El administrador del sistema deberá registrar en el formato de incidencia las causas de la falla y las medidas preventivas que se deben tomar para que no vuelva a ocurrir.

Desactivar el plan de contingencia una vez se ha alcanzado la operación del servicio al 100%.

8.2.1 Plan de respuesta y recuperación sistema de información ZAFIRO

Contingencia: **Sistema de información ZAFIRO fuera de servicio**
*Versión***:** 1.0 *Fecha de actualización***:** Octubre 2017

Objetivo: Recuperar la continuidad del servicio del sistema de información Zafiro.

Alcance: el procedimiento aplica para el escenario en que:

- Exista un daño físico o lógico en el servidor de aplicación
- Falle el servicio de base de datos del aplicativo

Recursos necesarios:

- Ultima copia de la Base de datos
- Instaladores de la aplicación
- Administrador del servidor
- Coordinador TI
- Líder en comunicación y recuperación del proceso de ventas

Plan de Respuesta:

- El administrador del sistema debe hacer un diagnóstico para identificar la causa de la falla del servicio: inoperatividad de la base de datos o daño en el servidor de aplicaciones.

- Si es una falla del servicio de base de datos de acuerdo al diagnóstico se puede decidir entre:

  - Recuperar el servicio en el mismo servidor. De acuerdo a la falla, se puede llegar a reinstalar el motor de base de datos y restaurar la última copia de la base de datos o los procedimientos que sean necesario.

  - Montar la última copia de la base de datos en el servidor alterno y re-direccionar los clientes al nuevo servidor.

- Si es una falla ocasionado por el daño del servidor físico o lógico, dependiendo del daño se decide entre:

  - Recuperar el servidor arreglando la falla física o lógica y restaurar los servicios. Ver el plan de respuesta y recuperación Servidor 1.

  - Montar la última copia de la base de datos en el servidor alterno y re-direccionar los clientes al nuevo servidor.

- Una vez se identifica la falla y el procedimiento a seguir se procede a comunicar al líder del proceso de ventas el tiempo estimado para arreglar la falla, para que junto con el comité del plan de contingencia decidan las excusas que van a presentar a los clientes.

Exclusión: Si por algún motivo no está disponible el servidor alterno y no es posible recuperar el servicio en menos del tiempo objetivo de recuperación, puede proceder activar el plan de servicio de venta manual.

- Se verifica que el servidor opera adecuadamente.
- Se procede a restablecer el servicio.

Tiempo objetivo de recuperación: menos de 4 horas.

Plan de recuperación:

- En el evento que haya sido puesto en funcionamiento el servidor alterno o activado el procedimiento de facturación manual, se procede a realizar los procedimientos requeridos para la normalización del servicio.

- El administrador del sistema deberá registrar en el formato de incidencia las causas de la falla y las medidas preventivas que se deben tomar para que no vuelva a ocurrir.

- Desactivar el plan de contingencia una vez se ha alcanzado la operación del servicio al 100%.

8.2.2 Plan de respuesta y recuperación daño en los equipos de informática personal

Contingencia: **Daño en los equipos de informática personal**

*Versión***:** 1.0 *Fecha de actualización***:** Octubre 2017

Objetivo: Restaurare equipo de informática personal.

Alcance: el procedimiento aplica para el escenario en que:

- Exista un daño físico o lógico en el equipo de informática personal.

Recursos necesarios:

- Documentación sobre la configuración de los equipos personales.
- Instaladores de aplicaciones y sistema operativo.
- Hoja de vida del equipo informático. (Anexo G)
- Administrador de sistema
- Coordinador TI
- Copia de la información del equipo

Plan de Respuesta:

- El administrador de sistema debe hacer un diagnóstico para identificar la causa de la falla del equipo personal.

- Si es un daño físico o lógico de algunos de los componentes se tomará la pieza de remplazo del stock. Si es un daño del sistema operativo debe proceder a reinstalarlo e instalar las aplicaciones que se requieren de acuerdo al formato

- Una vez se ha restablecido el funcionamiento del equipo, se procede a restaurar la copia de la información del equipo en caso que se requiera.

- Realizar las configuraciones pertinentes de acuerdo a la hoja de vida del equipo informático.

- Se verifica que el equipo opera correctamente.

- Se restablece el equipo a la persona a cargo.

Tiempo objetivo de recuperación: menos de 4 horas.

Plan de recuperación:

- El administrador del sistema deberá registrar en el formato de incidencia las causas de la falla y las medidas preventivas que se deben tomar para que no vuelva a ocurrir

- Desactivar el plan de contingencia una vez se ha alcanzado la operación del servicio al 100%.

8.2.3 Plan de respuesta y recuperación del servidor de aplicaciones

Contingencia: **Servidor de aplicaciones fuera de servicio**

*Versión***:** 1.0 *Fecha de actualización***:** Octubre 2017

Objetivo: Recuperar la continuidad del servidor de aplicaciones.

Alcance: el procedimiento aplica para el escenario en que:

- Exista un daño físico o lógico en el servidor de aplicación

Recursos necesarios:

- Hoja de vida del equipo informático
- Instaladores del sistema operativo
- Instaladores de las aplicaciones
- Administrador del sistema

- Coordinador TI
- Líder en comunicación y recuperación del proceso de ventas

Plan de Respuesta:

- El administrador del sistema debe hacer un diagnóstico para identificar la causa de la falla del servicio: inoperatividad del sistema operativo o daño en alguna pieza del servidor

- Si es una falla del servicio del sistema operativo puede escoger entre:

○ Recuperar el servicio en el mismo servidor volviendo a un punto de restauración; si no es posible, realizar una reinstalación del sistema operativo. Restaurar los servicios de acuerdo a la hoja de vida del equipo informático.

○ Montar la última copia de la base de datos en el servidor alterno y re-direccionar los clientes al nuevo servidor. Ver los planes de respuesta sistema de información HELISA fuera de servicio y sistema de información ZAFIRO fuera de servicio.

- Si es una falla ocasionado por el daño del servidor físico o lógico, dependiendo del daño se decide entre:

○ Recuperar el servidor arreglando la falla física o lógica y restaurar los servicios de acuerdo a la hoja de vida del equipo informático

○ Montar la última copia de la base de datos en el servidor alterno y re-direccionar los clientes al nuevo servidor. Ver los planes de respuesta sistema de información HELISA fuera de servicio y sistema de información ZAFIRO fuera de servicio.

- Una vez se identifica la falla y el procedimiento a seguir se procede a comunicar al líder del proceso de ventas el tiempo estimado para arreglar la falla, para que junto con el comité del plan de contingencia decidan las excusas que van a presentar a los clientes.

Exclusión: Si por algún motivo no está disponible el servidor alterno y no es posible recuperar el servicio en menos del tiempo objetivo de recuperación, puede proceder activar el plan de servicio de venta manual.

- Se verifica que el servidor opera adecuadamente.
- Se procede a restablecer el servicio.

Tiempo objetivo de recuperación: menos de 4 horas.

Plan de recuperación:

- En el evento que haya sido puesto en funcionamiento el servidor alterno o activado el procedimiento de facturación manual, se procede a realizar los procedimientos requeridos para la normalización del servicio.

- El administrador del sistema deberá registrar en el formato de incidencia las causas de la falla y las medidas preventivas que se deben tomar para que no vuelva a ocurrir.

- Desactivar el plan de contingencia una vez se ha alcanzado la operación del servicio al 100%.

8.2.4 Plan de respuesta y recuperación red LAN fuera de servicio

Contingencia: **Red LAN fuera de servicio**

*Versión***:** 1.0 *Fecha de actualización***:** Octubre 2017

Objetivo: Recuperar la continuidad del servicio de la red LAN.

Alcance: el procedimiento aplica para el escenario en que:

- Exista un daño físico o lógico en uno o varios de los componentes de la red LAN

Recursos necesarios:

- Diagrama de la red LAN.
- Documentación sobre la configuración de la red
- Administrador de la red
- Coordinador TI
- Líderes en comunicación y recuperación de procesos

Plan de Respuesta:

1. El administrador de la red debe hacer un diagnóstico para identificar la causa de la falla del servicio.

2. Si es un daño físico o lógico de algunos de los componentes se tomará la pieza de remplazo del stock.

Exclusión: Si por algún motivo no está disponible la pieza de remplazo y no es posible recuperar el servicio en menos del tiempo objetivo de recuperación, puede proceder activar el plan de servicio de venta manual.

- Una vez se identifica la falla y el procedimiento a seguir se procede a comunicar a los líderes del proceso el tiempo estimado para arreglar la falla.

- Realizar la instalación y configuración de la pieza.
- Se verifica que la pieza de remplazo esté operando correctamente.
- Se procede a restablecer el servicio.

Tiempo objetivo de recuperación: menos de 4 horas.
Plan de recuperación:

- El administrador del sistema deberá registrar en el formato de incidencia las causas de la falla y las medidas preventivas que se deben tomar para que no vuelva a ocurrir.

- Desactivar el plan de contingencia una vez se ha alcanzado la operación del servicio al 100%.

8.2.5 Plan de respuesta y recuperación Internet

Contingencia: **Internet fuera de servicio**

*Versión***:** 1.0 *Fecha de actualización***:** Octubre 2017

Objetivo: Recuperar la continuidad del servicio de Internet

Alcance: el procedimiento aplica para el escenario en que:

- Exista un daño físico o lógico en alguno de los componentes de conexión a internet.

Recursos necesarios:

- Números de contacto de los proveedores del servicio. Anexo F
- Documentación sobre la configuración de la red
- Administrador de la red
- Coordinador TI
- Líderes en comunicación y recuperación de procesos

Plan de Respuesta:

- El administrador de la red debe hacer un diagnóstico para identificar la causa de la falla del servicio.

- Llamar al soporte técnico del servicio de internet. Los números de contacto los encuentra en el formato de contactos de proveedores. Anexo F

- Recuperar el servicio empleando el otro canal de servicio de internet.

- Con la ayuda del soporte técnico se debe proceder a restablecer el servicio

- Se valida la configuración y se realizan las pruebas del restablecimiento del servicio. Si la prueba es insatisfactoria volver al paso 4.

- Servicio restablecido. Informar a los líderes de procesos que el servicio fue restablecido

Tiempo objetivo de recuperación: menos de 24 horas.

Plan de recuperación:

- El administrador del sistema deberá registrar en el formato de incidencia las causas de la falla y las medidas preventivas que se deben tomar para que no vuelva a ocurrir.

- Desactivar el plan de contingencia una vez se ha alcanzado la operación del servicio al 100%.

8.2.6 Plan de respuesta y recuperación red inalámbrica

Contingencia: **Red Inalámbrica fuera de servicio**

*Versión***:** 1.0 *Fecha de actualización***:** Octubre 2017

Objetivo: Recuperar la continuidad del servicio de la red inalámbrica.

Alcance: el procedimiento aplica para el escenario en que:

- Exista un daño físico o lógico en uno o varios de los componentes de la red inalámbrica

Recursos necesarios:

- Diagrama de la red LAN.
- Documentación sobre la configuración de la red
- Administrador de la red
- Coordinador TI
- Líderes en comunicación y recuperación de procesos

Plan de Respuesta:

- El administrador de la red debe hacer un diagnóstico para identificar la causa de la falla del servicio.

- Si es un daño físico o lógico de algunos de los componentes se tomará la pieza de remplazo del stock.

Exclusión: Si por algún motivo no está disponible la pieza de remplazo se debe proceder a realizar la gestión de compra de la pieza.

- Realizar la instalación y configuración de la pieza.
- Se verifica que la pieza de remplazo esté operando correctamente.
- Se procede a restablecer el servicio.

Tiempo objetivo de recuperación: menos de 24 horas.

Plan de recuperación:

- El administrador del sistema deberá registrar en el formato de incidencia las causas de la falla y las medidas preventivas que se deben tomar para que no vuelva a ocurrir.

- Desactivar el plan de contingencia una vez se ha alcanzado la operación del servicio al 100%.

8.2.7 Mantenimiento del plan de contingencia. El responsable del mantenimiento y documentación del plan de respuesta y recuperación de TIC es el Coordinador TI.

Las auditorías internas al plan de contingencia se realizarán anualmente.
La actualización del plan de contingencia puede realizarse una vez finalice la auditoría interna o en los siguientes casos: se adquieran nuevos aplicativos, exista un cambio en la red de datos, ocurra un cambio de instalaciones, uno o varios procesos sean tercerizados o exista un cambio de proveedores de servicios

críticos. El plan de contingencia contiene un control de cambios como lo muestra el Tabla 4 donde se incluye la versión, fecha y descripción del cambio o modificación, el cual debe ser diligenciado cada vez que se realice alguna modificación al plan de contingencia informático.

Tabla 4. Control de cambios del plan de contingencia

Versión	Fecha	Descripción de la modificación
1.	Octubre 2017	Creación del documento.

Fuente: autor.

8.2.8 Pruebas o simulacros del plan de contingencia. Anualmente se realizará una prueba o simulacro del plan de contingencia informático. La prueba puede realizarse de dos maneras:

- Una prueba de escritorio: que consistirá en crear un escenario y el personal escribirá en el papel las estrategias y procedimientos a seguir. Esta prueba puede ser realizada en una sala de conferencia.

- Una prueba real con previo aviso al personal: se puede simular un incidente informático y ejecutar las estrategias y procedimientos de recuperación.

Para la realización de pruebas es necesario que se diligencie el formato de plan de pruebas ver Anexo K.

Durante la fase de pruebas el personal deberá notificar el incidente simulado al coordinador TI, quien de acuerdo a las circunstancias activará los planes que considere necesarios y llevará a cabo las acciones requerida para mantener la continuidad de los procesos en los tiempos objetivos de recuperación.

Una vez finalizada la prueba se hará un acta de reunión donde se escribirán las conclusiones de las pruebas y las acciones que mejoren las estrategias de continuidad. Se informará al comité el resultado de las mismas. Las actas de reunión deben ser resguardadas y tenidas en cuenta para las mejoras continuas al plan de contingencia.

En el cuadro 13 se describe el guion de pruebas para la simulación de una falla catastrófica del servidor de aplicaciones que requiera la puesta en marcha del servidor de contingencia.

Cuadro 13. Guion de pruebas de continuidad de negocio

No.	Actividad	Responsable	Duración ejecución (Minutos)	Resultados
Actividades previas a la realización de la prueba				
1	Notificar a los líderes en comunicaciones y recuperación de procesos sobre la realización de la prueba.	Coordinador TI	5	
2	Notificar a los proveedores del sistema Zafiro y Helisa sobre la realización de la prueba, para su participación y asistencia técnica remota.	Coordinador TI	5	
3	Comprobar que el servidor de contingencia tenga instalado y en funcionamiento Oracle Express.	Coordinador TI	5	
4	Comprobar la existencia de las tablestacas necesarias para la importación de la copia de la base de datos.	Coordinador TI	3	
5	Verificar en el firewall de Windows la regla para permitir el servicio del puerto 1521 de Oracle.	Coordinador TI	3	
6	Comprobar la comunicación entre los clientes y el servidor de contingencia.	Coordinador TI	10	
Actividades durante la realización de la prueba				
1	Comunicar al coordinador de TI sobre incidencias tecnológicas en el proceso asignado.	Líderes en comunicaciones y recuperación de procesos	5	
2	Apagar el servidor de aplicaciones	Coordinador TI	3	
3	Encender el servidor de contingencia	Coordinador TI	4	
4	Realizar la importación de la copia de respaldo de la base de datos Zafiro.	Coordinador TI	15	
5	Realizar pruebas de conectividad y funcionamiento al programa Zafiro.	Coordinador TI	10	
6	Si las pruebas fallan y se ha superado el tiempo objetivo de recuperación. El coordinador TI debe notificar a los líderes en comunicaciones y recuperación de procesos, la puesta en marcha del procedimiento de contingencia de registro manual de operaciones.	Coordinador TI		
7	Una vez que las pruebas sean satisfactoria el coordinador TI notifica a los líderes en	Coordinador TI	5	

Cuadro 13. (Continuación)

No.	Actividad	Responsable	Duración ejecución (Minutos)	Resultados
	comunicaciones y recuperación de procesos sobre la reanudación del servicio Zafiro.			
8	Los líderes en comunicaciones y recuperación de procesos deberán actualizar los consecutivos de los últimos documentos generados en el programa Zafiro de su área correspondiente.	Líderes en comunicaciones y recuperación de procesos	5	
9	Realizar actividades de recuperación y pruebas del sistema Helisa de acuerdo a las instrucciones del servicio técnico.	Coordinador TI	30	
10	Realizar monitoreo del comportamiento del servidor de contingencia y de la prueba en general.	Coordinador TI	20	
Actividades de finalización de la prueba				
11	Notificar a los líderes en comunicaciones y recuperación de procesos sobre la finalización de la prueba.	Coordinador TI	5	
12	Apagar el servidor de contingencia.	Coordinador TI	5	
13	Encender el servidor de producción.	Coordinador TI	5	
14	Realizar pruebas de conectividad y funcionamiento al programa Zafiro y Helisa.	Coordinador TI	10	
15	Revisar y elaborar las conclusiones sobre el impacto causado en cada área durante la contingencia.	Líderes en comunicaciones y recuperación de procesos	15	
16	Elaborar las recomendaciones de mejora del proceso en caso que haya lugar y diligenciar las conclusiones generales del proceso, en el formato de pruebas de contingencia (Anexo K)	Coordinador TI	20	
	Duración total de la prueba:		188	

Fuente: autor.

8.3 SOCIALIZACIÓN, PRUEBAS Y CAPACITACIÓN

El plan de contingencia inicialmente fue socializado con los directivos y los ingenieros de sistemas que prestan asesoría a la empresa, se presentó el análisis de riesgos, las estrategias de prevención y recuperación diseñadas para el plan de contingencia. Los directivos manifestaron su agrado y alto compromiso con el proyecto, autorizaron a sus ingenieros para invertir en la compra del aire acondicionado para el centro de datos, el servidor alterno, el traslado del centro de datos a una mejor ubicación dentro del edificio, la adquisición de las UPS que hacen falta y los elementos necesarios para el mantenimiento y organización de todo el cableado de datos.

En compañía del ingeniero Amilkar Sierra Romano encargado del área de soporte de la Ferretería Cesar, se realizó prueba controlada sobre los procedimientos de respuesta y recuperación que debe llevar a cabo el área de sistemas. Se elaboró un guion de pruebas para la recuperación del sistema Zafiro, en un servidor alterno (ver cuadro 13) la prueba fue exitosa y el ingeniero aprobó los procedimientos planteados.

También, se realizó capacitación a todos los empleados de la Ferretería Cesar, los cuales comprendieron sus acciones en caso de una contingencia y se socializaron las estrategias preventivas. Durante la capacitación el gerente Germán Tapias, manifestó a todos sus empleados su apoyo con el proyecto y solicitó a los empleados toda la colaboración y compromiso para el cumplimiento de las estrategias preventivas diseñadas. Se anexan evidencias en los anexos N y O.

5. CONCLUSIONES

El plan de contingencia informático diseñado para la Ferretería Cesar describe una guía paso a paso de lo qué se debe hacer para mantener las operaciones y restablecer los servicios críticos de la compañía rápidamente ante un incidente que afecte los recursos tecnológicos o los activos de información de la empresa.

Durante el diseño se identificaron los procesos críticos de negocio que están soportados por las TIC y se realizó el análisis riesgo utilizando la metodología Magerit, centrando el análisis en los activos que son de importancia para la continuidad de las actividades de negocio. El análisis de riesgos realizado permitió determinar los activos de información más relevantes de la empresa, identificar las amenazas a los que estaban expuestos, estimar las salvaguardas y realizar todas las valoraciones correspondientes. De esta manera se identificaron los activos de información que se encontraban en riesgo y que requerían de una alta prioridad para el despliegue de las estrategias de prevención y de recuperación del plan de contingencia informático.

De acuerdo a los resultados del análisis de riesgos se establecieron varias estrategias de prevención que permiten a la empresa disminuir la probabilidad de un estado de contingencia.

En común acuerdo con la gerencia se definió un tiempo objetivo de recuperación tal como lo indica estándar ISO / IEC22301 y se definieron los procedimientos para recuperase en el menor tiempo posible teniendo en cuenta las directrices del estándar ISO / IEC 27031.

Se realizó la sensibilización del personal para promover el buen uso y manejo del plan de contingencia. Durante el desarrollo de este proyecto se evidenció la escasa formación de los empleados acerca de aspectos importantes de la seguridad de la información, y se percibió por parte de la gerencia y directivas de la empresa una alta disposición para mejorar en este aspecto. Desde que se realizó la socialización inicial del análisis de riesgos informático, las estrategias preventivas y los procedimientos de recuperación ante incidentes, el proyecto conto con gran acogida por parte de la dirección, la cual destinó muchos esfuerzos y recursos económicos para lograr que la propuesta fuera implementada con total éxito.

En conclusión, el diseño e implementación del plan de contingencia informático en la Ferretería Cesar obtuvo un resultado positivo. La gerencia conoció los riesgos a los que están expuestos, apoyó y promovió medidas preventivas que ayuden a mitigarlos y se creó conciencia y compromiso entre los empleados sobre seguridad de la información. Hoy la Ferretería Cesar cuenta con una guía

planificada para la recuperación ágil y ordenada de la infraestructura tecnológica que soporta los procesos críticos del negocio.

6. RECOMENDACIONES

La gerencia deberá continuar promoviendo la importancia de la seguridad de la información y a mediano plazo considerar contar con un plan de continuidad de negocio para toda la empresa.

El comité del plan de contingencia debe velar porque este plan sea actualizado y probado periódicamente para que sea eficaz en el momento de una contingencia.

De igual manera, por el cumplimiento de las estrategias preventivas.

Es muy importante que antes y durante la ocupación de un puesto de trabajo se sensibilice y capacite al empleado sobre seguridad de la información, ya que esta constituye una estrategia imprescindible de prevención contemplada en el plan de contingencia.

Se requiere que el área de recursos humanos y el área de sistemas trabajen juntos y mantengan un buen índice de cultura en seguridad de la información.

El área de sistemas debe mantener siempre informada a la gerencia sobre las necesidades e inversiones que deban destinar para mejorar la seguridad informática de la empresa.

Los empleados deben comprometerse a documentar y comunicar los incidentes informáticos al área de sistema, para que ésta lleve el registro en el formato destinado para estos casos y puedan ser tenidos en cuenta para la actualización del plan de contingencia o para replantear estrategias.

El área de sistema deberá mantener organizada toda la documentación de los procesos de su área, actualizar y diligenciar los formatos diseñados en este plan de contingencia.

Mantener una copia del plan de contingencia fuera de la empresa junto con las copias de seguridad de la información.

7. DIVULGACIÓN

La gerencia y los asesores en sistemas de la Ferretería Cesar participaron activamente en todas las fases del proyecto. Una vez se finalizó la documentación del plan de contingencia fue socializado a través de una charla a la gerencia y jefes de área, dándoles a conocer los riesgos a los que estaban expuestos, las estrategias preventivas y de recuperación que se diseñaron.

Dada la poca cultura en seguridad de la información entre los empleados, se realizó una charla de sensibilización, se entregaron folletos que contenían información acerca de las amenazas de las cuales pueden ser víctimas y las medidas preventivas que deberían tomar ante esas amenazas. Luego, se realizó capacitación del plan de contingencia a todos los empleados y se entregaron folletos informativos sobre el plan. De esta manera este proyecto fue ampliamente divulgado en la Ferretería Cesar.

BIBLIOGRAFÍA

DE PABLOS HEREDERO, Carmen, *et al*. Informática y comunicaciones en la empresa. Madrid España: ESIC Editorial, 2004. 316p.

DEPOSITO CENTRAL DE VALORES. Plan de Contingencia del DCV Fundamentos y Metodología Aplicada. [En línea]. Agosto 2008. [Revisado: agosto 2017]. Disponible en internet: https://www.contacto. dcv.cl/ portalweb/ Servicios/Portal/empresa/procedimientos/download/PlandeContingenciade0DCV2008.pdf

DÍAZ SAMPEDRO, Manuel. Contingencia TIC vs Continuidad de negocio [en línea], 30 de septiembre de 2011 [Revisado agosto 2017]. Disponible en internet: https://www.incibe.es/protege-tu-empresa/blog/contingencia-vs-continuidad

GONZÁLEZ ROJAS, H.D. en Contribuciones a la Economía. Importancia de la tecnología en las empresas [En línea]. Febrero 2010. [Revisado: agosto 2017]. Disponible en internet: http://www.eumed.net/ce/2010a/hdgr.htm

GRANDA, Andrea. Diseño de un plan de contingencias de Tics para la empresa eléctrica CENTROSUR. Trabajo de grado maestría en gerencia de sistemas de información. Cuenca, Ecuador. Universidad de Cuenca.Facultad de Ingeniería. 2011. 237p.

GUZMÁN, Cindy y PACHECO, Zaidy. Diseño de un plan de contingencia y recuperación ante desastres en el centro de cómputo de la Universidad Popular del Cesar. Trabajo de Grado Ingeniero de Sistemas. Valledupar, Colombia. Universidad Popular del Cesar. Facultad de ingeniería. 2013. 186p.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistemas de gestión de continuidad de negocio. NTC-ISO22301:2012. Bogotá D.C: El Instituto, 2012. 28p.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Directrices para la preparación de la tecnología de la información y las comunicaciones para la continuidad de negocio. NTC-ISO27031:2011. Bogotá D.C: El Instituto, 2016. 42p.

LEÓN LÓPEZ, Diana Rocío. Plan de Contingencia para el archivo de la Universidad de la Salle como parte de la implantación del sistema integrado de Conservación. Trabajo de grado profesional en Sistemas de Información, bibliotecología y archivística. Bogotá, Colombia. Universidad La Salle. Facultad de sistemas de Información y Documentación. 2007. 186p.

MAGERIT. Libro III Metodología. Versión 3. [Revisado agosto 2017]. [En línea], [consultado el 22 de septiembre de 2017]. Disponible en internet: https://www. ccn-cert.cni.es/ documentos-públicos/1793-magent

MINISTERIO DE HACIENDA Y ADMINISTRACIÓN PÚBLICA DEL GOBIERNO DE ESPAÑA. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. Madrid, España: 2012. 127p.

MOLINER, Francisco. Grupos A y B de informática bloque especifico temario Volumen II. Sevilla, España: Editorial MAD, 2011. 203 p.

MONCADA VIGO, Gilberto. Guía práctica para el desarrollo de planes de contingencia de sistemas de información. Lima: Centro de Edición del INEI, 2001. 81 p.

RAMÍREZ ROBAYO, Maritza Yohana, LONDOÑO RÚA, Edwin Alberto y GÓMEZ GÓMEZ, Jairo Andrés. Propuesta de Mejoramiento y Contingencia de Sistemas Informáticos en la Empresa “T”.Trabajo de Grado. Especialización en Gerencia Informática. Bogotá, Colombia. Universidad EAN. Facultad de ingeniería. 2012. 165p.

ANEXOS

ANEXO A. Resultados de la encuesta aplicada

ENCUESTA APLICADA A LOS EMPLEADOS DE LA FERRETERÍA CESAR Y RESULTADOS OBTENIDOS.

Fecha (DD/MM/AAAA): _____

Empresa**:** _____

Nombre**:** _____

Cargo**:** _____

1. Marque con una **X** cuales de los siguientes recursos considera usted que son de vital importancia para las funciones de su cargo:

   Computador _____ Celular _____ Aplicaciones de software o programas _____ Tableta _____ Teléfono Fijo _____ Herramientas Ofimáticas (Word, Excel) _____ Impresora _____ Scanner _____ Red de datos _____ Internet _____ Correo electrónico corporativo (Email) _____ Pagina Web de la Empresa _____ Otro: ____ ¿Cuál? _____

2. Especifique el nombre de las aplicaciones de software o programas que requiere para desarrollar funciones a su cargo:
   _____
   _____

3. ¿Al encender su computador tiene asignado una contraseña para el inicio de sesión?
   Sí____ No ____

4. ¿Comparte o ha compartido alguna vez la contraseña asignada para el ingreso a los programas o aplicaciones con otros empleados?
   Sí ____ No ____

5. ¿Recibe usted por parte de la empresa capacitaciones sobre la seguridad de la información?
   Sí___ No ___

6. ¿Considera usted que tiene un computador óptimo para sus labores?
   Sí ___ No ___ ¿Por qué?
   _____

7. ¿Tiene conocimiento sobre Ransomware?
   SI___ No ___

8. ¿Tiene conocimiento sobre Ingeniería Social?
   SI___ No ___

9. ¿Tiene conocimiento sobre políticas de seguridad de la información?
   SI___ No ___

10. Si su computador se daña en promedio que tiempo se demoran en arreglarlo
    De 1 a 3 horas ____ De 3 a 6 horas ___ De 8 a 24 horas ___ Varios días ____

De acuerdo a una escala de 1 a 5 donde:

1) Nunca, 2) A veces, 3) Frecuentemente, 4) Casi siempre, 5) Siempre

Responda las siguientes preguntas:

11. En el desarrollo de sus funciones con qué frecuencia ha tenido alguno de estos incidentes informáticos:

    Virus ____

    Perdida de datos o archivos importantes en su labor ____
    Interrupción del servicio de la red de datos ____
    Interrupción del servicio de Internet ____
    Interrupción del servicio de correo electrónico ____
    Incidentes en las aplicaciones de software o programas ____
    Suspensión del servicio telefónico ____
    Caída de la página Web de la empresa ____

12. ¿Con que frecuencia recibe mantenimiento preventivo su computador? _____

13. ¿Con que frecuencia cambia las contraseñas asignadas para ingresar a las aplicaciones de software o programas? _____

14. ¿Con que frecuencia realiza copia de seguridad de información importante de la empresa que usted tiene a su cargo? _____

15. ¿En caso de tener algún incidente con las aplicaciones de software comunica usted al jefe de sistema para que se tomen medidas correctivas? _____

16. En caso de tener un incidente con algunos de los recursos que marcó en la primera pregunta, considera usted que influye en:

La calidad de atención al cliente _____, la calidad de su trabajo _____, la imagen de la empresa ante los proveedores y clientes ____

17. ¿Con que frecuencia es capacitado en planes de emergencia y recuperación de desastres? _____

18. ¿Con que frecuencia bloquea el escritorio de su computador cuando se ausenta del puesto de trabajo? _____

19. ¿Con que frecuencia escanea las memorias USB que conecta a su computador? _____

20. ¿Con que frecuencia se ausenta de su trabajo en días laborales? _____

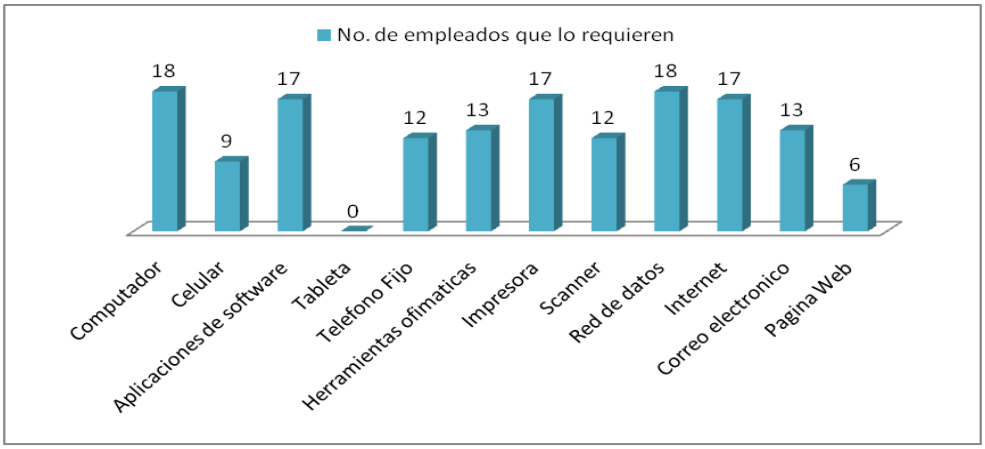
Muchas gracias por su tiempo y colaboración

RESULTADO DE LA ENCUESTA APLICADA

La encuesta fue aplicada al personal de ventas, bodega, compras, cartera y contabilidad para un total de 18 empleados.

A la pregunta orientada a identificar cuales recursos son considerados como de vital importancia para las funciones del cargo desempeñado para cada empleado, los encuestados identificaron en primer lugar al computador y a la red de datos, en segundo lugar, a las aplicaciones de software y el internet, en tercer lugar, al correo electrónico y las herramientas ofimáticas. En cuarto lugar, el teléfono fijo y el scanner, en quinto lugar, el celular, en sexto lugar la página web y séptimo lugar la tableta. Los resultados fueron graficados en la figura 5.

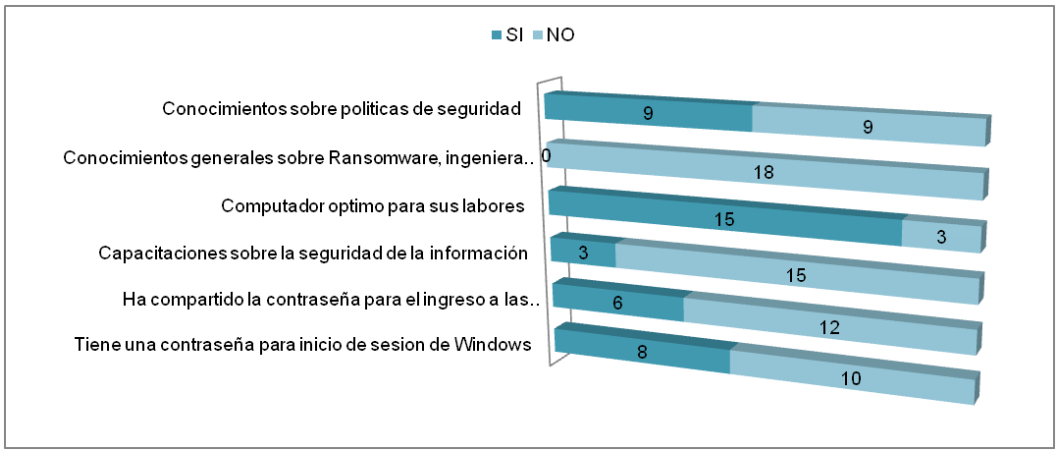
Figura 5. Resultado de la encuesta a la pregunta 1



Fuente: autor.

De las preguntas de la 3 a las 10, la encuesta señala que nueve de los encuestados tienen conocimientos generales sobre políticas de seguridad de la información, los encuestados no están familiarizados sobre los conceptos Ransomware e ingeniería social. Quince de los encuestados consideran que tienen un computador óptimo para sus labores. Los encuestados aseguran que no reciben capacitaciones acerca de seguridad de la información. Muchos empleados han compartido su contraseña para el ingreso a las aplicaciones. La gran mayoría de los empleados no tiene una contraseña para el inicio de sesión de Windows. En la figura 6.

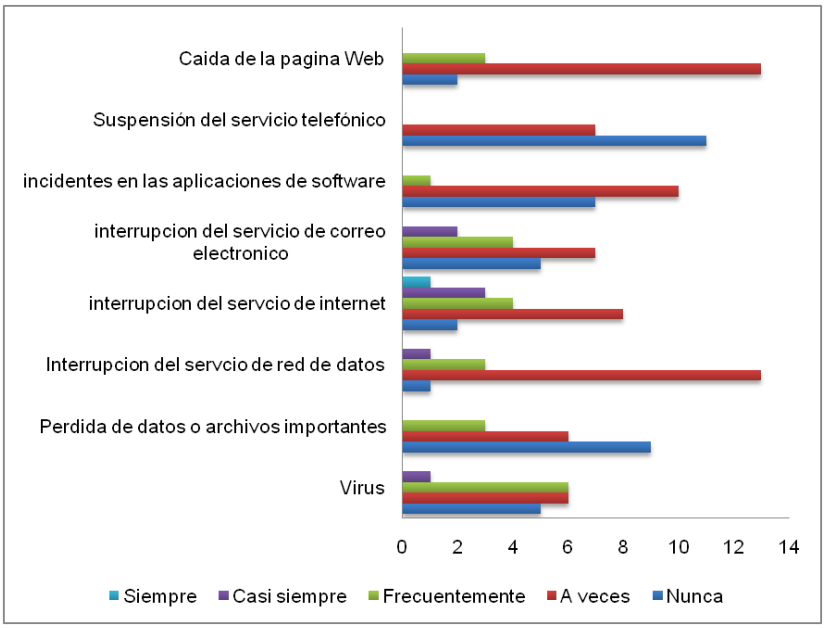
Figura 6. Resultados de la encuesta respecto a las preguntas de la 3 a 10



Fuente: autor.

Respecto a la pregunta 11 referente a los incidentes informáticos graficados en la figura 7 se evidencia que a veces la página Web presenta interrupciones, no se presentan continuamente la suspensión del servicio telefónico, a veces hay incidentes aplicaciones de software, a veces hay interrupciones del servicio de internet, a veces hay interrupciones del servicio de la red datos.

Figura 7. Resultados de encuesta a la pregunta 11

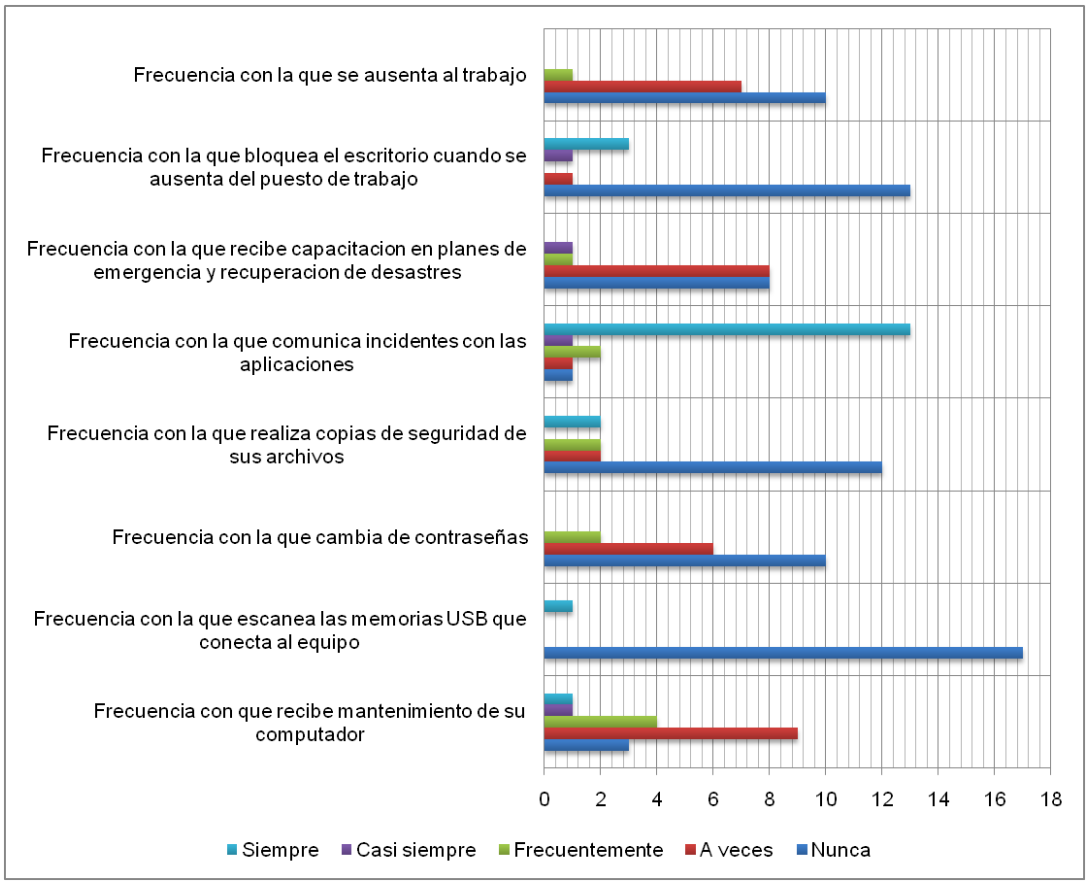


Fuente: autor.

Nueve de los encuestados contestaron que no han perdido archivos importantes, sin embargo, seis de los encuestados a veces han perdido datos o archivos importantes. A veces han sido infectados de virus.

Los resultados a las preguntas 12 a la 20, se grafican en la figura 8. Los encuestados anotaron que nunca se ausenta de su trabajo, nunca bloquean el escritorio cuando se ausentan de su puesto de trabajo, aceces reciben capacitación sobre planes de emergencia y recuperación de desastres, siempre comunican los incidente con las aplicaciones, nunca realizan copia de seguridad de sus archivos, nunca cambian sus contraseñas, nunca escanean las memorias USB que conecta al equipo, a veces sus computadores reciben mantenimiento preventivo.

Figura 8. Resultados de la encuesta a las preguntas de la 12 a la 20



Fuente: autor.

ANEXO B. Procesos críticos de negocios

Cuadro 14. Descripción del proceso de gestión de venta

Gestión de Ventas	
Descripción del proceso: 1. El cliente solicita la cotización de los productos que requiere, esta solicitud se realiza de forma personal, telefónica o por email. 2. El Vendedor verifica la disponibilidad del producto, su valor y realiza la facturación de los productos en el programa Zafiro. 3. En caso de ser una factura contado el cliente realiza la cancelación en caja. El registro del pago se registra en el programa Zafiro. 4. En caso de ser una factura crédito el vendedor verifica el saldo del cupo crédito del cliente en el programa Zafiro. Si el cliente no tiene cupo, debe solicitar al área de cartera, quien hace el estudio de crédito y asigna el cupo en el programa Zafiro. 5. El cliente se dirige al área de despacho, donde los auxiliares de bodega entregan la mercancía. 6. En caso que el cliente no vaya a retirar la mercancía o la retire de manera parcial, el área de despacho registra en el programa Zafiro los productos que quedarán pendiente por entregar. 7. El cliente puede hacer devoluciones de mercancía. En ese caso el jefe de venta registra en el programa Zafiro la devolución.	
Infraestructura tecnológica:	Equipo de informática personal
	Impresora
	Red de datos LAN
	Aplicativo Zafiro
	Internet
	Email
	Red telefónica
Recurso humano:	Vendedores
	Auxiliares de bodega
	Jefe de venta
	Auxiliares de cartera
Tiempo de espera máximo por la interrupción del servicio:	La gerencia establece que la interrupción por más de 4 horas de este servicio representaría una pérdida de ingresos por más de 20 millones de pesos. En una hora pico más de 20 clientes resultaría afectado.
Se puede crear un proceso alternativo en caso de contingencia.	Si. Llevar un registro manual de ventas utilizando facturas por talonarios y registro en libros para el despacho en bodega.

Fuente: autor.

Cuadro 15. Descripción del proceso cartera

Gestión de Cartera	
Descripción del proceso: 1. El cliente solicita al área de cartera el estudio para asignación de cupo de crédito. 2. El auxiliar de cartera solicita la documentación requerida y diligencia con el cliente los formatos de solicitud de cupo de crédito. 3. El auxiliar de cartera realiza la consulta del historial crediticio en línea a las centrales de riesgo. 4. El auxiliar de cartera asigna una puntuación y remite toda la documentación al gerente. 5. El gerente revisa la documentación y autoriza un cupo de crédito para el cliente. 6. El auxiliar de cartera registra el cupo de crédito en el programa Zafiro. 7. El auxiliar de cartera comunica al cliente a través de email y llamada telefónica los resultados del estudio. 8. Por otra parte, los auxiliares de cartera realizan la gestión de cobro a los clientes con cartera vencida. Para esto se apoyan en el programa Zafiro que tiene la información correspondiente al año actual y el programa Siffox que contiene la cartera anterior al año 2017.	
Infraestructura tecnológica:	Equipo de informática personal
	Red de datos LAN
	Aplicativo Zafiro
	Aplicativo Siffox
	Internet
	Email
	Red telefónica
Recurso humano:	Auxiliares de cartera
	Gerente
Tiempo de espera máximo por la interrupción del servicio:	En fines de mes y quincena se establece que la interrupción por más de 8 horas de este servicio representaría una pérdida por recaudos por más de 60 millones de pesos.
Se puede crear un proceso alternativo en caso de contingencia.	Si. Llevar un registro manual de recaudos por medio de talonarios de recibos de caja. Para el proceso de asignación de cupos de créditos se espera hasta el restablecimiento del servicio.

Fuente: autor.

Cuadro 16. Descripción del proceso compras

Gestión de Compras	
Descripción del proceso: 1. El jefe de compras genera informes estadísticos en el aplicativo Zafiro sobre la rotación de inventario, la existencia de los productos, productos por proveedores, etc. 2. El jefe de compras analiza la información, determina los productos y la cantidad que debe comprar. 3. Contacta a proveedores vía telefónica o email para solicitar cotización de los productos. 4. Se reúne con el gerente para la autorización de la compra. 5. El jefe de compras contacta a proveedores para la facturación y envío de la mercancía. 6. Registra la solicitud de pedido en el aplicativo Zafiro 7. Cuando llega la compra el jefe de bodegas recibe y verifica que la mercancía que recibe sea igual a la cantidad que facturaron. 8. El jefe de compras registra la llegada del pedido en el aplicativo Zafiro. Verifica que lo facturado sea igual al pedido inicial y en caso de no serlo realiza los respectivos ajustes.	
Infraestructura tecnológica:	Equipo de informática personal
	Red de datos LAN
	Aplicativo Zafiro
	Internet
	Email
	Red telefónica
Recurso humano:	Jefe de compras
	Auxiliares de Bodega
	Gerente
Tiempo de espera máximo por la interrupción del servicio:	En fines de mes y quincena se establece que la interrupción por más de 8 horas afectaría el control del inventario.
Se puede crear un proceso alternativo en caso de contingencia.	Si. Llevar un registro manual de la mercancía que llega.

Fuente: autor.

Cuadro 17. Descripción del proceso contable

Gestión de Contabilidad	
Descripción del proceso: 1. Los auxiliares contables mensualmente llevan a cabo el proceso de integración del aplicativo Zafiro y el aplicativo Helisa. El aplicativo Zafiro genera un archivo plano con todos los movimientos de facturación, devolución, inventario y compras. El aplicativo Helisa sube este archivo plano y genera los respectivos asientos contables. 2. El jefe de contabilidad genera los balances y reporta al gerente las pérdidas o utilidades generadas en el mes. 3. Los auxiliares contables junto con el jefe de contabilidad liquidan los impuestos a los que haya lugar a través del portal DIAN, la periodicidad de liquidación se hace en unas fechas que establece la DIAN. También realizan liquidación de impuestos en la página web de la alcaldía de Valledupar. 4. Registran todo movimiento de entrada y salida de dinero de la empresa en el aplicativo Helisa. El aplicativo Helisa contiene el registro contable de los años 2016 y 2017. El registro contable 2010-2015 está registrada en el programa Sisconplus. Anterior al año 2010 en el programa Linker.	
Infraestructura tecnológica:	Equipo de informática personal
	Red de datos LAN
	Aplicativo Helisa
	Aplicativo Zafiro
	Aplicativo Sisconplus
	Aplicativo Linker
	Internet
	Red telefónica
Recurso humano:	Jefe de compras
	Auxiliares de Bodega
	Gerente
Tiempo de espera máximo por la interrupción del servicio:	En fechas de liquidación de impuestos se establece que la interrupción por más de 24 horas ocasionaría el pago de sanciones por reportes extemporáneos.
Se puede crear un proceso alternativo en caso de contingencia.	Si, parcialmente. Contabilización en Excel con formato de archivos planos para un posterior cargue.

Fuente: autor.

Cuadro 18. Descripción del proceso administrativo

Gestión Administrativa	
Descripción del proceso: 1. Pagos a proveedores. El gerente solicita la información diariamente a cartera y contabilidad sobre los pagos que debe realizar en el día. Los pagos menores a cinco millones se hacen en efectivo o en cheque. Mayores a ese monto se realizan a través de transferencia electrónica o consignación. 2. Otros Pagos. El gerente autoriza el pago de otras cuentas como servicios públicos, cuentas de cobros por prestación de servicios. 3. El jefe de recursos humanos y sus auxiliares registran las novedades de nómina y liquidan quincenalmente la nómina, para esto se apoyan el aplicativo Helisa. Mensualmente calculan el valor de la bonificación por ventas a los vendedores, apoyados en el aplicativo Zafiro. 4. Los auxiliares registran información en la página web de la policía nacional acerca de la venta y compra de productos controlados como el thinner.	
Infraestructura tecnológica:	Equipo de informática personal
	Red de datos LAN
	Aplicativo Helisa
	Aplicativo Zafiro
	Internet
	Red telefónica
Recurso humano:	Jefe de recursos humanos
	Auxiliares
	Gerente
Tiempo de espera máximo por la interrupción del servicio:	En fechas de reporte en la plataforma web de la policía nacional más de 24 horas ocasionaría el pago de multas y sanciones por el no reporte oportuno de la información. El no pago de las cuentas por pagar oportunamente generarían costos por concepto de intereses, además de reportes de mala calificación por parte de los proveedores y bancos a centrales de riesgos.
Se puede crear un proceso alternativo en caso de contingencia.	No.

Fuente: autor.

ANEXO C. Evidencias fotográficas de vulnerabilidades

En la figura 9 se evidencia que el cableado de datos está expuesto a mucha acumulación de polvo. Se requiere de una limpieza periódica para disminuir el riesgo de deterioro causado por la contaminación medio ambiental.

Figura 9. Contaminación medio ambiental del cableado de datos

Fuente: autor.

En la figura 10 se observa que el centro de datos tiene una ventana contigua a la oficina de contabilidad, con el abanico distribuyen el aire acondicionado hacia el centro de datos. Sin embargo, la temperatura del centro de datos no es la adecuada, se requiere la adquisición de un aire acondicionado que mantenga al centro de datos en una temperatura óptima entre 18 y 27 ºC.

Figura 10. Sistema de refrigeración y ventana de acceso del centro de datos

Fuente: autor

Además, esa ventana permite que el centro de datos pueda ser accedido por una persona no autorizada desde la oficina de contabilidad.

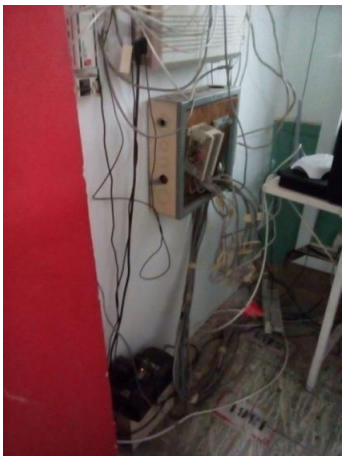
En la figura 11 se puede ver que la puerta de entrada al centro de datos no tiene la seguridad apropiada, puede ser violada con facilidad.

Figura 11. Puerta de entrada para el centro de datos.

Fuente: autor

En la figura 12 se evidencia que dentro del centro de datos hay una gran parte del cableado que esta expuesto. Por seguridad debe estar en canaletas y marcado para una facil identificación.

Figura 12. Exposición del cableado de datos



Fuente: autor

La figura 13 corresponde a la rejilla del aire acondicionado que hay sobre los equipos informáticos de la sala de ventas, las gotas caen sobre los escritorios esto puede ocasionar un daño a los equipos informáticos, deterioro a los escritorios y a documentos.

Figura 13. Rejilla del aire acondicionado sobre los equipos informáticos

Fuente: autor

ANEXO D. Formato para reporte de incidentes informáticos

	FERRETERIA CESAR S.A.	Formato 01 Octubre 2017 Versión 1.0
REPORTE DE INCIDENTES INFORMÁTICOS		
Fecha del incidente (dd/mm/aaaa):		
Forma Reporte l	Telefonico ☐ Ema ☐	Personal ☐
Solicitante:		
Dependencia:		
Prioridad:	Baja ☐ Media ☐	Alta ☐
DESCRIPCION DEL INCIDENTE		
CAUSAS DE LA FALLA		
SOLUCION		
MEDIDAS PREVENTIVAS		
Fecha solución:	Modificar el Plan i	☐ o ☐
REPORTADO POR	SOLUCIONADO POR	
Nombre: Firma:	Nombre: Firma:	

ANEXO E. Lista de contacto comité del plan de contigencia informático

Por motivos de confidencialidad se omiten los datos de contactos en este proyecto.

<table>
<tr><td colspan="2">  FERRETERIA CESAR S.A.S.</td><td>Formato 02
Octubre 2017
Versión 1.0</td></tr>
<tr><td colspan="3">COMITE DE PLAN DE CONTINGENCIA</td></tr>
<tr><td colspan="3">Coordinador de continuidad y recuperación</td></tr>
<tr><td>Titular: Germán Tapias
Cargo: Gerente
Email: Dirección:
Celular:
Teléfono: Extensión:</td><td colspan="2">Suplente: Daniel Tapias
Cargo: Jefe de compras
Email: Dirección:
Celular:
Teléfono: Extensión:</td></tr>
<tr><td colspan="3">Coordinador TI</td></tr>
<tr><td>Titular: Cesar Acosta Díaz
Cargo: Asesor de sistemas
Email: Dirección:
Celular
Teléfono: Extensión:</td><td colspan="2">Titular: Amilkar Sierra romano
Cargo: Asesor de sistemas
Email: Dirección:
Celular
Teléfono: Extensión:</td></tr>
<tr><td colspan="3">Líder en comunicación y recuperación del proceso de Ventas</td></tr>
<tr><td>Titular: Dolber Pumarejo
Cargo: Vendedor
Email: Dirección:
Celular:
Teléfono: Extensión:</td><td colspan="2">Suplente: Hugo Flores
Cargo: Vendedor
Email: Dirección:
Celular:
Teléfono: Extensión:</td></tr>
<tr><td colspan="3">Líder en comunicación y recuperación del proceso de Compras</td></tr>
<tr><td>Titular: Edgar Tapias
Cargo: Jefe de compras
Email: Dirección:
Celular:
Teléfono: Extensión:</td><td colspan="2">Suplente: Yullis Quintero
Cargo: Auxiliar de compras
Email: Dirección:
Celular:
Teléfono: Extensión:</td></tr>
<tr><td colspan="3">Líder en comunicación y recuperación del proceso de Contabilidad</td></tr>
<tr><td>Titular: Noel Ortiz
Cargo: Contador
Email: Dirección:
Celular:
Teléfono: Extensión:</td><td colspan="2">Suplente: Meredith Arzuaga
Cargo: Auxiliar contable
Email: Dirección:
Celular:
Teléfono: Extensión:</td></tr>
<tr><td colspan="3">Líder en comunicación y recuperación del proceso de Nomina</td></tr>
<tr><td>Titular: Cindy Rodriguez
Cargo: Jefe de recursos humanos
Email: Dirección:</td><td colspan="2">Suplente:ElicethPava
Cargo: Auxiliar de nomina
Email Dirección:
Celular</td></tr>
</table>

Celular: Teléfono: Extensión:	Teléfono: Extensión:
Líder en comunicación y recuperación del proceso de Cartera	
*Titular:*Claudia Galvis Cargo: Auxiliar de Cartera Email Dirección: Celular Teléfono: Extensión:	*Suplente:*MiriamCalederon Cargo: Auxiliar de cartera Email Dirección: Celular Teléfono: Extensión:

ANEXO F. Lista de contacto de proveedores

Por motivos de confidencialidad se omiten los datos de contactos en este proyecto.

 FERRETERIA CESAR S.A.S.		Formato 03 Octubre 2017 Versión 1.0
LISTA DE CONTACTO DE PROVEEDORES		
Proveedor:		
Nombre del contacto:		
Nombre del contacto alterno:		
Descripción del proveedor :		
Dirección:		
Teléfono principal:	Celular:	
Teléfono alterno:	Celular alterno:	
Email:		
Proveedor:		
Nombre del contacto:		
Nombre del contacto alterno:		
Descripción del proveedor :		
Dirección:		
Teléfono principal:	Celular:	
Teléfono alterno:	Celular alterno:	
Email:		
Proveedor:		
Nombre del contacto:		
Nombre del contacto alterno:		
Descripción del proveedor :		
Dirección:		
Teléfono principal:	Celular:	
Teléfono alterno:	Celular alterno:	
Email:		

ANEXO G. Formato hoja de vida de los equipos informáticos

	FERRETERIA CESAR S.A.S.	Formato 04 Octubre 2017 Versión 1.0
HOJA DE VIDA DE EQUIPOS INFORMÁTICOS		
No. ticket del Equipo:		
Empleado responsable:		
Ubicación:		
Descripción del equipo :		
Seriales de hardware		
Monitor:	Teclado:	
CPU:	Mouse:	
Sistema operativo:		
No. de licencia del sistema operativo:		
Aplicaciones críticas de negocio instaladas:		
Herramienta de ofimática instalada:		
No. de licencia de la herramienta ofimática:		
Otras aplicaciones necesarias:		
Direccionamiento IP:		
Dirección IP:	Mascara:	
Puerta de enlace:	DNS:	
Nombre del equipo:		
Dominio:	Grupo de Trabajo:	
Perfil de usuario del sistema operativo:		
Prioridad de evacuación:		
Impresoras instaladas de red:		
Impresora local instalada:		
Observación:		
Fecha de actualización (dd/mm/aaaa):		
Elaboró:		

ANEXO H. Formato para el registro de perfiles de usuarios

FERRETERIA CESAR S.A.S.	Formato 05 Octubre 2017 Versión 1.0
REGISTRO DE PERFILES DE USUARIOS	
Nombre del Perfil:	
Puesto de trabajo:	
Área:	
Permisos de acceso a los servicios de red :	
Permisos requeridos al sistema de información Zafiro:	
Permisos requeridos al sistema de información Helisa:	
Observaciones:	
Fecha de actualización (dd/mm/aaaa):	
Elaboró:	

ANEXO I. Formato para el registro de control de backups

 FERRETERIA CESAR S.A.S.			Formato 06 Octubre 2017 Versión 1.0
REGISTRO DE CONTROL DE BACKUPS			
No.	Fecha	Equipo o Sistema de Información	Realizado por
1			
2			

ANEXO J. Lista de contactos de emergencia

FERRETERIA CESAR S.A.S.		Formato 07 Octubre 2017 Versión 1.0
LISTA DE CONTACTOS DE EMERGENCIA		

No.	Nombre	Teléfono	Celular
1	Cuerpo de Bomberos	119	
2	Cruz Roja	132	
3	Defensa Civil	144	
4	Policía Nacional	123	
5	CTI	122	
6	Gaula de la Policía Nacional	165	
7	Hospital Eduardo Arredondo Daza E.S.E	5842828	
8	Hospital Rosario Pumarejo de López E.S.E	5748462	
9	Acueducto Daños y Reclamos	116	
10	Energía Daños y Reclamos	115	
11	Gas Daños y Reclamos	164	
12	Ambulancia Proyectar	5801798	
13	Ambulancia Clínica Laura Daniela	5803535	
14	Ambulancia vital Medic	5843686	
15	Brigadista: Jorge Ojeda	5708585 Ext. 120	3008163651
16	Brigadista: Eliseth Pava	5708585 Ext. 102	3012292763

ANEXO K. Formato del plan de pruebas

FERRETERIA CESAR S.A.S.	Formato 08 Octubre 2017 Versión 1.0
PLAN DE PRUEBAS	
Tipo de Prueba: ☐ Escritorio ☐ Real con previo aviso	
Fecha de la prueba:	
Tiempo estimado:	
Duración real:	
Objetivos :	
Alcance:	
Escenario de incidente:	
Acciones:	
Conclusiones:	
Elaboró:	

ANEXO L. Registro de control de asistencia

	FERRETERIA CESAR S.A.S.	Formato 09 Octubre 2017 Versión 1.0
REGISTRO DE CONTROL DE ASISTENCIA		
Tema: [ ]Capacitación plan de contingencia [ ]Prueba plan de contingencia		
Fecha (dd/mm/yyyy):	No. Horas:	

Cedula	Nombre	Firma

ANEXO M. Carta de aceptación para el desarrollo del proyecto

FERRETERIA CESAR S.A.S.

NIT. 892301090-1

Todo bajo un solo nombre

Valledupar, 31 de agosto de 2017

Señores
COMITÉ DE PROYECTO DE GRADO
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

Cordial saludo,

De manera atenta manifestamos nuestro interés y conocimiento de la propuesta de proyecto de grado titulada:

DISEÑO DE UN PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LAS NORMAS ISO/IEC 22301 E ISO / IEC 27031: 2011 PARA LA FERRETERÍA CESAR S.A.S EN LA CIUDAD DE VALLEDUPAR

Elaborada por la ingeniera SHIRLEY TATIANA PITTA PICÓN identificada con cedula de ciudadanía No. 1.065.563.682, con el fin dè optar por el título de Especialista en Seguridad Informática.

En este sentido, nos comprometemos a participar del proceso ofreciendo la información y el apoyo necesario para el desarrollo de dicho proyecto.

Cordialmente,

FERRETERIA CESAR S.A.S
NIT. 892.301.090-1
GERENCIA

GERMAN TAPIAS DIAZ
Gerente

Calle 20 No. 11-06 Valledupar, Cesar
Tels: 574 5057 - 574 5547 - 574 5044
570 8585 - 574 3332 - 574 5380
300 816 3651 - 313 555 2304 - 315 741 5391

Ventas: ventas@ferreteriacesar.com.co
Administración: gerencia@ferreteriacesar.com.co
Cartera: yasira.m@ferreteriacesar.com.co
meredith.a@ferreteriacesar.com.co
Tesorería: naive.p@ferreteriacesar.com.co

ANEXO N. Registro fotografico de la capacitación del Plan de Contigencia.


HERRAGRO
HERRAGRO


HERRAGRO


HERRAGRO

ANEXO O. Registro de control de asistencia a capacitación

FERRETERIA CESAR S.A.S.		Formato 09 Octubre 2017 Versión 1.0
REGISTRO DE CONTROL DE ASISTENCIA		
Tema: [X]Capacitación plan de contingencia [ ]Prueba plan de contingencia		
Fecha (dd/mm/yyyy): 27/11/2017	No. Horas: 2	
Cedula	Nombre	Firma
49765714	[illegible]	
5134796	Dolber A. Ramon/o	
8946074	Claudio B.	
21164601	[illegible]	
77184186	Jorge Ojeda	
49730307	Naomi Pérez Avila	
1065.616.640	Elvirth Fabiana Pavon Mendez	
1065819.126	Dolys M. Rojas Rondón	Dolys Rojas
49606118	Claida Arnez Sanchez	Claida Arnez S.
1065823048	Mary Calderas, Calvis	
49786167	Miriam Calderon	
49758916	Heredith Arzuaga Trigozo	
13701726	Gustavo Bolola Rojas	
91066595	Daniel Tapias P.	
1.065.632.046	Sindy Medina C.	Sindy M.
Yollis 1065589	Yollis Quintero	Yollis Quinte
1065618779	Yosvia Mendoza Arteaga	
77170961	Hugo Florez	

ANEXO P. Resumen analítico educativo RAE

Título del documento	DISEÑO DE UN PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LAS NORMAS ISO/IEC 22301 E ISO / IEC 27031: 2011 PARA LA FERRETERÍA CESAR S.A.S EN LA CIUDAD DE VALLEDUPAR
Autor	SHIRLEY TATIANA PITTA PICÓN
Lugar y año de publicación:	Valledupar – Colombia, 2018
Descripción:	Tesis de grado que propone diseñar un plan de contingencia informático para la empresa Ferretería Cesar. Con la finalidad de identificar los riesgos a los que están expuestos, establecer estrategias preventivas y de recuperación que asegure la continuidad de las tareas críticas de la empresa acorde a sus necesidades e infraestructura, basados en las normas internacionales ISO 22301 y 27031 que provee las técnicas y directrices de gestión de continuidad de negocio y recuperación de los servicios de TIC.
Palabras claves:	Plan de contingencia, incidente informático, gestión de continuidad TIC, análisis de riesgos Magerit.
Fuentes bibliográficas	Se referencia 13 fuentes bibliográficas, algunas que mencionan la temática principal son: GRANDA, Andrea. Diseño de un plan de contingencias de Tics para la empresa eléctrica CENTRO SUR. Trabajo de grado maestría en gerencia de sistemas de información. Cuenca, Ecuador. Universidad de Cuenca. Facultad de Ingeniería. 2011. 237p. INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistemas de gestión de continuidad de negocio. NTC-ISO22301:2012. Bogotá D.C: El Instituto, 2012. 28p. INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Directrices para la preparación de la tecnología de la información y las comunicaciones para la continuidad de negocio. NTC-ISO27031:2011. Bogotá D.C: El Instituto, 2016. 42 p. MINISTERIO DE HACIENDA Y ADMINISTRACIÓN PÚBLICA DEL GOBIERNO DE ESPAÑA. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. Madrid, España: 2012. 127p MONCADA VIGO, Gilberto. Guía práctica para el desarrollo de planes de contingencia de sistemas de información. Lima: Centro de Edición del INEI, 2001. 81 p.
Problema	El proceso comercial de la empresa Ferretería Cesar está

	soportado sobre una infraestructura tecnológica que provee el espacio para registrar todas sus transacciones comerciales y almacenar la información sensible. El uso de la infraestructura tecnológica ha generado una amplia dependencia entre ella y la actividad principal del negocio, así que una falla técnica o la parálisis de las operaciones normales de los servicios tecnológicos y de información, pueden llegar a impactar negativamente a los ingresos y reputación de la empresa.
Objetivos	Asegurar la continuidad de los servicios de la Ferretería Cesar frente a la posible ocurrencia de un incidente de seguridad que comprometa total o parcialmente la prestación de los servicios informáticos, mediante el diseño de un plan de contingencia informático. Objetivos Específicos • Identificar los riesgos que pueden afectar el normal funcionamiento de los procesos informáticos de la empresa con el fin de hacer una valoración de los mismos, utilizando la metodología Magerit. • Establecer las estrategias preventivas que permitan disminuir la probabilidad de ocurrencia de un estado de contingencia. • Diseñar los procedimientos de recuperación que pueden asegurar la continuidad de los servicios informáticos en caso de una interrupción, alineados con el estándar ISO / IEC 27031: 2011 e ISO/IEC 22301:2012. • Sensibilizar al personal para promover el buen uso y manejo del plan de contingencia informático, a través de una capacitación. • Elaborar un plan de contingencias que asegure la continuidad de las tareas críticas, acorde a la infraestructura y necesidades de la empresa alineado al estándar ISO / IEC 27031: 2011 e ISO/IEC 22301:2012.
Metodología	La metodología aplicada para el desarrollo del proyecto fueron las recomendadas por el Instituto Nacional de Estadística e Informática del Perú (INEI), el instituto nacional de Ciberseguridad de España, alineándola con el estándar internacional ISO / IEC 27031: 2011 e ISO/IEC 22301:2012. La metodología consta de varias fases y las actividades que se desarrollaron en cada fase son las siguientes: Fase 1: Identificación de Riesgos Durante esta fase se identificaron los riesgos que pueden afectar el normal funcionamiento de los procesos informático de la empresa. De acuerdo a la metodología Magerit, se realizaron las siguientes actividades:

	• Determinar los activos relevantes de la empresa • Determinar las amenazas a los que están expuestos los activos • Estimar los impactos potenciales y residuales • Estimar las salvaguardas de los activos • Se consolidarán los resultados obtenidos. Durante esta fase también se analizaron los procesos de la empresa para identificar los procesos críticos de negocio y determinar el tiempo objetivo de recuperación. Fase 2: Identificación de soluciones y Estrategias Durante esta fase se establecieron las estrategias preventivas que permitían disminuir la probabilidad de ocurrencia de un estado de contingencia. Además de planes de respuestas y de recuperación en caso de una emergencia de acuerdo al estándar ISO / IEC 27031 e ISO/IEC 22301. Fase 3: Documentación del proceso: Durante esta fase se diseñaron los procedimientos de recuperación que pueden asegurar la continuidad de los servicios informáticos en caso de una interrupción. Se elaboró el documento que contiene el plan de contingencia informático, en él está consolidado todo el análisis y documentación que se ha recogido en las fases anteriores y las soluciones a las contingencias. Fase 4: Implementación, socialización y evaluación del plan de contingencia Durante esta fase se evaluó el plan de contingencia informático realizando una prueba controlada con la finalidad de garantizar que se entrega un plan de contingencia acorde a la infraestructura de la empresa y de acuerdo a los estándares internacionales. Además, se socializó con la gerencia y se realizó la sensibilización al personal para promover el buen uso y manejo del plan de contingencia informático.
Conclusiones	Se identificaron los procesos críticos de negocio que están soportados por las TIC y se realizó el análisis riesgo utilizando la metodología Magerit. Se establecieron varias estrategias de prevención que permiten a la empresa disminuir la probabilidad de un estado de contingencia. Se definieron los procedimientos para recuperase en el menor tiempo posible teniendo en cuenta las directrices del estándar ISO / IEC 22301 e ISO / IEC 27031. Se realizó la sensibilización del personal para promover el buen uso y manejo del plan de contingencia. Se elaboró un plan de contingencia que asegura la continuidad de los servicios de la Ferretería Cesar frente a la posible ocurrencia de un incidente de seguridad que comprometa total o parcialmente la prestación de los servicios informáticos.

Recomendaciones	La gerencia deberá continuar promoviendo la importancia de la seguridad de la información y a mediano plazo considerar contar con un plan de continuidad de negocio para toda la empresa. El comité del plan de contingencia debe velar porque este plan sea actualizado y probado periódicamente para que sea eficaz en el momento de una contingencia. De igual manera, por el cumplimiento de las estrategias preventivas. El área de sistemas debe mantener siempre informada a la gerencia sobre las necesidades e inversiones que deban destinar para mejorar la seguridad informática de la empresa. Los empleados deben comprometerse a documentar y comunicar los incidentes informáticos al área de sistema, para que ésta lleve el registro en el formato destinado para estos casos y puedan ser tenidos en cuenta para la actualización del plan de contingencia o para replantear estrategias. El área de sistema deberá mantener organizada toda la documentación de los procesos de su área, actualizar y diligenciar los formatos diseñados en este plan de contingencia. Mantener una copia del plan de contingencia fuera de la empresa junto con las copias de seguridad de la información.