ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ

MANUEL FÉLIX LÓPEZ

CARRERA INFORMÁTICA

TESIS PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN INFORMÁTICA

TEMA:

ANÁLISIS DE RIESGO EN LA INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO CALCETA LIMITADA

AUTORAS:

MAYRA ALEXANDRA DÁVILA MUÑOZ
GEMA VANESSA PÁRRAGA ANDRADE

TUTOR:

ING. JÉSSICA JOHANNA MORALES CARRILLO, Mg. Sc.

CALCETA, NOVIEMBRE 2015

DERECHOS DE AUTORÍA

Mayra Alexandra Dávila Muñoz y Gema Vanessa Párraga Andrade, declaran bajo juramento que el trabajo aquí escrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su reglamento.

…….. ……...

MAYRA A. DÁVILA MUÑOZ **GEMA V. PÁRRAGA ANDRADE**

CERTIFICACIÓN DE AUTORÍA

Jéssica Johanna Morales Carrillo certifica haber tutelado la tesis **ANÁLISIS DE RIESGO EN LA INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO CALCETA LIMITADA,** que ha sido realizada por Mayra Alexandra Dávila Muñoz y Gema Vanessa Párraga Andrade, previa a la obtención del título de Ingeniera en Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACION DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

…..……

ING. JÉSSICA JOHANNA MORALES CARRILLO Mg.Sc.

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaran que han **APROBADO** la tesis **ANÁLISIS DE RIESGO EN LA INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO CALCETA LIMITADA,** que ha sido propuesta, desarrollada y sustentada por Mayra Alexandra Dávila Muñoz y Gema Vanessa Párraga Andrade, previa a la obtención del título de Ingeniera en Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACION DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

…… .....……..….

ING. ÁNGEL A. VÉLEZ MERO, MGS
MIEMBRO

LIC. JOSÉ G. INTRIAGO CEDEÑO, Mg. Sc
MIEMBRO

……

ING. LUIS C. CEDEÑO VALAREZO, Mg. Sc
PRESIDENTE

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, a los docentes, a nuestro tutor, de manera especial a la Cooperativa de Ahorro y Crédito Calceta Limitada por la oportunidad que nos brindó y la apertura para llevar a cabo el trabajo dentro de la misma, y a nuestros amigos que han contribuido a la buena realización del presente trabajo.

LAS AUTORAS

DEDICATORIA

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que me dio la oportunidad de una educación superior de calidad y en la cual he forjado mis conocimientos profesionales día a día;

A Dios por el don de la vida, a mis padres y hermanas por haberme dado el apoyo necesario para seguir adelante día a día e impulsarme a conseguir la meta propuesta.

A mi esposo e hija, por ser incondicionales conmigo, por compartir los buenos y malos momentos y ser mí apoyo en las épocas difíciles.

A los docentes por los conocimientos impartidos los cuales servirán de guía en mi vida profesional.

MAYRA A. DÁVILA MUÑOZ.

DEDICATORIA

Dedico este trabajo de tesis a Dios por el don de la vida y las fortalezas para cumplir mi meta, a mi madre Doris Andrade, a mis hermanos Ángel Neil, Steven Alexander, Roque Elian y Yesli Madeleine, a mi compañero de vida Jefferson Guerrero por la paciencia y comprensión que tuvieron para encumbrar un escalón más en el viaje del conocimiento, y a las personas que me abrieron camino para la realización del presente trabajo de tesis.

GEMA V. PÁRRAGA ANDRADE.

CONTENIDO GENERAL

CONTENIDO DE CUADROS Y FIGURAS

RESUMEN

La investigación tuvo como objetivo desarrollar un análisis de riesgos, para determinar el grado de exposición a eventos no deseados en la infraestructura de Tecnologías de Información de la Cooperativa de Ahorro y Crédito Calceta Limitada del Cantón Bolívar, para esto se utilizó la metodología Magerit, que fue desarrollada para este tipo de trabajos específicamente, la cual permitió identificar las amenazas y los riesgos a los que está expuesta la institución y el impacto que sufriría en caso de materializarse, este se realizó priorizando las tareas más relevantes en la organización, a partir de ello se obtuvo una propuesta de salvaguardas de la infraestructura de Tecnologías de Información de la institución, para saber cómo y cuándo actuar frente a los riesgos, la cual contribuye a que la institución comprenda sus vulnerabilidades y tome medidas necesarias para que sus activos estén seguros y de esta manera no comprometa la integridad, confidencialidad y disponibilidad de los datos de la institución.

PALABRAS CLAVES

Magerit, Riesgos tecnológicos, Infraestructura tecnológica.

ABSTRACT

The research aimed to develop a risk analysis to determine the degree of exposure of undesirable events in the information technology infrastructure of the Credit and Saving Union Calceta Limited in Bolivar Canton, Magerit methodology was used to develop this type of work specifically, threats and risks where identified to which the Bank are exposed and the impact would be materialized, this was done to prioritize the most important tasks in the organization, safeguards where proposed for the infrastructure of Information Technology in the institution, to know how and when to act against risks, which helps the institution to understand their vulnerabilities and take necessary measures for the safety of the assets and not compromise the integrity, confidentiality and availability of data.

KEYWORDS

Magerit, technological risks, technological infrastructure

CAPITULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

Las tecnologías de información, como cualquier activo, están expuestas a riesgos y cuando estos se materializan, degradan el recurso e impactan en el cumplimiento de los objetivos. Si se estima la frecuencia y magnitud de sus consecuencias, podemos tomar medidas para reducir su impacto. Tomando en cuenta que el recurso tecnológico es considerado importante y valioso en la organización, es necesario administrar adecuadamente el riesgo, mitigando las pérdidas económicas asociadas a ellos (Jiménez, 2008).

Es importante que las instituciones sobre todo las financieras cuenten con equipos que soporten el flujo de información que administran, la cual es confidencial y los datos de los clientes deben estar seguros, por esto es necesario contar con recursos tecnológicos óptimos para así fortalecer y garantizar el buen desarrollo de las actividades de sus clientes y así brindar un servicio de calidad, dado que el nivel de aceptación que tengan este tipo de instituciones se mide por el grado de satisfacción de sus socios.

Los equipos informáticos en toda institución están expuestos a fallas que hacen vulnerable cualquier sistema, y si el sistema informático de la institución falla los procesos no podrán ser desarrollados a cabalidad, lo que podría generar problemas tanto para la organización como para los socios que no pueden acceder a su dinero en el momento requerido.

Las instituciones como la Cooperativa de Ahorro y Crédito Calceta Limitada están expuestos a riesgos informáticos los cuales afectan en la calidad de servicios que se brinda, considerando que este no es un tema exclusivamente informático porque de haber fallas en la infraestructura tecnológica se

presentan impactos en los servicios que presta la organización, por medio de sus diferentes departamentos.

Por los motivos antes mencionados las autoras del presente trabajo plantean la siguiente interrogante:

¿De qué manera se podría conocer la magnitud de los riesgos a los que está expuesta la infraestructura de tecnologías de información de la Cooperativa de Ahorro y Crédito Calceta Limitada?

1.2. JUSTIFICACIÓN

El análisis y gestión de riesgos es un instrumento fundamental para proteger la información, la cual a su vez, tiene implícitas definiciones como apetito y capacidad de riesgo; siendo la primera, el nivel de riesgo que cada organización está preparada para tolerar en sus negocios, y la segunda, el nivel de riesgo que cada organización no está financieramente capacitada para exceder; por lo tanto, la gestión del riesgo es propia para cada organización. (Angarita; Tabares 2012).

La elaboración de un análisis de riesgos tecnológico en la Cooperativa de Ahorro y Crédito Calceta Limitada ayudará a la institución en la identificación de los problemas a los que está expuesta su infraestructura tecnológica y los activos que están susceptibles a daños, así como también a diferenciar los activos que son críticos para el desempeño de las actividades de la institución y que deben priorizarse en su protección, en procura de asegurar la continuidad de los servicios y que el impacto sea en el buen desempeño de sus actividades, por este motivo es fundamental contar con el desarrollo de este trabajo ya que la Cooperativa de Ahorro y Crédito Calceta Limitada es una entidad financiera que debe disponer de una estructura de procedimientos que ayuden a la recuperación inmediata ante los desastres naturales, internos o externos que puedan presentarse. Así lograr el compromiso de la institución en general para fijar responsabilidades de la salvaguarda de todos los activos de la institución, garantizando la confidencialidad, integridad y disponibilidad de la información en el momento requerido, permitiendo un ambiente de trabajo seguro y confiable que permita minimizar costos de levantamiento de la información y recursos informáticos, para en caso de desastres garantizar la continuidad del negocio.

Este trabajo es realizado en cumplimiento con la Ley Orgánica de Educación Superior (LOES, 2013) en lo establecido en el Art. 8 literal h que textualmente expresa: “Contribuir con el desarrollo local y nacional de manera permanente, a través del trabajo comunitario o extensión universitaria”, lo cual se cumple en el

presente trabajo investigativo ya que se contribuye con un tema de interés social que beneficie no solo a los estudiantes que lo desarrollan sino también a la sociedad.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

- Desarrollar un análisis de riesgos para determinar el grado de exposición de eventos no deseados en la infraestructura de Tecnologías de Información de la Cooperativa de Ahorro y Crédito Calceta Limitada del Cantón Bolívar.

1.3.2. OBJETIVOS ESPECÍFICOS

- Determinar los activos de la institución susceptibles a riesgo.
- Identificar las potenciales amenazas que pueden comprometer el funcionamiento de la infraestructura de TI de la institución.
- Detallar las actividades a ejecutarse para prevenir riesgos y daños.
- Establecer una propuesta de salvaguardas de la infraestructura de TI de la institución.

1.4. IDEA A DEFENDER

El análisis de riesgos en la infraestructura tecnológica de Tecnologías de Información, orientará a la Cooperativa de Ahorro y Crédito Calceta Limitada en la toma de decisiones ante eventos que puedan poner el riesgo el buen funcionamiento de la misma.

CAPÍTULO II. MARCO TEÓRICO

2.1. INSTITUCIONES FINANCIERAS

Las instituciones financieras son entidades dedicadas principalmente a la adquisición de activos o pasivos financieros en el mercado, que aceptan depósitos a la vista, a plazo o de ahorro (Vergara, 2011).

Los tipos más importantes de instituciones financieras son:

- Bancos Comerciales
- Asociaciones de ahorro
- Compañías de seguro de vida
- Fondos privados de pensiones
- Fondos de pensiones municipales y estatales
- Compañías financieras
- Bancos de ahorro
- Compañías de inversión
- Fondos del mercado monetario
- Cooperativas de crédito

Las instituciones financieras son aquellas que se dedican a brindar servicio a todos los grupos sociales existentes en un estado, estas sirven como mediador a sus clientes cuando necesiten depositar o adquirir dinero en un lugar seguro para el buen desarrollo de sus actividades habituales, además sirven como medio para que aquellos que necesiten emprender un negocio o adquirir bienes para su satisfacción, contribuyendo al desarrollo de los pueblos.

2.1.1 COOPERATIVA DE AHORRO Y CRÉDITO

De la Fuente y Díaz (2013) indican que las cooperativas son asociaciones autónomas que ayudan a sus asociados a enfrentar sus necesidades

económicas, sociales y culturales. Las cooperativas de ahorro y crédito tienen como función entregar intermediación financiera en beneficio de sus clientes, permitiendo ofrecer un lugar seguro a sus asociados, para que realicen depósitos en cuentas de ahorro y puedan acceder a créditos u otras actividades financieras.

Ante lo expuesto, las autoras, determinan que las cooperativas de ahorro y crédito son entes financieros dedicadas a brindar servicio y asistencia a sus socios sirviéndoles de soporte para ahorrar y hacer crecer su capital y de esta manera obtener beneficios como ganar intereses, acceder a créditos y demás servicios que brinde la institución; las cooperativas de ahorro y crédito centran sus esfuerzos en brindar un servicio de calidad que le permita tener el prestigio necesario para la captación de clientes.

2.1.1.1 COOPERATIVA DE AHORRO Y CRÉDITO CALCETA LTDA

La Cooperativa de Ahorro y Crédito Calceta Limitada cuenta con gran número de socios distribuidos en diferentes sucursales, en el Cantón 24 de Mayo tiene 2250 socios, en Manta 8082 socios, en Calceta 17462 y en Jama 673 socios.

- **Misión:** Contribuir al desarrollo socioeconómico de los microempresarios y de la población en general de la provincia de Manabí y del país, a través de productos y servicios financieros sostenibles y de calidad con enfoque de responsabilidad social.

- **Visión:** Ser una institución especializada socioeconómica de los sectores productivos de Manabí y del país (Cooperativa de Ahorro y Crédito Calceta Limitada, 2014).

2.1.1.2. ORGANIGRAMA ESTRUCTURAL

La cooperativa de ahorro y crédito Calceta limitada del cantón Bolívar es una de las entidades financieras más notables no solo en la cuidad, sino también de la provincia, cuenta con tres sucursales, en Manta, 24 de Mayo y Jama, las cuales han sido creadas con el fin de favorecer y apoyar sectores económicos dedicados a distintas labores comerciales y formas de vida diferente, dando la certeza de ser una institución confiable en la cual los socios se pueden sentir seguros de pertenecer, es por esto que la aceptación a la institución ha ido creciendo a través del tiempo y ha sido necesario crecer y evolucionar en función a las demandas de sus socios (Anexo 1).

2.2. TECNOLOGIAS DE LA INFORMACIÓN

Las tecnologías de información son las tecnologías que se necesitan para la gestión y transformación de la información, y muy en particular el uso de ordenadores y programas que permiten crear, modificar, almacenar, proteger y recuperar esa información, ya que la información es el activo más importante de la organización y debe ser administrada de mejor manera (Cobo, 2009).

Álvarez y Pérez (2004) citado por Ojeda, *et al.* (2010) indica que las tecnologías de información han impulsado de múltiples formas y al mismo tiempo han generado transformaciones en las organizaciones, los mercados y el mundo de la modernidad y de la posmodernidad. Son cambios que, además de sus grandes ventajas, han traído simultáneamente para las personas y las organizaciones, amenazas, riesgos y espectros de incertidumbre en los escenarios de internet, intranet, desarrollo tecnológico, gestión de la información, la comunicación y los sistemas.

Se considera tecnologías de información, según las autoras, a todo aquello que manipula información dentro de una organización, convirtiéndose en una herramienta importante para la organización y tratamiento de la misma, en este

grupo se encuentran inmersos los activos de hardware, equipos de red y personal que labora dentro de la institución, los cuales son considerados primordiales para el buen desempeño de las actividades dentro de la misma y que coadyuva al desarrollo y crecimiento de los sectores productivos del país permitiéndole realizar las actividades sin demoras para la satisfacción de sus clientes.

2.2.1. TECNOLOGÍAS DE INFORMACIÓN EN ECUADOR

El desarrollo y utilización de las Tecnologías de la Información en Ecuador es muy importante, ya que radica en su aporte a la transformación de la matriz productiva del país a través de la transferencia y difusión de nuevas tecnologías, como también la generación de empleos y la exportación de servicios. Las tecnologías de información impactan de forma transversal y tienen efectos positivos sobre los demás sectores de la economía, induce aumentos de productividad empresarial y contribuye a diversificar la oferta exportadora, constituyéndose en el motor más importante del crecimiento económico del siglo XXI, y contribuyendo con la reducción de la pobreza y las brechas sociales (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2014).

El personal que labora en las organizaciones hace uso diario de las tecnologías de la información para realizar su trabajo de forma rápida y efectiva representando una herramienta primordial para el desarrollo de la misma, ya que ayudan en el proceso de transformación y almacenamiento de la información facilitando al personal humano el acceso rápido a información actualizada y almacenada dentro de sus sistemas, al igual que permite el envío y recepción de información por medios electrónicos logrando que los procesos se lleven a cabo de forma inmediata sin necesidad de esperar la correspondencia u otros medios, ante ello las autoras expresan, que las tecnologías de la información fueron creadas para facilitar el trabajo que normalmente se llevaba a mano para mejorar los procesos y brindar servicios de calidad en un ambiente de trabajo sano y sin demoras.

2.2.2. IMPORTANCIA DE LAS TECNOLOGÍAS DE INFORMACIÓN

Hoy en día la era de la información invade las empresas, permitiendo aumentar la competencia de las mismas, tanto nacional como internacionalmente. Por tal razón es necesario la adquisición de buenos equipos de cómputo y software que satisfaga las necesidades permitiendo disminuir los costos de operación en las empresas y reducción de tiempo en la entrega de productos o servicios, asegurando a sus clientes tiempo, calidad y resultados óptimos. Por ende, la mejor manera de mantener estas características de empresa emprendedora, es la utilización de tecnologías de la información, ya que estas se presentan en las organizaciones desde los años 80, para beneficiar a las mismas, y hacerlas sobresalir entre sus competidores brindándoles a sus clientes mayores beneficios (Espinoza, 2009).

Las tecnologías de la información son de gran importancia en las instituciones, ya que ayudan en el desarrollo de sus actividades permitiendo que éstas se lleven a cabo de manera rápida y con menos esfuerzo, para así lograr brindar un mejor servicio a los clientes, convirtiéndose en recursos relevantes en todos los sectores productivos del país, como las instituciones financieras a las cuales les permite acceder a información rápidamente como por ejemplo los saldos de los clientes y el dinero que tienen disponible para retiro, evitando la consulta en libros que tardaría mucho más, además ayudan a una mejor y mayor organización dentro de las instituciones a la vez que genera un reto para muchas personas ya que les brinda la oportunidad de prepararse para así poder introducir nuevas tecnologías que apoyen en el crecimiento de la provincia y el país.

2.2.3. SEGURIDAD INFORMÁTICA EN TECNOLOGÍA DE INFORMACIÓN (TI)

La seguridad informática es el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos

tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización y que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos (Voutssas, 2010).

De acuerdo a Gaona (2013) la seguridad de la información busca un equilibrio entre el nivel de seguridad y el costo, el cual se logra implantando un conjunto adecuado de controles como políticas, procedimientos, estructuras organizativas y funciones de software, que han sido establecidos para el cumplimiento de los objetivos específicos de la seguridad de la empresa. Así mismo la contribución de Montesino *et al.* (2013) determina que la seguridad informática, o seguridad de la información, es la preservación de la confidencialidad, integridad y disponibilidad de la información. Esto se logra mediante la implantación de un grupo de controles que incluyen políticas, procedimientos, estructuras organizativas y sistemas de hardware y software

La información ha ido adquiriendo valor a través del tiempo, tanto es así que es considerada un activo fundamental de toda organización, ya que sin ella la empresa no pudiera llevar a cabo sus actividades, pero ésta se convierte en un blanco al cual apuntan muchas otras instituciones con fines diferentes como por ejemplo ofertar productos y servicios a las personas dependiendo de las actividades que estas realicen o en muchos casos para delinquir con ellos, por tal motivo es necesario que la organización adopte medidas de seguridad estrictas que le permitan proteger los datos de sus clientes, para lo que es necesario que el personal que trata datos sensibles tenga pleno conocimiento y conciencia de que la información suministrada por el cliente no es propiedad de la empresa por lo tanto debe de protegerla y evitar que caiga en manos de personas malintencionadas que puedan hacer mal uso de la misma y así dañar la integridad de las personas.

Villegas, *et al.* (2011) establece que para que un sistema informático se pueda definir como seguro, debe tener las características:

2.2.3.1 CONFIDENCIALIDAD

La confidencialidad se refiere a que la información sólo debe estar legible para los autorizados, es decir que solo personas autorizadas pueden acceder a la información.

Los datos de los clientes deben ser tratados con mucha cautela para evitar que caiga en las manos equivocadas y prevenir daños a terceras personas, ya que muchas veces proporcionar un dato pequeño de una persona a otra puede causar daños en ella, por esto la confidencialidad se trata de dar la información necesaria solo al dueño de la misma y ésta persona será quien decide a que institución se la proporciona y porque.

2.2.3.2 INTEGRIDAD

La integridad indica que la información sólo puede ser modificada por quien esté autorizado. Es un factor importante al momento que se recibe un documento digital o físico, dando la confianza de que el documento no ha sufrido ninguna alteración o corrupción.

Es importante que las instituciones almacenen en sus registros la información suministrada por el cliente sin enmiendas ni asumiendo cosas, ya que de esta forma los datos serian alterados y en muchos casos alejados de la realidad del mismo, ya que el registrar datos erróneos puede significar problemas para el cliente al momento de realizar otras actividades dentro y fuera de esta institución lo cual ocasiona molestias y en muchos casos la pérdida de clientes.

2.2.3.3 DISPONIBILIDAD

La disponibilidad es que la información debe estar disponible cuando se necesite, este implica que tanto el hardware como el software se mantengan funcionando correctamente y sea capaz de recuperarse rápidamente de cualquier fallo.

2.2.3.4 AUTENTICIDAD

Este término se refiere a los mecanismos de seguridad que posean los equipos que utilicemos para comunicarnos, permitiendo verificar si origen de los datos es correcto, de que fuente fueron enviados y la fecha que fueron enviados y recibidos.

2.2.4 SISTEMAS DE INFORMACIÓN

Pérez *et al.* (2009) manifiesta que los sistemas de información ofertan, regulan y gestionan todo tipo de recursos de información. Con este objetivo se producen los procesos de almacenamiento, identificación, transformación, organización, tratamiento y recuperación de la información. Los sistemas de información tiene cuatro funciones principales que son: recopilación de la información, acumulación de información, tratamiento de información y difusión de información.

Los sistema de información se han convertido en un pilar fundamental sobre el cual reposa una institución, pues con su uso los procesos dentro de la institución se llevan a cabo de una manera rápida y eficaz, permitiendo la correcta actualización, transformación y almacenamiento de información que resulte útil para a organización, por lo que es considerado un conjunto de procesos que recolectan datos de acuerdo a las necesidades de la institución, en donde esta almacena, procesa y transforma los datos para tener como

resultado información, el cual se distribuye para desempeñar sus funciones y servir de apoyo en la toma de decisiones en la organización.

2.2.5 ACTIVOS

El activo es considerado un recurso controlado por una entidad, identificado, cuantificado en términos monetarios del que se esperan fundadamente beneficios económicos futuros, derivados de operaciones ocurridas en el pasado, que han afectado económicamente dicha entidad (Marcotrigiano, 2011).

Los activos son los bienes más importantes de toda organización, que permite la realización de las actividades y generar flujo de efectivo, el cual van evolucionando al pasar el tiempo de acuerdo a las necesidades de los usuarios.

2.2.5.1 ACTIVOS DE HARDWARE

Según Gómez (2001) manifiesta que los activos que posee la empresa simbolizan los recursos que los dueños tienen para el desarrollo de la actividad productiva de la entidad y como resultado de las operaciones diarias que en un futuro le traerán beneficios económicos.

En referencia a activos de hardware, Revilla (2012) hace referencia que los recursos tecnológicos constituyen activos fundamentales para muchas empresas en la consecución de ventajas competitivas.

Los activos son de vital importancia para la organización, no solo por su valor adquisitivo, sino también porque son necesarios para el cumplimiento de procesos que realiza la organización diariamente y por lo tanto tienen que ser protegidos, por lo cual es importante estructurar los activos por tipos para tener una mejor visión de los mismos y mantenerlos organizados, de tal manera que permita identificar los más relevantes y así conocer los que necesitan mayor

protección contra las amenazas. Los tipos de activos más importantes son: estaciones de trabajo, servidores, equipos de impresión equipos de comunicación, sistemas de administración de energía, equipamiento auxiliar y talento humano.

2.2.5.2 AMENAZA

Pandini y Pallero (2013) indican que las amenazas son acontecimientos no deseados que pueden causar daños en los recursos de la organización, estas pueden ser intencionadas por el ser humano o pueden ser de origen natural como terremotos e inundaciones. Así mismo Meliá *et al*. (2010) hacen mención a que la amenaza es el objetivo del adversario para violar una vulnerabilidad relativa a la seguridad del sistema.

Todas las organizaciones necesitan contar con activos que contribuyan en el proceso de prestación de servicios, pero si bien es cierto que estos equipos facilitan el trabajo de los humanos también pueden representar problemas a la institución, ya que como todas las cosas están expuestos a varias amenazas que pueden materializarse causando daños dentro de la organización, es necesario que se prevean los recursos necesarios para evitar fallas, por esta razón es importante adaptarse a las nuevas tecnologías, ya que a medida que adquieren más activos se generan nuevas amenazas en la organización y hay que estar preparados para hacerles frente.

2.2.5.2.1 CLASIFICACIÓN DE LAS AMENAZAS

Las amenazas se clasifican en amenazas en amenazas intencionadas, no intencionadas y naturales.

Las amenazas intencionadas las ejercen usuarios no autorizados que acceden a la información o datos de la institución, los usuarios no autorizados pueden ser externos o pertenecientes a la propia organización y se pueden clasificar

como curioso o maliciosos. En cambio las amenazas no intencionadas provienen típicamente de empleados con poca formación que no han seguido los pasos para proteger sus contraseñas, asegurar adecuadamente sus ordenadores o actualizar con la frecuencia debida el programa antivirus, estos pueden implicar a los programadores o personal de proceso de datos y las amenazas naturales incluyen fallos de equipos y calamidades tales como incendios, inundaciones y terremotos que pueden causar la pérdida de equipos y datos, estas suelen afectar a la disponibilidad de los recursos y de la información (Gonzales *et al.,* 2010).

2.2.5.3 VULNERABILIDADES

Andrade *et al.* (2013) manifiesta que a medida que avanza la tecnología, también surgen nuevas amenazas informáticas, las cuales sólo buscan descubrir nuevas vulnerabilidades que pueden ser utilizadas para comprometer nuestros sistemas. Una vulnerabilidad o fallo de seguridad, es todo aquello que provoca que nuestros sistemas informáticos funcionen de manera diferente para lo que estaban pensados, afectando a la seguridad de los mismos, pudiendo llegar a provocar entre otras cosas la pérdida y robo de información sensible.

2.2.5.4 RIESGOS

El riesgo es la vulnerabilidad ante un potencial perjuicio o daño para las unidades, personas, organizaciones o entidades. Cuanto mayor es la vulnerabilidad mayor es el riesgo, pero cuanto más factible es el perjuicio o daño, mayor es el peligro. También puede definirse como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad (Rodríguez, 2015).

Ramírez (2009) hace alusión que el concepto riesgos ha estado tradicionalmente ligado a las potenciales amenazas e impactos generados por

múltiples eventos de origen natural tales como sismos, remoción de masas, inundaciones, entre otros. No obstante, en los últimos años ha emergido un campo de análisis de los riesgos asociados a la inserción y el desarrollo de eventos tecnológicos (industria química, telecomunicaciones, fuentes energéticas y alimenticias, e incluso el mismo escenario armamentista) aportando con ello relevantes elementos de análisis para pensar la compleja relación entre sociedad y ambiente, en un momento donde el progreso tecno científico representa concomitantemente el ascenso de una "sociedad del riesgo".

Todas las instituciones están expuestas a amenazas, que cuando se materializan pueden llegar a dañar en mayor o en menor grado a la organización, esto dependiendo de cómo la organización se ha preparado para hacerle frente a cada una de ellas, ya que al no estimar el impacto que tendrían los riesgos estos pueden ser irreparables y dejar secuelas como fugas de información o la suspensión del servicio dentro de la organización lo cual causa pérdidas no solo materiales sino también económicas por lo que es importante conocer los riesgos a lo que están expuestos los activos, y crear medidas de seguridad para mitigarlos, prevenirlos o en ciertos casos trasladarlos.

2.3 ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN (TI)

Vásquez (2010) refiere que los riesgos tecnológicos están subestimados en los procesos de negocio y son relegados a los especialistas técnicos.
Administrar riesgos tecnológicos no puede ser tema exclusivo de la Dirección de TI:

- Cada parte o área de la empresa debe tener un papel protagónico.
- Un posible impacto en los sistemas afectaría a diversas áreas de la organización en igual o mayor manera

La información y tecnología representan uno de los más valiosos pero menos comprendidos activos de una empresa. La administración de riesgos tecnológicos juega un papel crítico en la protección de la información de las cooperativas, teniendo como requerimiento de la dirección la implementación de políticas, planes y procedimientos que aseguren razonablemente que los objetivos de negocio de cumplan y que los eventos no deseados se prevengan o detecten y corrijan.

2.3.3 CLASES DE RIESGOS

Departamento Administrativo de la Función Pública (2011) considera que entre las clases de riesgos que pueden presentarse están:

- **Riesgo Estratégico**

Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

- **Riesgos de Imagen**

Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

- **Riesgos Operativos**

Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

- **Riesgos Financieros**

Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

- **Riesgos de Cumplimiento**

Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad. Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Para todas las instituciones es muy importante tener una buena imagen corporativa inspirar confianza a sus clientes para que se sientan seguros de pertenecer a ella, en el caso de las entidades financieras estar preparados y tener la solidez económica suficiente para apoyar a sus clientes en el momento requerido y tener la capacidad de servir de soporte para ellos sin excusas, por lo que es importante estimar los riesgos a los que están expuestos como organización lo cual le permita tomar medidas que le permitan mantenerse operante durante el tiempo y así darle un procedimiento indicado.

2.3.4 ANÁLISIS DE RIESGOS

La sociedad actual está inmersa en un ambiente tecnológico en donde la información juega un papel importante en las actividades, el cual las TI se ha convertido en un factor de riesgo y unos de los más importantes para la mejora y eficiencia de productividad para las empresas, pero la tecnología no es perfecta, en ella existen vulnerabilidades, amenazas y riesgos, el cual los riesgos se pueden disminuir pero nadie puede asegurar que no va haber riesgo en la organización (Gómez *et al.,* 2010).

Suarez y Menéndez (2011) hacen referencia a que es importante conocer los riesgos al que están sometidos los activos de TI, para así poder gestionarlos, el cual para ello es importante realizar un análisis de riesgo, ya que es el inicio de una gestión planificada y ordenada de los riesgos operacionales y de TI.

A través de un análisis de riesgos las instituciones pueden identificar sus falencias en cuanto a seguridad, fallos técnicos, desastres naturales e industriales, entre otros, para darle el tratamiento adecuado en el momento que ocurra, ayudando a reducir el impacto para evitar que afecte a los procesos, ayudándole a una pronta recuperación ante el desastre y en la reducción de costos.

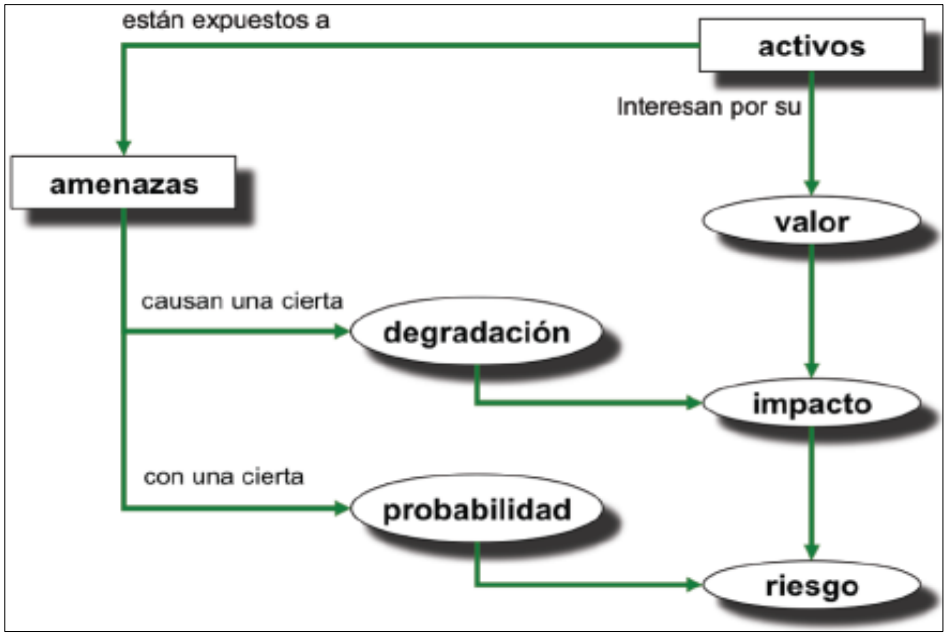


Figura 2.02. Elementos del análisis de riesgos
Fuente: Magerit

2.3.4.1 BENEFICIOS DEL ANÁLISIS DE RIESGO

Según indica Jiménez (2008) para saber qué medidas se deben tener cuando ocurra algo inesperado en la organización se debe implementar la valoración y gestión de riesgos para evitarlo, pero que dada su materialización, nuestras acciones serán precisas y correctas, reduciendo los tiempos de atención y

restando costos innecesarios en la atención de eventos previamente analizados.

Así entre sus principales beneficios se encuentran asegurar la continuidad operacional de la organización, manejar apropiadamente las amenazas y riesgos críticos, mantener una estrategia de protección y de reducción de riesgos, justificar una mejora continua de la seguridad de la información y minimizar el impacto con reducción de costos que incluyen pérdidas de dinero, tiempo y mano de obra. Aunque el análisis de riesgos en las organizaciones nos es nuevo, pero ha adquirido recientemente una gran importancia, especialmente en el sector público de nuestro país, dado el establecimiento de nuevas normativas por parte de la Contraloría General de la República en relación con el control interno, la valoración de riesgos y la gestión de las tecnologías de información. Pero se debe percibir el valor agregado de estas normativas, en razón no solo de su cumplimiento obligatorio, sino como apoyo en la previsión de eventos perjudiciales a la organización que permita ahorrarle dinero, tiempo y esfuerzos.

Las instituciones que cuentan con un análisis de riesgos oportuno les permite tener una ventaja sobre otras, ya que le proporciona información importante al momento de su ocurrencia, sirviendo de apoyo en la toma de decisiones gerenciales en cuanto al tratamiento del riesgo, garantizando el buen desempeño de las actividades empresariales, pronta recuperación ante el desastre y continuidad del negocio de forma rápida.

2.4 METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN (MAGERIT)

Magerit es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información y es reconocida por ENISA (Agencia Europea de Seguridad de las Redes y de la Información) y promovida por el Consejo Superior de

Administración Electrónica, con el fin de sistematizar el análisis de los riesgos que pueden presentar los activos de una organización.

La metodología Magerit resulta ser la opción más efectiva y completa ya que protege la información en cuanto a integridad, confidencialidad, disponibilidad y otras características importantes para garantizar la seguridad de los sistemas y procesos de la organización. La aplicación de metodologías de análisis de riesgos es de utilidad a las organizaciones para tener un mayor control sobre sus activos, su valor y las amenazas que pueden impactarlas, obligándolas a implementar medidas de seguridad que garanticen el éxito de sus procesos y una mayor competitividad en el mundo empresarial (Abril *et al.,* 2013).

Magerit es una metodología que se utiliza para dar a conocer el nivel de seguridad que tienen los sistemas de información e implementar salvaguardas que permitan mitigar las vulnerabilidades y reducir los riesgos que existen en los activos tecnológicos de la institución, con el fin de garantizar la confidencialidad, integridad, disponibilidad, de la información con el fin de brindar confianza a los clientes hacia la empresa. Esta metodología presenta una guía la cual le permite implementarse en cualquier institución sin importar lo grande o pequeña que sea, esta se divide en tres libros, el primero describe la estructura de la metodología, el segundo presenta los inventarios para enfocar el análisis de riesgos y el tercero una guía técnica.

Cordones y Piedra (2011) establecen que Magerit persigue los siguientes objetivos directos e indirectos los cuales son:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos:

- **Modelo de valor:** Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.
- **Mapa de riesgos:** Relación de las amenazas a que están expuestos los activos.
- **Declaración de aplicabilidad:** Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.
- **Evaluación de salvaguardas:** Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.
- **Estado de riesgo:** Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.
- **Informe de insuficiencias:** Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.
- **Cumplimiento de normativa:** Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.
- **Plan de seguridad:** Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos.

2.4.1. MÉTODO DE ANÁLISIS DE RIESGOS

La Dirección General de Modernización Administrativa (2012a) señala que el análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia o expectativa de materialización de la amenaza.

2.4.1.1. PASO 1: ACTIVOS

Los activos son definidos como los recursos con los que cuenta una organización, estos son componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización, el cual incluye: información, datos, servicios o software, hardware, comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

En esta fase de la metodología Magerit se determinan los activos críticos con los que cuenta la organización para el desempeño de sus actividades, para luego analizar las amenazas a que estas expuestos. Además también se pueden identificar otros activos de gran relevancia como: Datos, servicios, las aplicaciones informáticas, los equipos informáticos, los soportes de información, el equipamiento auxiliar, las redes de comunicaciones, las instalaciones, las personas, entre otros. No todos los activos son de la misma

especie y dependiendo del tipo de activo al que pertenece se puede determinar las amenazas y salvaguardas aplicadas según el tipo de activo a proteger.

2.4.1.1.1. DEPENDENCIAS

La dependencia entre los activos es muy importante a la hora de realizar una análisis de riesgos, ya que es una forma de ver cuándo se encuentra afectado un activo superior por alguna amenaza y que se presenta en un activo inferior.

Los activos vienen a formar árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o 'superiores' depende de los activos que se encuentran más abajo o 'inferiores'. Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior.

Magerit ha desarrollado una forma de dependencia de los activos los cuales son:

El equipamiento informático

- aplicaciones (software)

Equipos informáticos (hardware)

- comunicaciones
- soportes de información: discos, cintas, etc.

El entorno: activos que se precisan para garantizar las siguientes capas

- Equipamiento y suministros: energía, climatización, etc.
- Mobiliario

Los servicios subcontratados a terceros

Las instalaciones físicas

- El personal
- Usuarios
- Operadores y administradores
- Desarrolladores

2.4.1.1.2. DIMENSIONES

De un activo puede interesar calibrar diferentes dimensiones:

- **Su confidencialidad:** ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
- **Su integridad:** ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
- **Su disponibilidad:** ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios (Dirección General de Modernización Administrativa, 2012a).

2.4.1.1.3. CRITERIOS DE VALORACIÓN

Para valorar los activos vale, teóricamente cualquier escala de valores, sin embargo es muy importante que se use una escala común para todas las dimensiones, permitiendo comparar riesgos, se use una escala logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas y se use un criterio homogéneo que permita comparar análisis realizados por separado.

Si la valoración es económica, hay poco más que hablar: dinero. Pero frecuentemente la valoración es cualitativa, quedando a discreción del usuario; es decir, respondiendo a criterios subjetivos (Dirección General de Modernización Administrativa. 2012b).

Cuadro 2.01. Escalas de criterio de valoración

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 efecto práctico

Fuente: Dirección General de Modernización Administrativa (2012b)

2.4.1.2. PASO 2: AMENAZAS

Dirección General de Modernización Administrativa (2012a) indica que el siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son cosas que ocurren y que afectan a los activos el cual pueden ser de origen natural como terremotos e inundaciones, de origen industrial, defectos en las aplicaciones y causas por las personas de forma deliberada.

2.4.1.2.1. VALORACIÓN DE LAS AMENAZAS

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, el cual una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos: según su degradación que es cuan perjudicado resultaría el valor del activo y según la probabilidad, si es probable o improbable es que se materialice la amenaza.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela cualitativamente por medio de alguna escala nominal:

Cuadro 2.02. Degradación del valor

MA	muy alta	casi seguro	Fácil
A	Alta	muy alto	Medio
M	media	posible	Difícil
B	Baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Fuente: Dirección General de Modernización Administrativa (2012a)

A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar un año como referencia, de forma que se recurre a la tasa anual

de ocurrencia como medida de la probabilidad de que algo ocurra. Son valores típicos:

Cuadro 2.03. Probabilidad de ocurrencia

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Fuente: Dirección General de Modernización Administrativa (2012a)

2.4.1.2.2. EFECTO DE LAS SALVAGUARDAS

Las salvaguardas entran en un cálculo de riesgos de dos formas:

- **Reduciendo la probabilidad de las amenazas.** Se llaman salvaguardas preventivas, las cuales llegan a impedir completamente que la amenaza se materialice.

- **Limitando el daño causado.** Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye.

2.4.1.2.3. DETERMINACIÓN DEL IMPACTO

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza, conociendo el valor de los activos en varias dimensiones y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos.

Para la valoración del impacto, se consideró la siguiente escala para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

- **MB:** muy bajo
- **B:** bajo
- **M:** medio
- **A:** alto
- **MA:** muy alto

La Dirección General de Modernización Administrativa (2012c) plantea que se puede calcular el impacto en base a tablas sencillas de doble entrada:

Cuadro 2.04. Calculo del impacto en base a tablas sencillas doble entrada.

impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: Dirección General de Modernización Administrativa (2012c)

Aquellos activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata.

2.4.1.2.4. DETERMINACIÓN DEL RIESGO

Se denomina riesgo a la medida del daño probable sobre un sistema, conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo el cual son:

- **Zona 1:** Riesgos muy probables y de muy alto impacto.
- **Zona 2 Franja amarilla:** cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo.
- **Zona 3:** Riesgos improbables y de bajo impacto.
- **Zona 4:** Riesgos improbables pero de muy alto impacto.

La escala para calificar la frecuencia del riesgo según la metodología Magerit mediante alguna escala sencilla es:

- **MF:** muy frecuente (a diario)
- **F:** frecuente (mensual)
- **FN:** frecuencia normal (anual)
- **PF:** poco frecuente (cada varios años)

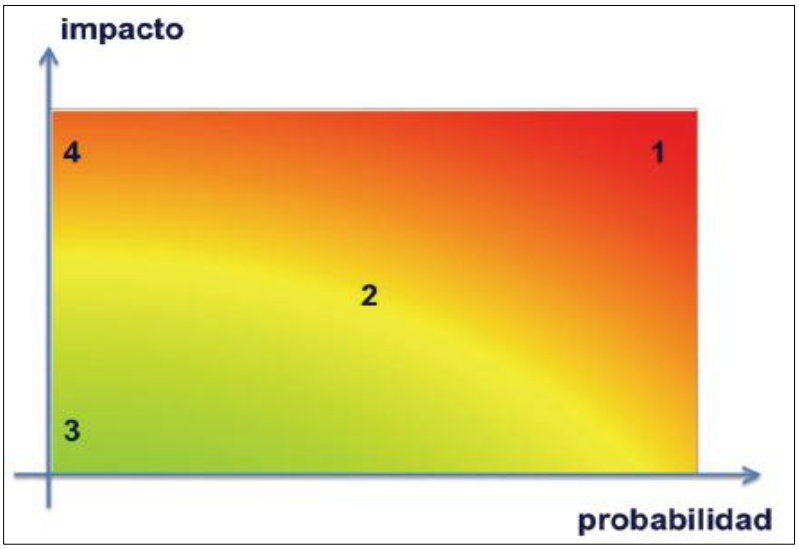


Figura 2. 03. Riesgos en función del impacto y la probabilidad

La Dirección General de Modernización Administrativa (2012c) indica que se modelan impacto, probabilidad y riesgo por medio de escalas cualitativas:

Cuadro 2.05. Escalas cualitativas del impacto, probabilidad y riesgos

Escalas		
Impacto	**Probabilidad**	**Riesgo**
MA: muy alto	**MA:** prácticamente seguro	**MA:** critico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Fuente: Dirección General de Modernización Administrativa (2012c)

Pudiendo combinarse impacto y frecuencia en una tabla para calcular el riesgo:

Cuadro 2.06. Cálculo del riego con el impacto y la frecuencia

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: Dirección General de Modernización Administrativa (2012c)

La Dirección General de Modernización Administrativa (2012b) presenta un catálogo de amenazas posibles sobre un activo y para cada amenaza se presenta un cuadro como el siguiente:

Cuadro 2.07. Descripción de las amenaza de acuerdo al tipo de activo

{código} descripción sucinta de lo que puede pasar	
Tipos de activos: • Que se pueden ver afectados por este tipo de amenazas.	**Dimensiones:** De seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más o menos relevante
Descripción: Complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas.	

Fuente: Dirección General de Modernización Administrativa (2012b)

2.4.1.3. PASO 3: SALVAGUARDAS

La Dirección General de Modernización Administrativa (2012a) indica que las salvaguardas o contra medidas son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos como programas o equipos, otras seguridad física y, por último, está la política de personal.

2.4.1.3.1. SELECCIÓN DE SALVAGUARDAS

Ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedar con aquellas que son relevantes para lo que hay que proteger. En esta criba se deben tener en cuenta los siguientes aspectos:

- Tipo de activos a proteger, pues cada tipo se protege de una forma específica
- Dimensión o dimensiones de seguridad que requieren protección
- Amenazas de las que se necesitan proteger
- Si existen salvaguardas alternativas

Además, es prudente establecer un principio de proporcionalidad y tener en cuenta:

- El mayor o menor valor propio o acumulado sobre un activo, centrando en lo más valioso y obviando lo irrelevante
- La mayor o menor probabilidad de que una amenaza ocurra, centrando en los riesgos más importantes.
- La cobertura del riesgo que proporcionan salvaguardas alternativas

Esto lleva a dos tipos de declaraciones para excluir una cierta salvaguarda del conjunto de las que conviene analizar:

- **No aplica:** se dice cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración.
- **No se justifica:** se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que se tiene que proteger.

Como resultado de estas consideraciones se dispondrá de una “declaración de aplicabilidad” o relación de salvaguardas que deben ser analizadas como componentes nuestro sistema de protección.

2.4.1.3.2. TIPOS DE PROTECCIÓN PRESTADOS POR LAS SALVAGUARDAS

Cuadro 2.08 Tipos de salvaguardas

Efecto	Tipo
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente: Dirección General de Modernización Administrativa (2012a)

2.4.1.4. PASO 4: IMPACTO RESIDUAL

Según la Dirección General de Modernización Administrativa (2012a) después de cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que se ha modificado el impacto, desde un valor potencial a un valor residual.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real. El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

2.4.1.5. PASO 5: RIESGO RESIDUAL

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que se ha modificado el riesgo, desde un valor potencial a un valor residual.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual. La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real. El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

El riesgo residual es el riesgo que queda después de implementar un conjunto de salvaguardas, el cual si el riesgo residual es mayor al valor de las salvaguardas, las salvaguardas implementadas no tendrían sentido ya que no estaría ayudando a prevenir las amenazas en la organización (Dirección General de Modernización Administrativa, 2012a).

CAPÍTULO III. DESARROLLO METODOLÓGICO

El trabajo investigativo se realizó en la oficina matriz de la Cooperativa de Ahorro y Crédito Calceta Limitada del Cantón Bolívar, ubicada en la calle Ricaurte y Salinas, la cual proporcionó información disponible en cuanto a los procesos a seguir ante posibles riesgos tecnológicos en la institución.

3.1. MAGERIT

Se usó la metodología Magerit en el análisis de riesgos realizado en la Cooperativa de Ahorro y Crédito Calceta Limitada, con el fin de estimar las vulnerabilidades a las cuales está expuesta.

Con el fin de adaptar la metodología al trabajo realizado en la institución se tomaron en cuenta los siguientes pasos:

1. Determinar los activos relevantes para la institución.
2. Determinar a qué amenazas están expuestos los activos.
3. Estimar el impacto
4. Estimar el riesgo

La metodología Magerit cuenta con 5 pasos definidos, de los cuales se creyó oportuno obviar el paso 3 el cual es determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo, considerando que después de haber realizado el trabajo se obtendrá un escenario real para proponer las salvaguardas idóneas según sea el caso.

Para iniciar con el proceso que sigue Magerit, se realizó una visita al gerente de la institución y a la encargada del Departamento de Riesgos, con el fin de conocer sobre los riesgos que ha tenido la institución, cómo han sido tratados y los daños que ha sufrido ya que para hacer un análisis de riesgos es necesario conocer a fondo el lugar, y de este modo se asegura un mejor entendimiento de los escenarios.

3.1.1. IDENTIFICACIÓN DE ACTIVOS

Con el fin de entender el negocio, se realizó una visita a la institución en un día normal de labores para identificar los procesos de mayor relevancia para la institución, luego con la ayuda del personal del Departamento de Sistemas se realizó el inventario de equipamiento informático de la Cooperativa por tipos, con los precios de adquisición, relevando su importancia dentro de la institución, el cual es el siguiente:

Cuadro 3.02. Inventario de activos de la Cooperativa de Ahorro y Crédito Calceta Limitada (Servidores)

Servidores								
Item	Detalle	Unidad	Marca	Capacidad	Memoria	Fecha de ad.	Precio	Total
1	Servidor 2 Intel Xeon de 2GHZ	2	Hp	1920 GB	16 GB	41487	22500	45000
2	Servidor Xeon E3-1225 V3 3.10GHZ	2	Lenovo	1 TB	8 GB	41791	2000	4000
3	Servidor 2 Intel Xeon de 2.4GHZ	1	Ibm	500 GB	4 GB	40756	2000	2000
4	Servidor 2 Intel Xeon DE 3GHZ	1	Ibm	1920 GB	4 GB	40513	2000	2000
5	Servidor Intel XeonE 2.8GHZ	1	Ibm	80 GB	1 GB	39083	2000	2000
6	Servidor Intel Pentium D 3 GHZ	2	Ibm	120 GB	4 GB	39722	2000	2000
							TOTAL	57000

Fuente: Cooperativa Calceta.

Cuadro 3.03. Inventario de activos de la Cooperativa de Ahorro y Crédito Calceta Limitada (Equipos de Impresión)

Equipos de Impresión						
Item	Detalle	Unidad	Marca	Fecha de ad.	Precio	Total
1	Impresora MG-2120	2	Canon	feb-14	300	600
2	Impresora ML-2010	3	Samsung	ene-14	800	2400
3	Impresora TX410	1	Epson	feb-14	850	850
4	Impresora MP-250	6	Canon	sep-08	180	1080
5	Impresora MP-280	1	Canon	ene-07	180	180
6	Impresora FX-890	2	Epson	nov-12	900	1800
7	Impresora TMU-950S	3	Epson	ene-14	1000	3000
8	Impresora ML-2165	1	Samsung	feb-14	250	250
9	Impresora MP-230	2	Canon	dic-11	150	300
10	Impresora P361A	1	Epson	feb-07	350	350
11	Impresora FX-890	1	Samsung	feb-15	900	900
16	Impresora LX-355	1	Epson	feb-14	750	750
17	Impresora FX-890	1	Samsung	feb-15	900	900
14	Impresora WC4118	1	Xerox	ene-14	3500	3500
12	Copiadora Aficio MP301	1	Ricoh	feb-14	3800	3800
15	Copiadora Studio 2505	1	Toshiba	ago-10	3800	3800
13	Fax KX-FT981LA	1	Panasonic	ene-14	3400	3400
					TOTAL	24460

Fuente: Cooperativa Calceta.

Cuadro 3.01. Inventario de activos de la Cooperativa de Ahorro y Crédito Calceta Limitada (Estaciones de Trabajo)

Estaciónes de trabajo							
Item	**Detalle**	**Unidad**	**Marca**	**Capacidad**	**Memoria**	**Fecha de ad.**	**Precio**
1	Computador Intel Core I7-4770	1	Xtratech	1 TB	8 gb	feb-15	1550
2	Computador Core I7-4770 3.40 GHZ	1	Xtratech	1 TB	9 gb	abr-15	1550
3	Computador Core I7-3770 3.4 GHZ	1	Xtratech	1 TB	4 gb	ene-14	1550
4	Computador Intel Core I7-4770	1	Xtratech	1TB	8 gb	feb-15	1550
5	Computador Intel Pentium IV 2.66 GHZ	1	Xtratech	1160 GB	3 gb	jun-06	1200
6	Computador Intel Pentium IV 3.0 GHZ	1	Intel	120 GB	1 GB	jul-06	1200
7	Computador Core I7-3770 3.40 GHZ	1	Intel	1 TB	4 GB	ene-14	1550
8	Computador Core I7-2600 3.40 GHZ	1	Intel	500 GB	2 GB	may-11	1400
9	Computador Intel Core I7-2600 3.4 GHZ	1	Xtratech	1 TB	2 GB	sep-12	1550
10	Computador Untel Core I7-2600 3.4 GHZ	1	Xtratech	120 GB	2 GB	sep-12	1550
11	Compuador Intel Pentium 4 3.00 GHZ	1	Intel	121 GB	1 GB	ene-06	1200
12	Computador Core 2 DUO E4500 2.2 GHZ	1	Intel	160 GB	2 GB	sep-08	1200
13	Computador Core I7-2600 3.40 GHZ	1	Intel	500 GB	2 GB	may-11	1400
14	Computador Core I7-2600 3.40 GHZ	1	Xtratech	1 TB	4 GB	oct-12	1550
15	Computador Intel Pentium D 3.00 GHZ	1	Xtratech	500 GB	1 GB	dic-08	1200
16	Computador Intel Pentium 3.00GHZ	1	Intel	200 GB	1 GB	feb-07	1200
17	Computador Intel Celeron 1.7 GHZ	1	Xtratech	40 GB	255 MB	feb-07	1200
18	Computador Intel Pentium D 1.6 GHZ E2140	1	Xtratech	160 GB	1 GB	oct-12	1550
19	Computador Intel Core I3 3.07 GHZ	1	Xtratech	500 GB	2 GB	ago-10	1200
20	Computador Intel Core I3 540 3.07 GHZ	1	Xtratech	500 GB	2 GB	ago-10	1200
21	Computador Intel Core I7 3770 3.4 GHZ	1	Xtratech	500 GB	2 GB	dic-12	1550
22	Computador Intel Core 2 QUAD Q8400 2.66 GHZ	1	Xtratech	500 GB	2 GB	jun-10	1200
23	Computador Intel Core I7 870 2.93 GHZ	1	Xtratech	160 GB	2 GB	dic-11	1400
24	Computador Intel Core2 DUO E7500 2.94 GHZ	1	Xtratech	500 GB	4 GB	oct-07	1200
25	Computador Core 2 QUAD Q8400 2.66 GHZ	1	Xtratech	500 GB	4 GB	jun-10	1200
26	Computador Core I7-3770 3.40 GHZ	1	Xtratech	2 TB	4 GB	dic-11	1400
27	Computador Intel Dual Core E2160 1.80 GHZ	1	Xtratech	160 GB	1 GB	dic-07	1200
28	Computador CoreE I7 - 2600 3.40 GHz	1	Xtratech	470 GB	2 GB	mar-11	1400
29	Computador Core I7-2600 3.40 GHZ	1	Xtratech	500 GB	2 GB	mar-11	1400
30	Computador Core I7-3770 3.4 GHZ	1	Xtratech	2 TB	2 GB	feb-14	1550
31	Computador Core I7-870 2.93 GHZ	1	Intel	500 GB	4 GB	nov-12	1550
32	Computador Core 2 QUAD Q6600 2.4 GHZ	1	Intel	500 GB	2 GB	jun-10	1200
33	Computador Core I7-4770 3.40 GHZ	1	Xtratech	1 TB	8 GB	abr-15	1550
34	Computador Core I7-870 2.93 GHZ	1	Xtratech	1 TB	4 GB	nov-12	1550
35	Computador Core I7-870 2.93 GHZ	1	Xtratech	1 TB	4 GB	nov-12	1550
36	Computador Pentium D 2160 1.70 GHZ	1	Intel	160 GB	2 GB	dic-08	1200
						TOTAL	**49650**

Fuente: Cooperativa Calceta.

Cuadro 3.04. Inventario de activos de la Cooperativa de Ahorro y Crédito Calceta Limitada (Computador portátil)

Computador Portatil								
Item	Detalle	Unidad	Marca	Capacidad	Memoria	Fecha de ad.	Precio	Total
1	Portatil Pavilon 2725LA	1	Hp	160 GB	4 GB	sep-08	950	950

Fuente: Cooperativa Calceta.

Cuadro 3.05. Inventario de activos de la Cooperativa de Ahorro y Crédito Calceta Limitada (Equipos de comunicación)

Equipos de comunicación						
Item	Detalle	Unidad	Marca	Fecha de ad.	Precio	Total
1	Switch GbE2c Layer 2/3 Ethernet Blade	1	Hp	mar-13	3200	3200
2	Switch SG500-52	1	Cisco	mar-13	2500	2500
3	Switch SG500-52	1	Cisco	abr-13	3400	3400
4	Central Telefonica KX-TES824	2	Panasonic	feb-08	1200	2400
					TOTAL	11500

Fuente: Cooperativa Calceta.

Cuadro 3.06. Inventario de activos de la Cooperativa de Ahorro y Crédito Calceta Limitada (Sistemas de Administración de Energía)

Sistemas de Administración de Energía						
Item	Detalle	Unidad	Marca	Fecha de ad.	Precio	Total
1	Ups Prestige 3000 20 KWA	1	POWERWARE	mar-13	15000	15000

Fuente: Cooperativa Calceta.

Cuadro 3.07. Inventario de activos de la Cooperativa de Ahorro y Crédito Calceta Limitada (Otros activos de Hardware)

Otros Activos de Hardware						
Item	DETALLE	Unidad	Unidad	Fecha de ad.	Precio	Total
1	Cámara Digital DMC-LS80	1	LUMIX	ene-08	600	600
2	Cámara Ip de Seguridad STC-165	3	STV	ene-08	200	200
3	Lector de Firmas D-LBK460-HSDR	1	TOPAZ	ene-08	450	450
4	Reloj Biométrico de Control de Asistencia	1	ANVIZ	feb-13	350	350
5	Reloj Biométrico de Control de Acceso	5	ZKTECO	feb-13	300	1500
					TOTAL	3100

Fuente: Cooperativa Calceta.

Cuadro 3.08. Inventario de activos de la Cooperativa de Ahorro y Crédito Calceta Limitada (Softwares)

DETALLE	LICENCIA	PRECIO DE AD.
Base de datos Oracle 2cc	PROPIO	27000
Base de datos SQL Server 2007	PROPIO	2500
Core Financiero Softbank 2.16	PROPIO	60000
Sistema Caefic	PROPIO	20000
PowerBuilder 12.5	PROPIO	5000
Antivirus Mcafee	PROPIO	2300
Winrar	LIBRE	0
Adobe Reader	LIBRE	0
Zero	LIBRE	0
Teamviewer	LIBRE	0
Vnc	LIBRE	0
Sistema de correo Electronico Oulook	PROPIO	0
Sitio web empresarial	PROPIO	0
	TOTAL	116800

Fuente: Cooperativa Calceta.

Una vez realizado el inventario de los activos de la institución, se procedió a la revisión de la nómina del personal que labora en cada uno de los departamentos de la cooperativa y la persona responsable del mismo.

Cuadro 3.09. Talento Humano de la Cooperativa de Ahorro y Crédito Calceta

Talento Humano			
Ítem	**Departamento**	**Responsable**	**# de Empleados**
1	Colocaciones	Econ. Lilian Magdalena Álvarez Cedeño	9
2	Captaciones	Tlgo. Martha Andrea Correa Zambrano	7
3	Financiero	Lcda. María Isabel Vidal Loor	3
4	Talento Humano	Ing. María Ángeles Vera Rivas	3
5	Dirección de Administración y Operaciones	Ing. Patricio Rubén Maya Mendoza	2
6	Riesgos	Econ. Helen Mariana Bravo Bravo	1
7	Cumplimiento	Tlgo. José Iván Caicedo Farías	1
8	Auditoria	Lcda. Rosa Amparo Vélez Mendoza	1
9	Secretaria	Ing. Jessie Rebeca Gonzáles Burgos	2
10	Sistemas	Párraga Loor Ramón Geovanny	4
		Total	**33**

Fuente: Cooperativa Calceta.

3.1.2. PROCESOS DE LA INSTIUCIÓN

La Cooperativa de Ahorro y Crédito Calceta Limitada se encuentra dividida por departamentos, los cuales brindan servicios de acuerdo a sus competencias, de éstos departamentos se han seleccionado los que se consideran más relevantes los cuales son Captaciones y Colocaciones, los procesos de soporte: Tecnología de Información, Riesgos, Auditoria Interna, Cumplimiento, que es donde se llevan a cabo las operaciones de mayor importancia dentro de la institución, a continuación se describe en detalle los procesos que se llevan a cabo en cada uno de ellos.

3.1.2.1. CAPTACIONES

En este departamento se realizan todas las operaciones relacionadas a la recepción de dinero de los socios, por concepto de depósitos, transferencias, entre otros.

Gestión de Captaciones

- ✓ Promoción de cuentas
- ✓ Control y cierre de cuentas
- ✓ Ejecución de seguimiento de planes
- ✓ Plan futuro

Captaciones depósito a plazo fijo

- ✓ Información de plazo fijo
- ✓ Apertura plazo fijo
- ✓ Cancelación renovación y endoso plazo fijo
- ✓ Pérdida de certificado de plazo fijo
- ✓ Archivo de plazo fijo
- ✓ Prevención y detección de lavado de activos plazo fijo
- ✓ Cuadro plazo fijo

Cajas

- ✓ Apertura de caja
- ✓ Depósitos
- ✓ Retiros
- ✓ Prestamos
- ✓ Faltantes y sobrantes
- ✓ Custodia de dinero
- ✓ Cierre de caja
- ✓ Archivo
- ✓ Prevención y detección de lavado de activos
- ✓ Billetes falsos

- ✓ Reposición de fondos
- ✓ Evacuación de fondos
- ✓ Depósito de cheques
- ✓ Bono de desarrollo humano
- ✓ Cajero automático
- ✓ Ahorro móvil
- ✓ PuntoMático

3.1.2.2. COLOCACIONES

En colocaciones se otorga créditos a los socios, con el compromiso de devolución del mismo a manera de cuotas con un interés como compensación al acreedor.

Créditos

- ✓ Información a socios
- ✓ Recepción de documentos
- ✓ Verificación e inspección
- ✓ Análisis, evaluación y resolución
- ✓ Instrumentación
- ✓ Desembolso
- ✓ Recuperación de créditos S.P.I. (Sistema de Pagos Interbancarios)
- ✓ Créditos vinculados
- ✓ Castigo de créditos

Microcrédito

- ✓ Promoción información microcrédito
- ✓ Recepción solicitudes
- ✓ Verificación e inspección
- ✓ Análisis y aprobación
- ✓ Otorgamiento desembolso
- ✓ Seguimiento y recuperación

Microcrédito grupal

- ✓ Identificación y evaluación de comunidades
- ✓ Constitución de grupos comunales
- ✓ Formalización y solicitud de crédito
- ✓ Desembolso de crédito
- ✓ Administración de cartera supervisión, recuperación, control de morosidad
- ✓ Cierre de ciclo

3.1.2.3. TECNOLOGÍA DE INFORMACIÓN

En tecnologías de información se realiza todo el trabajo relacionado a la organización de la información en el software institucional, el desarrollo y mejoramiento de herramientas de trabajo para los usuarios, y de mantener operante el sistema de la institución.

- ✓ Inicio de día
- ✓ Fin de día
- ✓ Respaldo de las bases de datos
- ✓ Data Center
- ✓ Internet
- ✓ Desarrollo de software
- ✓ Monitoreo de la red y comunicaciones
- ✓ Telecomunicaciones
- ✓ Soporte técnico
- ✓ Soporte técnico de hardware
- ✓ Mantenimiento de equipos
- ✓ Soporte técnico de software
- ✓ Recuperación de bases de datos
- ✓ Reportes y estructuras

3.1.2.4. RIESGOS

Este departamento es el encargado del análisis de los riesgos que tiene la institución, especialmente enfocado en los riesgos financieros con el fin de proveer soluciones oportunas que ayuden a una buena gestión del riesgo.

- ✓ Calificadora de riesgos
- ✓ Estructura reportes
- ✓ Generación y monitoreo de modelos y herramientas
- ✓ Comité de riesgos

3.1.2.5. AUDITORÍA INTERNA

Este departamento se ocupa de la valoración independiente de las actividades que agregan valor y mejoran las operaciones de la institución, y que contribuyen al cumplimiento de sus objetivos y metas.

- ✓ Plan anual
- ✓ Evaluación y seguimiento
- ✓ Comité de auditoría

3.1.2.6. CUMPLIMIENTO

En auditoria interna se realizan las actividades de control, de que se realicen los cambios y mejoras establecidas por los organismos de control institucional y externo en el tiempo establecido.

- ✓ Plan anual
- ✓ Evaluación y seguimiento
- ✓ Comité de ética
- ✓ Estructuras reportes

3.1.3. ANÁLISIS FODA DEL DEPARTAMENTO TECNOLOGÍAS DE INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO CALCETA LIMITADA

FORTALEZAS

- ✓ Personal Técnico del departamento totalmente comprometido con la cooperativa y sus objetivos.
- ✓ Respaldo por parte de los directivos para la actualización de la plataforma tecnológica.
- ✓ Empleados del departamento con predisposición al trabajo en grupo y bajo presión, así como dinámico y abierto al cambio.
- ✓ Conocimiento del sistema SOLFBANK.
- ✓ Diversidad de productos de ahorro y captaciones
- ✓ Diversidad de productos de crédito Prestación de Servicios complementarios (cajeros automáticos, tarjetas de débito, remesas, transferencias interbancarias, Ahorro móvil, entre otras.)
- ✓ Plataforma tecnológica actualizada
- ✓ Respaldo de información en línea y con disponibilidad inmediata (Servidores espejo entre Agencia y Matriz)
- ✓ Core Financiero Robusto y parametrizable hacia nuevos producto y líneas de negocio

OPORTUNIDADES

- ✓ Mercado Financiero con oportunidades de crecimiento
- ✓ POS Página Web Transaccional.
- ✓ Consulta de saldos vía celular. Utilización de software libre (gratuito)
- ✓ Apertura de nuevas agencias.
- ✓ Recordatorio de pago vía SMS y agradecimiento del mismo.

DEBILIDADES

- ✓ Funcionalidad del comité de sistemas.
- ✓ Deficiencias en el control de la infraestructura tecnológica de la entidad.
- ✓ Débil proceso de inducción y capacitación al personal del área de sistemas.
- ✓ Falta de página web Transaccional
- ✓ Ausencia de monitoreo a los servicios prestados por terceros
- ✓ Debilidad en los contratos o faltas de SLA. (Modelo de acuerdo de nivel de servicios)

AMENAZAS

- ✓ Desastres naturales
- ✓ Robo o sabotaje
- ✓ Incendio
- ✓ Ataques de virus

3.1.4. DEPENDENCIA DE ACTIVOS

Se realizó la identificación de los activos de la institución que dependen de otros para su funcionamiento, tomando en cuenta los procesos productivos como son: Captaciones y Colocaciones, así mismo con los procesos de soporte o apoyo de los procesos productivos como son talento humano tecnología de información, financiero, auditoria, cumplimiento y riesgos como se demuestra a continuación:

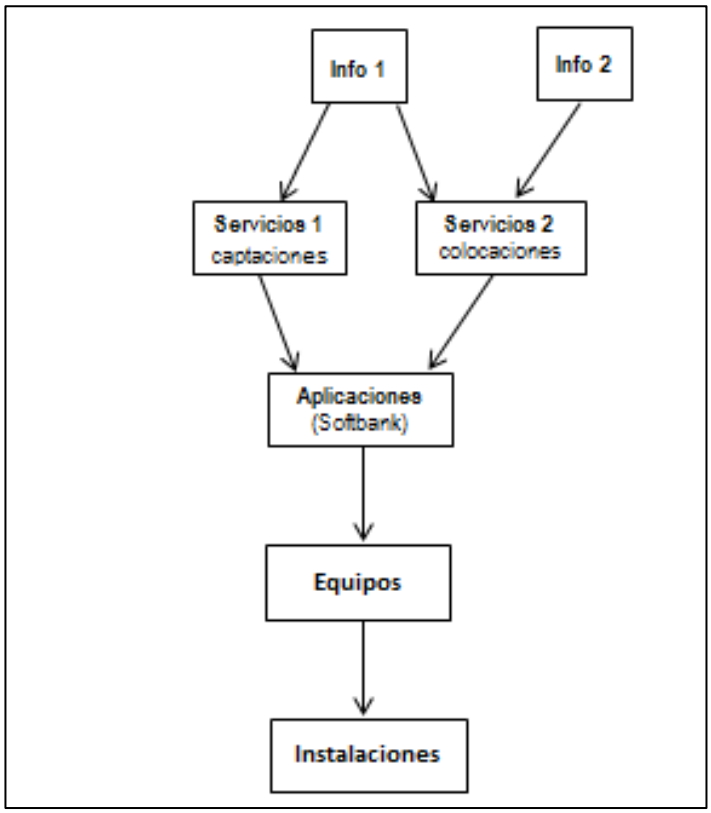


Figura 3.01. Dependencia de activos – Procesos Productivos
Fuente: las autoras

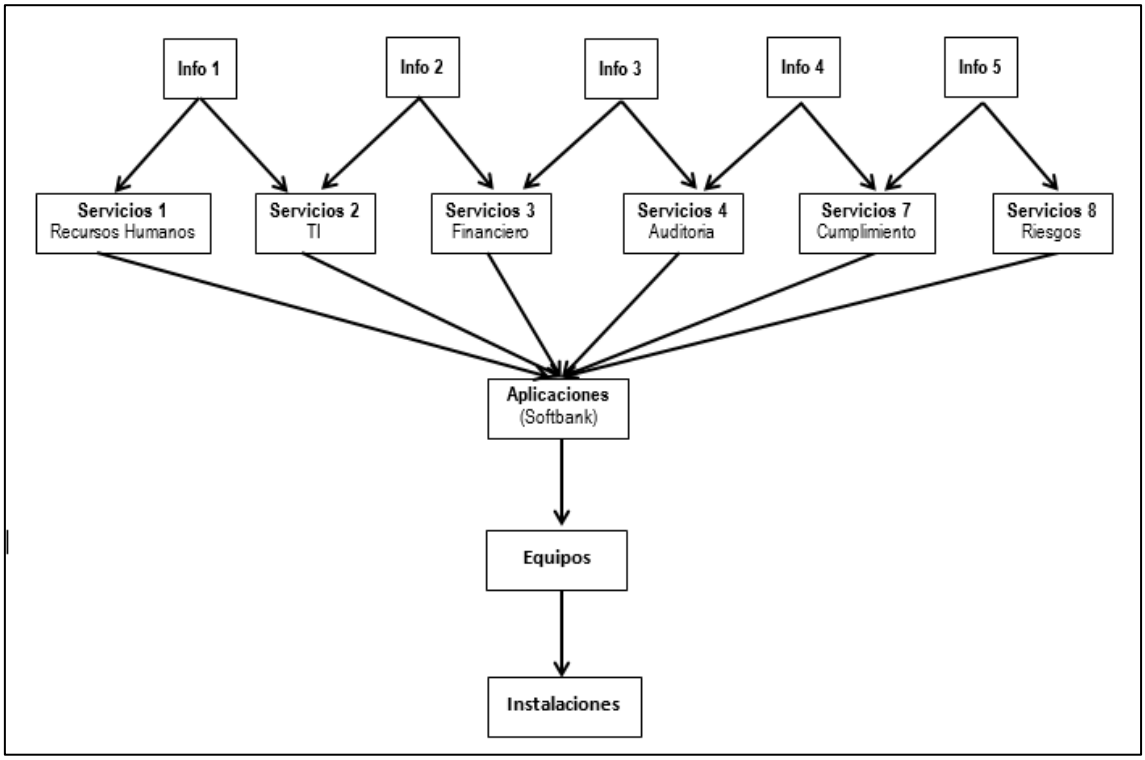


Figura 3.02. Dependencia de activos (Procesos de soporte y apoyo)
Fuente: Las Autoras

3.2. IDENTIFICACIÓN DE POTENCIALES AMENAZAS

Considerando que las amenazas son hechos que pueden ocurrir, causar daños y comprometer el buen funcionamiento de los activos de la institución, es necesario que sean identificadas a tiempo y evitar que ocurran y si ocurren que su impacto no cause mayor daño, por lo que se realizó una evaluación de las amenazas a las que están expuestos los activos.

Para hacer la identificación de las amenazas, se tomó en cuenta las más importantes de acuerdo al tipo de institución en la cual se aplicó y los activos que se verían afectados por dicha amenaza, las cuales son: desastres naturales, de origen industrial, errores y fallos no intencionados, ataques intencionados.

3.2.1. [N] DESASTRES NATURALES

Los desastres naturales son eventos que ocurren de forma inesperada, por lo cual es necesario tomar medidas para evitar pérdidas humanas y materiales, por esto fue necesario determinar las amenazas de este tipo que se pueden presentar dentro de la organización, encontrando las que se detallan a continuación:

Cuadro 3.010. Identificación de las amenazas de tipo natural

Origen	Amenazas	Tipos de Activos
Desastres Naturales	[n.1] Fuego	Equipos informáticos (hardware)
		Soporte de información
		Instalaciones
		Redes de comunicaciones
		Equipamiento auxiliar
	[n.2] Daños por agua	Equipos informáticos (hardware)
		Soporte de información
		Instalaciones
		Redes de comunicaciones
		Equipamiento auxiliar
	[n.*] Desastres naturales	Equipos informáticos (hardware)
		Soporte de información
		Instalaciones
		Redes de comunicaciones
		Equipamiento auxiliar

Fuente: Las autoras

3.2.2. [I] DESASTRES DE ORIGEN INDUSTRIAL

Este tipo de desastres son los que se generan dentro de la institución causando daños que pueden ser irreparables, los accidentes de este tipo que se podrían presentar son:

Cuadro 3.11 Identificación de las amenazas de tipo Industrial

Origen	Amenazas	Tipos de Activos
De Origen Industrial	[i.1] Fuego	Equipos informáticos (hardware)
		Soporte de información
		Instalaciones
		Redes de comunicaciones
		Equipamiento auxiliar
	[i.2] Daños por agua	Equipos informáticos (hardware)
		Soporte de información
		Instalaciones
		Redes de comunicaciones
		Equipamiento auxiliar
	[i.*] Desastres Industriales	Equipos informáticos (hardware)
		Soporte de información
		Instalaciones
		Redes de comunicaciones
		Equipamiento auxiliar
	[i.3] Contaminación Mecánica	Equipos informáticos (hardware)
		Soporte de información
		Redes de comunicaciones
		Equipamiento auxiliar
	[i.4] Contaminación Electromagnética	Equipos informáticos (hardware)
		Soporte de información
		Redes de comunicaciones
		Equipamiento auxiliar
	[i.5] Avería de origen Físico o Lógico	Equipos informáticos (hardware)
		Soporte de información
		Aplicaciones (software)
		Redes de comunicaciones
		Equipamiento auxiliar
	[i.6] Corte del Suministro Eléctrico	Equipos informáticos (hardware)
		Soporte de información (eléctricos)
		Redes de comunicaciones
		Equipamiento auxiliar
	[i.7] Condiciones Inadecuadas de Temperatura y/o Humedad	Equipos informáticos (hardware)
		soporte de información (eléctricos)
		Redes de comunicaciones
		Equipamiento auxiliar

[i.8] Fallo de Servicios de Comunicaciones	Redes de comunicaciones
[i.9] Interrupción de otros Servicios y Suministros Esenciales	Equipamiento auxiliar
[i.10] Degradación de los Soportes de Almacenamiento de la Información	Soporte de información (eléctricos)

Fuente: Las autoras

3.2.3. [E] ERRORES Y FALLOS NO INTENCIONADOS

Este tipo de errores son aquellos generados por las personas sin ninguna malicia, pero que pueden afectar en el buen desempeño de las actividades de la empresa, se los cita a continuación:

Cuadro 3.12. Identificación de las amenazas de tipo humanas, no intencionadas

Origen	Amenazas	Tipos de Activos
Errores y Fallos no Intencionados	**[e.1] Errores de los Usuarios**	Dato/Información
		Servicios
		Soportes de información
	[E.2] Errores del Administrador	Dato/Información
		Servicios
		Soportes de información
		Soporte de Información (eléctricos)
		Redes de comunicaciones
	[e.4] Errores de Configuración	Dato/Información
		Redes de Comunicaciones
		Servicios
		Equipos Informáticos
		Aplicaciones (software)
	[e.7] Deficiencias en la Organización	Personal
		Servicios
	[e.8] Difusión de Software Dañino	Aplicaciones (software)
	[e.9] Errores de [re-]encaminamiento	Servicios
		Aplicaciones (software)
		Redes de comunicaciones
	[e.10] Errores de secuencia	Servicios
		Aplicaciones (software)
		Redes de comunicaciones
	[E.14] Escapes de información	Dato/Información
		redes de comunicaciones
		Aplicaciones (software)
	[e.15] Alteración Accidental de la Información	Dato/Información
	[e.18] Destrucción de Información	Dato/Información
	[e.19] Fugas de Información	Dato/Información
	[e.20] Vulnerabilidades de los Programas (Software)	Aplicaciones (software)

	[e.23] Errores de Mantenimiento / Actualización de Equipos (Hardware)	Equipos Informáticos (hardware)
	[e.24] Caída del Sistema por Agotamiento de Recursos	Servicios
		Equipos informáticos (hardware)
		Redes de comunicaciones
	[e.25] Pérdida de Equipos	Equipos informáticos (hardware)
		Soportes de información
		Equipamiento auxiliar
	[e.28] Indisponibilidad del Personal	Personal

Fuente: Las autoras

3.2.4. [A] ATAQUES INTENCIONADOS

Se dan por personas que tienen la intención de causar daños y afectar el buen desempeño de la institución, este tipo de ataques son planificados con el fin de causar o de tener un beneficio, a continuación se citan los posibles ataques que podría sufrir la institución:

Cuadro 3.13. Identificación de las amenazas humanas de tipo intencionadas.

Origen	Amenazas	Tipos de Activos
Ataques Intencionados	**[a.4] Manipulación de la Configuración**	Redes de comunicaciones
		Equipos informáticos (hardware)
		Aplicaciones (software)
		Servicios
	[a.5] Suplantación de la Identidad del Usuario	Dato/Información
		servicios
		Aplicaciones (software)
	[a.6] Abuso de Privilegios de Acceso	Dato/Información
		Servicios
		Equipos informáticos (hardware)
	[A.7] Uso no Previsto	Dato/Información
		Servicios
		Equipos informáticos (hardware)
		Aplicaciones (software)
		Soportes de información
		Redes de comunicaciones
		Equipamiento auxiliar
	[a.8] Difusión de Software Dañino	Aplicaciones (software)
	[a.11] Acceso no Autorizado	Dato/Información
		servicios
		Equipos informáticos (hardware)
		Aplicaciones (software)
		Soportes de información
		Redes de comunicaciones
		Equipamiento auxiliar
		Instalaciones
	[a.12] Análisis de Tráfico	Redes de comunicaciones
	[a.13] Repudio	Servicios
	[a.14] Interceptación de Información (escucha)	Redes de comunicaciones
	[a.15] Modificación Deliberada de la Información	Dato/Información
	[a.18] Destrucción de Información	Dato/Información
	[a.19] Revelación de Información	Dato/Información

	[a.19] Revelación de Información	Dato/Información
	[a.22] Manipulación de Programas	Aplicaciones (software)
	[a.23] manipulación de los Equipos	Equipos informáticos (hardware)
		Soportes de información
		Equipamiento auxiliar
	[a.25] Robo	Equipos informáticos (hardware)
		Soportes de información
		Equipamiento auxiliar
	[a.26] Ataque Destructivo	Equipos informáticos (hardware)
		Soportes de información
		Equipamiento auxiliar
		Redes de comunicaciones
		Instalaciones
	[a.28] Indisponibilidad del Personal	Personal
	[a.29] Extorsión	Personal
	[a.30] Ingeniería Social (Picaresca)	Personal

Fuente: Las autoras

3.2.5. DETERMINACIÓN DE RIESGOS

Luego de haber realizada la identificación de las amenazas que se pueden dar dentro de la institución, se realizaron las matrices para determinar los riesgos a los que se encuentra expuesta la institución, se realizó una matriz por cada amenaza, ya que es el proceso que sigue la metodología Magerit de individualizar cada una con su riesgo, impacto y razón por las cuales pueden presentarse cada una de ellas, ya que aunque las amenazas se repitan las causas por las cuales se dan son totalmente aisladas una de otra, los cuadros quedaron esquematizados de la siguiente manera:

Cuadro 3.14. Desastres Naturales – Fuego

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [L] instalaciones • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** **1.** [D] Disponibilidad
Descripción: Incendios: posibilidad de que el fuego acabe con recursos del sistema.	

ESTIMACIÓN DEL IMPACTO						**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**				**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**				**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	**MA**		**IMPACTO**	**MA**	**A**	MA	MA	MA
	A	B	M	A			**A**	M	A	MA	MA
	M	MB	B	M			**M**	B	M	A	MA
	B	MB	MB	B			**B**	MB	B	M	A
	MB	MB	MB	MB			**MB**	MB	MB	B	M

Causa: Los incendios, son siniestros que puede causar la destrucción parcial o total de los bienes afectados, según datos del cuerpo de bomberos del cantón Bolívar, éstos se registran con poca frecuencia en la ciudad, por ello su impacto se considera muy alto y su riesgo alto, aunque este tipo de daños se dan con poca frecuencia.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.15. Desastres Naturales – Daños por agua

[N.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [L] instalaciones • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** **2.** [D] Disponibilidad
Descripción: Inundaciones: posibilidad de que el agua acabe con recursos del sistema.	

ESTIMACIÓN DEL IMPACTO						**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**				**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**				**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	MA		**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	M	A			**A**	M	A	MA	MA
	M	MB	**B**	M			**M**	B	M	A	MA
	B	MB	MB	B			**B**	MB	**B**	M	A
	MB	MB	MB	MB			**MB**	MB	MB	B	M

Causa: Por la ubicación de la institución y considerando que Bolívar no es una zona fácilmente inundable además que los equipos más relevantes como servidores y otros están ubicados en la segunda planta de la institución este tipo de amenaza puede pasar desapercibida en la institución, por lo que su impacto y su riesgo son bajos y se dan con frecuencia normal.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.16. Desastres Naturales – Desastres naturales

[N.*] Desastres naturales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [L] instalaciones • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** **3.** [D] Disponibilidad
Descripción: Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, avalancha, se excluyen desastres específicos tales como incendios e inundaciones, se excluye al personal por cuanto se ha previsto una amenaza específica para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	**M**	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	**M**	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: Los desastres naturales ocurren sin aviso, pero es necesario considerar que en la cuidad no se registran daños ocasionados por este motivo, por tanto se estima con frecuencia normal, un riesgo y un impacto medio.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.17. Origen industrial – Fuego

[I.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [L] instalaciones • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** **4.** [D] Disponibilidad
Descripción: Incendio: posibilidad de que el fuego acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	**MA**
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	**A**	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: Los incendios, pueden causar la destrucción parcial o total de los bienes afectados, según datos del cuerpo de bomberos del cantón Bolívar, se registran con poca frecuencia en la ciudad, su impacto se considera muy alto y su riesgo alto.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.18. Origen industrial – Daños por agua

[I.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [L] instalaciones • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** **5.** [D] Disponibilidad
Descripción: Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	**M**
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	**B**	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: Este tipo de daños se da en lugares donde las instalaciones sean obsoletas, lo que no es el caso de la Cooperativa Calceta, ya que su infraestructura es nueva y hasta la actualidad no ha presentado este tipo de daños.				
MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.19. Origen industrial – Desastres industriales

[I.*] Desastres industriales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [L] instalaciones • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** **6.** [D] Disponibilidad
Descripción: Otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico. Se excluyen amenazas específicas como incendio e inundación. Se excluye al personal por cuanto se ha previsto una amenaza específica, para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	M	A
	M	MB	**B**	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	**MB**	B	M	A
	MB	MB	MB	B	M

Causa: La institución se encuentra ubicada en la zona céntrica de la cuidad y el flujo del tráfico es pesado, por lo que se considera un riesgo muy bajo y un impacto bajo.				
MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.20. Origen industrial – Contaminación mecánica

[I.3] Contaminación mecánica	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** **7.** [D] Disponibilidad
Descripción: Vibraciones, polvo, suciedad,... **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	M	A
	M	MB	**B**	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	**A**
	MB	MB	MB	B	M

Causa: La cooperativa Calceta se encuentra ubicada en el centro de la ciudad donde el tráfico es constante, por lo que siempre habrá presencia de polvo, por lo que se considera un impacto bajo y un riesgo alto.				
MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.21. Origen industrial – Contaminación electromagnética

[I.4] Contaminación electromagnética	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** **8.** [D] Disponibilidad
Descripción: Interferencias de radio, campos magnéticos, luz ultravioleta,... **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	**MB**	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	**MB**	MB	B	M

Causa: En la institución se presentó una vez este tipo de sucesos, debido a la interferencia que presentaban los transformadores cercanos aun así no se presentaron daños por lo cual el impacto y el riesgo es muy bajo.				
MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.22. Origen industrial – Avería de origen físico o lógico

[I.5] Avería de origen físico o lógico	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [SW] aplicaciones (software) • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** **9.** [D] Disponibilidad
Descripción: Fallos en los equipos y/o fallos en los programas, puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	**A**	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	**A**	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: La cooperativa Calceta cuenta con 9 servidores, de sufrir daños físicos o lógicos afectaría en el desempeño de los servicios que brinda la institución y a sus sucursales, por lo que se estima un alto riesgo e impacto.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.23. Origen industrial – Corte de suministro eléctrico

[I.6] Corte del suministro eléctrico	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** **10.** [D] Disponibilidad
Descripción: Cese de la alimentación de potencia. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	MA	A	MA
	A	B	**M**	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	**A**	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: En el cantón Bolívar se registran fallos eléctricos constantemente, por lo cual representa un alto riesgo y un impacto medio para la institución por el daño que podrían sufrir los equipos, por lo cual cuenta con una planta generadora de energía propia que le garantice la continuidad del fluido eléctrico y por ende la atención al cliente.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.24. Origen industrial – Condiciones inadecuadas de temperatura y/o humedad

[I.7] Condiciones inadecuadas de temperatura y/o humedad	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** **11.** [D] Disponibilidad
Descripción: Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	M	A
	M	MB	**B**	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	**MB**	B	M	A
	MB	MB	MB	B	M

Causa: La cooperativa calceta cuenta con sensores que le permiten medir la temperatura dentro de ella, por lo que hasta la actualidad no han sufrido daños de este tipo, por esto que se estima un impacto bajo y un riesgo muy bajo.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.25. Origen industrial – Fallo de servicios de comunicaciones

[I.8] Fallo de servicios de comunicaciones	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** **12.** [D] Disponibilidad
Descripción: Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	**A**	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	**A**	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: La cooperativa Calceta es una institución financiera, por lo cual necesita mantener comunicación en línea para enviar y recibir datos de sus sucursales, ya que esta institución es matriz y cuenta con 3 agencias que dependen de ella para poder brindar servicio a la comunidad, por lo que se considera que de materializarse representaría un riesgo y un impacto alto.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.26. Origen industrial – Interrupción de otros servicios y suministros esenciales

[I.9] Interrupción de otros servicios y suministros esenciales	
Tipos de activos: • [AUX] equipamiento auxiliar	**Dimensiones:** **13.** [D] Disponibilidad
Descripción: Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

ESTIMACIÓN DEL IMPACTO					**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**			**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**			**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	MA	**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	**M**	A		**A**	M	A	MA	MA
	M	MB	B	M		**M**	B	**M**	A	MA
	B	MB	MB	B		**B**	MB	B	M	A
	MB	MB	MB	MB		**MB**	MB	MB	B	M

Causa: En la institución no se han presentado falta de suministros, el departamento de Talento humano es el encargado de proveerlos a cada departamento, aun así en caso de darse afectaría en el proceso de la prestación de servicios causando tardanza en los procesos, por lo que se considera un riesgo e impacto medio.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.27. Origen industrial – Degradación de los soportes de almacenamientos de la información

[I.10] Degradación de los soportes de almacenamiento de la información	
Tipos de activos: • [MEDIA] soporte de información	**Dimensiones:** **14.** [D] Disponibilidad
Descripción: Como consecuencia del paso del tiempo **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

ESTIMACIÓN DEL IMPACTO					**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**			**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**			**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	**MA**	**IMPACTO**	**MA**	**A**	MA	MA	MA
	A	B	M	A		**A**	M	A	MA	MA
	M	MB	B	M		**M**	B	M	A	MA
	B	MB	MB	B		**B**	MB	B	M	A
	MB	MB	MB	MB		**MB**	MB	MB	B	M

Causa: La cooperativa Calceta cuenta con un servidor de respaldo de información, además se hacen respaldos semanales en discos, pero en caso de que la contingencia falle tendría un impacto muy alto, pero este tipo de daños no ocurren con frecuencia.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.28. Errores y fallos no intencionados – Errores de los usuarios

[E.1] Errores de los usuarios	
Tipos de activos: • [MEDIA] soporte de información • [S] servicios • [D] datos/información	**Dimensiones:** 1. [C] Confidencialidad 2. [I] Integridad 3. [D] Disponibilidad
Descripción: Equivocaciones de las personas cuando usan los servicios, datos, etc.	

ESTIMACIÓN DEL IMPACTO					**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**			**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**			**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	**A**	MA	**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	M	A		**A**	M	**A**	MA	MA
	M	MB	B	M		**M**	B	M	A	MA
	B	MB	MB	B		**B**	MB	B	M	A
	MB	MB	MB	MB		**MB**	MB	MB	B	M

Causa: Es importante recalcar que la cooperativa Calceta cuenta con personal capacitado para cumplir las funciones encomendadas según el cargo que desempeñen dentro de la misma, por lo que se estima que el impacto y el riesgo son bajos.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.29. Errores y fallos no intencionados – Errores del administrador

[E.2] Errores del administrador	
Tipos de activos: • [MEDIA] soporte de información • [S] servicios • [D] datos/información • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] Confidencialidad 2. [I] Integridad 3. [D] Disponibilidad 4. [A_S] Autenticidad del servicio **5.** [A_D] Autenticidad de los datos
Descripción: Equivocaciones de personas con responsabilidades de instalación y operación	

ESTIMACIÓN DEL IMPACTO					**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**			**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**			**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	MA	**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	**M**	A		**A**	M	A	MA	MA
	M	MB	B	M		**M**	B	**M**	A	MA
	B	MB	MB	B		**B**	MB	B	M	A
	MB	MB	MB	MB		**MB**	MB	MB	B	M

Causa: Tecnologías cuenta con personal capacitado, pero considerando son 3 los usuarios que ingresan información en las bases de datos, representan riesgo potencial, el riesgo e impacto se considera medio.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.30 Errores y fallos no intencionados – Errores de configuración

[E.4] Errores de configuración	
Tipos de activos: • [D] datos/información • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] Confidencialidad 2. [D] Disponibilidad 3. [I] Integridad 4. [A_S] Autenticidad del servicio 5. [A_D] Autenticidad de los datos
Descripción: Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	**M**	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	**M**	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: Este daño se considera con riesgo e impacto es medio ya que la información puede llegar a manos equivocadas y ser cambiada o utilizada para fines delictivos.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.31. Errores y fallos no intencionados – Deficiencias en la organización

[E.7] Deficiencias en la organización	
Tipos de activos: • [P] personal	**Dimensiones:** 1. [D] Disponibilidad
Descripción: Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	M	A
	M	**MB**	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	**MB**	B	M

Causa: Es importante para la institución dejar claros los roles que cumple cada empleado dentro de la institución, ya que así se tiene clara la ruta y todos harán un buen trabajo para el buen desempeño de los servicios que brinda la institución, por esto se considera que tanto el riesgo como el impacto son muy bajos.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.32. Errores y fallos no intencionados – Difusión de software dañino

[E.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [C] Confidencialidad 2. [D] Disponibilidad 3. [I] Integridad
Descripción: Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	**A**	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	**A**	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: La cooperativa Calceta cuenta con un servidor antivirus que le permite detectar este tipo de riesgos, pero aun así, esta amenaza está presente dentro de toda institución y de materializarse puede causar daños en el sistema que ocasiona la demora en la prestación de servicios por lo que se considera un alto impacto y un riesgo Alto.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.33. Errores y fallos no intencionados – Errores de [re-]encaminamiento

[E.9] Errores de [re-]encaminamiento	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] Confidencialidad 2. [I] Integridad
Descripción: Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	**M**	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	**B**	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: En la cooperativa Calceta se hace uso de las redes de datos para envío y recepción constante de información de los clientes y el hecho de que sea enviada a personas que no les interesa puede provocar daños a la institución o a los clientes, por lo que se considera un impacto medio y un riesgo bajo considerando que nunca ha ocurrido.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.34. Errores y fallos no intencionados – Errores de secuencia

[E.10] Errores de secuencia	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [I] Integridad
Descripción: Alteración accidental del orden de los mensajes transmitidos.	

ESTIMACIÓN DEL IMPACTO					**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**			**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**			**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	MA	**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	M	A		**A**	M	A	MA	MA
	M	**MB**	B	M		**M**	B	M	A	MA
	B	MB	MB	B		**B**	MB	B	M	A
	MB	MB	MB	MB		**MB**	**MB**	MB	B	M

Causa: Para la cooperativa Calceta la Información es su principal activo, por lo cual los datos deben de mantenerse íntegros, es importante recalcar que dentro de la institución no se han presentado este tipo de amenazas, por lo cual la estimación del riesgo y del impacto son muy bajas.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.35. Errores y fallos no intencionados – Escapes de información

[E.14] Escapes de información	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] Confidencialidad
Descripción: La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	

ESTIMACIÓN DEL IMPACTO					**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**			**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**			**PF**	**FN**	**F**	**MF**
VALOR	**MA**	**M**	A	MA	**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	M	A		**A**	M	A	MA	MA
	M	MB	B	M		**M**	B	**M**	A	MA
	B	MB	MB	B		**B**	MB	B	M	A
	MB	MB	MB	MB		**MB**	MB	MB	B	M

Causa: Dentro de la institución no se ha presentado esta amenaza, ya que la información se maneja muy sigilosamente y la institución tiene políticas internas que sancionan este tipo de conductas en caso de producirse, por lo que el impacto y el riesgo se estiman medio.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.36. Errores y fallos no intencionados – Alteración accidental de la información

[E.15] Alteración accidental de la información	
Tipos de activos: • [D] datos/información	**Dimensiones:** 1. [I] Integridad
Descripción: Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	**M**	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	**B**	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: El riesgo de la alteración accidental de la información se considera medio por la importancia que tiene la información para la institución y el riesgo se considera bajo ya que el personal tiene la obligación de cuidar la información que tiene a su cargo.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.37 Errores y fallos no intencionados – Destrucción de información

[E.18] Destrucción de información	
Tipos de activos: • [D] datos/información	**Dimensiones:** 1. [D] Disponibilidad
Descripción: Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	M	**A**
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	**M**	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: Las instituciones tiene la obligación de garantizar la integridad de los datos proporcionados a sus clientes, es necesario acotar que en la cooperativa Calceta no se han registrado este tipo de amenazas, por lo que se considera un riesgo medio, pero en caso de materializarse su impacto sería alto.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.38. Errores y fallos no intencionados – Fugas de información

[E.19] Fugas de información	
Tipos de activos: • [D] datos/información	**Dimensiones:** 1. [C] Confidencialidad
Descripción: Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	

ESTIMACIÓN DEL IMPACTO						**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**				**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**				**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	**A**	MA		**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	M	A			**A**	**M**	A	MA	MA
	M	MB	B	M			**M**	B	M	A	MA
	B	MB	MB	B			**B**	MB	B	M	A
	MB	MB	MB	MB			**MB**	MB	MB	B	M

Causa: En la cooperativa Calceta no se han registrado este tipo de incidentes, pero en el intercambio de la información que se realiza a diario dentro de ella hace que este riesgo este presente siempre, por lo que se considera alto, y con un impacto alto.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.39. Errores y fallos no intencionados – Vulnerabilidades de los programas (software)

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] Integridad 2. [C] Confidencialidad 3. [D] Disponibilidad
Descripción: Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	

ESTIMACIÓN DEL IMPACTO						**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**				**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**				**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	**A**	MA		**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	M	A			**A**	M	**A**	MA	MA
	M	MB	B	M			**M**	B	M	A	MA
	B	MB	MB	B			**B**	MB	B	M	A
	MB	MB	MB	MB			**MB**	MB	MB	B	M

Causa: El uso de software en la instituciones las hacen vulnerables ante este tipo de riesgos aunque el software utilizado en la cooperativa Calceta no ha sufrido daños con consecuencias mayores hasta la actualidad pero de darse podría ser recuperado rápidamente ya que es un software desarrollado por el departamento de tecnología de la institución el cual se encuentra preparado para restaurarlo rápidamente, aun así en caso de materializarse esta amenaza se considera que su impacto sería alto.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.40. Errores y fallos no intencionados – Errores de mantenimiento / actualización de programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] Integridad 2. [D] Disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	**M**	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	B

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	**M**	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: El departamento de tecnología de la cooperativa Calceta está haciendo mantenimiento constante a su software por lo que se considera un riesgo e impacto medio.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.41. Errores y fallos no intencionados – Errores de mantenimiento / actualización de equipos (hardware)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información	**Dimensiones:** 1. [D] Disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	**M**	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	**M**	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: Por el flujo de información que se maneja en la cooperativa Calceta los equipos pueden sufrir daños o dejar de funcionar, por lo que el personal de tecnologías realiza monitoreos constantemente para evitar daños en ellos, por lo que se considera un riesgo e impacto medio.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.42. Errores y fallos no intencionados – Caída del sistema por agotamiento de recursos

[E.24] Caída del sistema por agotamiento de recursos	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicación	**Dimensiones:** 1. [D] Disponibilidad
Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	

ESTIMACIÓN DEL IMPACTO						**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**				**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**				**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	MA		**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	M	A			**A**	M	A	MA	MA
	M	MB	**B**	M			**M**	B	M	A	MA
	B	MB	MB	B			**B**	MB	**B**	M	A
	MB	MB	MB	MB			**MB**	MB	MB	B	M

Causa: En la cooperativa Calceta el riesgo e impacto por esta amenaza es bajo, esto se debe a que los equipos informáticos son frecuentemente monitoreados lo que garantiza su buen funcionamiento.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.43. Errores y fallos no intencionados – Indisponibilidad del personal

[E.28] Indisponibilidad del personal	
Tipos de activos: • [P] personal	**Dimensiones:** 1. [D] Disponibilidad
Descripción: Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica,...	

ESTIMACIÓN DEL IMPACTO						**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**				**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**				**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	MA		**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	M	A			**A**	M	A	MA	MA
	M	**MB**	B	M			**M**	B	M	A	MA
	B	MB	MB	B			**B**	MB	B	M	A
	MB	MB	MB	MB			**MB**	MB	MB	**B**	M

Causa: La falta de personal en una institución financiera representa problemas dentro de ella y aunque sea frecuente esto representa un riesgo bajo y un impacto muy bajo ya que si falta uno o dos empleados sus funciones pueden seguir desempeñadas por sus compañeros de trabajo.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.44. Ataques intencionados – Manipulación de la configuración

[A.4] Manipulación de la configuración	
Tipos de activos: • [COM] redes de comunicaciones • [HW] equipos informáticos (hardware) • [SW] aplicaciones (software) • [S] servicios • [D] datos/información	**Dimensiones:** 1. [C] Confidencialidad 2. [D] Disponibilidad 3. [I] Integridad 4. [A_S] Autenticidad del servicio 5. [A_D] Autenticidad de los datos
Descripción: Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	**A**	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	**M**	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: Aunque en la institución nunca se ha dado este tipo de amenaza, se considera un riesgo medio y un impacto alto, debido a que en caso de materializarse, esta causará problemas dado que no se podría llegar a saber que tanto fue manipulado el sistema y a que reto se enfrenta el personal de tecnología causando daños dentro y fuera de la institución.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.45. Ataques intencionados – Suplantación de la identidad del usuario

[A.5] Suplantación de la identidad del usuario	
Tipos de activos: • [D] datos/información • [S] servicios • [SW] aplicaciones (software)	**Dimensiones:** 1. [C] Confidencialidad 2. [D] Disponibilidad 3. [A_S] Autenticidad del servicio 4. [A_D] Autenticidad de los datos
Descripción: Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	**A**	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	**A**	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: Este es un peligro latente, ya que los datos que se manejan las instituciones sobre todo financieras siempre son apetecidos por personas que se dedican a actos delictivos, por esto se considera que en caso de materializarse la amenaza representaría un riesgo y un impacto alto.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.46. Ataques intencionados – Abuso de privilegios de acceso

[A.6] Abuso de privilegios de acceso	
Tipos de activos: • [D] datos/información • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] Confidencialidad 2. [D] Disponibilidad 3. [A_S] Autenticidad del servicio 4. [A_D] Autenticidad de los datos
Descripción: Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	**M**	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	**M**	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: A cada trabajador se le crea un perfil, y de acuerdo a su puesto de trabajo se le dan los privilegios de usuario, lo cual limita su acceso a la información y les permite tener un mejor y mayor control sobre ellos, por se estima un riesgo e impacto medio ante esta amenaza.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.47. Ataques intencionados – Uso no previsto

[A.7] Uso no previsto	
Tipos de activos: • [D] datos/información • [S] servicios • [HW] equipos informáticos (hardware) • [SW] aplicaciones (software) • [MEDIA] soporte de información • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] Disponibilidad
Descripción: Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: consultas en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	**B**	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	**B**	M	A
	MB	MB	MB	B	M

Causa: El uso de recursos de la institución para fines personales es común, pero cuando es frecuente e interfiere en la realización de las labores del trabajador representa problemas, este se considera un riesgo e impacto bajo.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.48. Ataques intencionados – Difusión de software dañino

[A.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [C] Confidencialidad 2. [D] Disponibilidad 3. [I] Integridad 4. [A_S] Autenticidad del servicio 5. [A_D] Autenticidad de los datos
Descripción: Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	**A**	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	**A**	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: En la cooperativa Calceta no se han registrado este tipo de incidentes, pero en caso de darse podría afectar en el buen funcionamiento tanto del hardware como del software por lo que se considera que tanto el riesgo como el impacto son altos.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.49. Ataques intencionados – Acceso no autorizado

[A.11] Acceso no autorizado	
Tipos de activos: • [D] datos/información • [S] servicios • [HW] equipos informáticos (hardware) • [SW] aplicaciones (software) • [MEDIA] soporte de información • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [C] Confidencialidad 2. [I] Integridad 3. [A_S] Autenticidad del servicio
Descripción: El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	**A**	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	**A**	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: Si una persona no autorizada accede al sistema de forma deliberada puede causar grandes pérdidas no solo económicas sino también de la información, por lo que se considera un riesgo e impacto alto

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.50. Ataques intencionados – Análisis de tráfico

[A.12] Análisis de tráfico	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] Confidencialidad 2. [I] Integridad
Descripción: El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina "monitorización de tráfico".	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	**B**	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	**MB**	B	M	A
	MB	MB	MB	B	M

Causa: Este tipo de amenaza no se ha dado en la Cooperativa Calceta, por lo cual su riesgo es muy bajo y su impacto bajo.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.51. Ataques intencionados – Repudio

[A.13] Repudio	
Tipos de activos: • [S] servicios	**Dimensiones:** 1. [T-S] Trazabilidad de servicios
Descripción: Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	**B**	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	**B**	M	A
	MB	MB	MB	B	M

Causa: En la cooperativa Calceta no se han registrado este tipo de amenazas, por esto se considera que en caso de materializarse es de riesgo e impacto bajo.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.52. Ataques intencionados – Interceptación de información

[A.14] Interceptación de información	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] Confidencialidad
Descripción: El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	**B**	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	**B**	M	A
	MB	MB	MB	B	M

Causa: La información de la institución es confidencial por lo cual si las personas no autorizadas tienen acceso a ella pueden surgir inconvenientes, en la institución hasta la actualidad no se ha presentado esta amenaza por lo cual se considera que tanto el riesgo como el impacto son bajos.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.53. Ataques intencionados – Modificación deliberada de la información

[A.15] Modificación deliberada de la información	
Tipos de activos: • [D] datos/información	**Dimensiones:** 1. [I] Integridad
Descripción: Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	A	MA
	A	B	**M**	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	**B**	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: La alteración de la información que maneja la cooperativa Calceta representaría grandes daños a la misma, pero considerando que no se ha registrado daños de este tipo se considera un riesgo medio y en caso de darse tendría un impacto bajo.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.54. Ataques intencionados – Destrucción de la información

[A.18] Destrucción de información	
Tipos de activos: • [D] datos/información	**Dimensiones:** 1. [D] Disponibilidad
Descripción: Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	

ESTIMACIÓN DEL IMPACTO						**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**				**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**				**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	**MA**		**IMPACTO**	**MA**	**A**	MA	MA	MA
	A	B	M	A			**A**	M	A	MA	MA
	M	MB	B	M			**M**	B	M	A	MA
	B	MB	MB	B			**B**	MB	B	M	A
	MB	MB	MB	MB			**MB**	MB	MB	B	M

Causa: Por la importancia que tiene información para la cooperativa Calceta su eliminación representaría pérdidas económicas muy grandes, cabe recalcar que en la institución no se han presentado este tipo de amenazas, pero si ocurriera se considera un riesgo alto, pero en caso de materializarse la amenaza su impacto sería muy alto.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.55. Ataques intencionados – Revelación de la información

[A.19] Revelación de información	
Tipos de activos: • [D] datos/información	**Dimensiones:** 1. [C] Confidencialidad
Descripción: Revelación de información.	

ESTIMACIÓN DEL IMPACTO						**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**				**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**				**PF**	**FN**	**F**	**MF**
VALOR	**MA**	**M**	A	MA		**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	M	A			**A**	M	A	MA	MA
	M	MB	B	M			**M**	B	**M**	A	MA
	B	MB	MB	B			**B**	MB	B	M	A
	MB	MB	MB	MB			**MB**	MB	MB	B	M

Causa: La divulgación de la información es muy común dentro de las instituciones, pero en la cooperativa Calceta cada trabajador cuenta con un perfil distinto que le da acceso solo a la información necesaria para realizar su trabajo y en caso de divulgación debe someterse a lo que dispone la ley, como hasta la actualidad no se presentan daños de este tipo pero se considera un riesgo e impacto medio.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.56. Ataques intencionados – Manipulación de los programas

[A.22] Manipulación de programas	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [C] Confidencialidad 2. [I] Integridad 3. [A_S] Autenticidad del servicio 4. [A_D]Autenticidad de los datos 5. [T_D] Trazabilidad de los datos
Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	**M**	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	**M**	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: La mala manipulación de los programas o del software de la institución puede representar la interrupción del servicio, pero considerando que este tipo de ataques no se ha dado dentro de la institución se considera un riesgo y un impacto medio.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.57. Ataques intencionados – Robo

[A.25] Robo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [C] Confidencialidad 2. [D] Disponibilidad
Descripción: La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	

ESTIMACIÓN DEL IMPACTO				
IMPACTO		**DEGRADACIÓN**		
		1%	**10%**	**100%**
VALOR	**MA**	M	**A**	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO					
RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	**A**	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: Esta amenaza está presente en todo lugar, en la cooperativa Calceta nunca se ha dado, es difícil que personal no autorizado tenga acceso privilegiado, por lo que se considera que el riesgo es bajo e impacto alto.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.58. Ataques intencionados – Ataque destructivo

[A.26] Ataque destructivo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [AUX] equipamiento auxiliar • [COM] redes de comunicaciones • [L] instalaciones	**Dimensiones:** 1. [C] Confidencialidad 2. [D] Disponibilidad
Descripción: Vandalismo, terrorismo, acción militar. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.	

ESTIMACIÓN DEL IMPACTO					**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**			**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**			**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	MA	**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	M	A		**A**	M	A	MA	MA
	M	MB	B	**M**		**M**	**B**	M	A	MA
	B	MB	MB	B		**B**	MB	B	M	A
	MB	MB	MB	MB		**MB**	MB	MB	B	M

Causa: El riesgo ante ataques destructivos es bajo, considerando que en la zona se registran con poca frecuencia este tipo de ataques, pero en caso de materializarse tendrían un impacto muy alto.				
MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.59. Ataques intencionados – Indisponibilidad del personal

[E.28] Indisponibilidad del personal	
Tipos de activos: • [P] personal	**Dimensiones:** 1. [D] Disponibilidad
Descripción: Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos.	

ESTIMACIÓN DEL IMPACTO					**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**			**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**			**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	MA	**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	**M**	A		**A**	M	A	MA	MA
	M	MB	B	M		**M**	**B**	M	A	MA
	B	MB	MB	B		**B**	MB	B	M	A
	MB	MB	MB	MB		**MB**	MB	MB	B	M

Causa: Esta amenaza tiene un impacto medio y con poca frecuencia, ya que en caso de que ocurriera la institución no prestaría los servicios a sus clientes el cual es perjudicial para la organización.				
MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.60. Ataques intencionados – Extorsión

[A.29] Extorsión	
Tipos de activos: • [P] personal	**Dimensiones:** 1. [C] Confidencialidad 2. [D] Disponibilidad 3. [I] Integridad
Descripción: Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	

ESTIMACIÓN DEL IMPACTO					**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**			**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**			**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	MA	**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	**M**	A		**A**	M	A	MA	MA
	M	MB	B	M		**M**	B	**M**	A	MA
	B	MB	MB	B		**B**	MB	B	M	A
	MB	MB	MB	MB		**MB**	MB	MB	B	M

Causa: Toda institución puede ser víctima de esta amenaza, pero la cooperativa calceta no ha presentado inconvenientes, ya que en el cantón Bolívar estos hechos ocurren poco frecuente, motivo por el cual el impacto es medio con un riesgo bajo.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

Cuadro 3.61. Ataques intencionados – Ingeniería social

[A.30] Ingeniería social	
Tipos de activos: • [P] personal	**Dimensiones:** 1. [C]Confidencialidad 2. [I] Integridad 3. [A_S] Autenticidad del servicio 4. [A_D] Autenticidad de los datos 5. [T_S] Trazabilidad del servicio 6. [T_D] Trazabilidad de los datos
Descripción: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	

ESTIMACIÓN DEL IMPACTO					**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACIÓN**			**RIESGO**		**FRECUENCIA**			
		1%	**10%**	**100%**			**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	MA	**IMPACTO**	**MA**	A	MA	MA	MA
	A	B	**M**	A		**A**	M	A	MA	MA
	M	MB	B	M		**M**	B	**M**	A	MA
	B	MB	MB	B		**B**	MB	B	M	A
	MB	MB	MB	MB		**MB**	MB	MB	B	M

Causa: La cooperativa calceta es una institución financiera donde los socios u otras personas tienen acceso a ellos, donde las mismas pueden hacer uso de la confianza en cualquier departamento para extraer información relevante que les interese, pero el personal de la institución está capacitado para no dar ningún tipo de información, el cual se estima que el impacto y el riesgo es medio

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Fuente: Las autoras

3.3. PREVENIR RIESGOS Y DAÑOS

De acuerdo al proceso que sigue la metodología Magerit, se procedió a hacer un detalle de las actividades a desplegarse dentro de la institución para mitigar riesgos y daños, tomando en cuenta los tipos de amenazas a los que está expuesta la institución y considerando que la gestión y tratamiento del riesgo es de competencia de la empresa se hacen la siguientes propuesta, las cuales quedaran en potestad de la institución su aplicación:

3.3.1. [N] AMENAZAS DE TIPO NATURAL

Este tipo de amenazas pueden darse en el momento menos esperado, por lo que es importante estar preparados para enfrentar situaciones adversas que ponen en peligro el buen funcionamiento de la institución, entendiendo que los elementos que conforman este tipo de amenazas son de difícil estimación previa, se vuelve fundamental que la organización cuente con medidas preventivas ante eventos inesperados.

Como resultado del desarrollo las amenazas **fuego** nos ha sido considerada como la amenaza de tipo natural con **riesgo alto y el impacto muy alto**, por lo que es necesario que la institución tome las medidas necesarias para reducir este riesgo, tales como:

- Respaldar sus activos de información, con la cobertura de seguros para la institución.
- Que las edificaciones, cuente con escaleras y salidas de emergencia, materiales de construcción resistentes al fuego, planes de evacuación.
- Habilitar sensores contra fuego y elementos de mitigación del mismo.

3.3.2. [I] DE ORIGEN INDUSTRIAL

Son provocadas por inconvenientes dentro de la institución como cortocircuitos y otros que puedan poner en riesgo la integridad de los trabajadores y la funcionalidad de los equipos, en este grupo se presentan los siguientes tipos de amenazas:

Fuego como la amenaza de mayor riesgo, presentando un **impacto muy alto y un riesgo alto**, para lo cual la institución debe tratar de reducir esta amenaza tomando medidas como:

- Evitar el almacenamiento de productos inflamables dentro de la institución.
- Que las redes eléctricas, estén diseñada de tal forma que no representen ningún riesgo, por sobre carga de equipos.
- Revisar periódicamente las conexiones eléctricas para evitar su deterioro.

Avería de origen físico o lógico esta amenaza es considerada con un **impacto muy alto y un riesgo alto** y la institución lo debe evitar para lo cual se podrían tomar medidas como:

- Realizar mantenimiento preventivo, de acuerdo a lo planificado para los equipos, con la finalidad de evitar daño físico que comprometa el buen funcionamiento del sistema.
- Deshabilitar en el equipo los servicios que no sean necesarios para evitar la caída del sistema en un momento dado.
- Instalar solamente el software requerido dentro de las estaciones de trabajo, para evitar la lentitud del equipo con la funcionalidad del mismo.

El fallo de servicios de comunicaciones es una amenaza considerada con un **impacto muy alto y un riesgo alto**, teniendo presente que es una institución del segmento financiero, que necesita estar en línea para poder

cumplir con los procesos y brindar los servicios, esta es una amenaza que se debe evitar, para lo cual se deben tomar acciones correctivas como:

- Disponer de redundancia de comunicaciones, en las redes.
- Desarrollar periódicamente, análisis en el estado de los equipos y su desempeño
- Gestionar el flujo de tráfico en todos sus segmentos

3.3.3. [E] ERRORES Y FALLOS NO INTENCIONADOS

Este tipo de fallos se puede presentar en cualquier institución ya sea por acción u omisión de procesos a seguir por parte del personal, generalmente se presentan cuando hay trabajadores nuevos dentro de la institución que no conocen bien el trabajo que se lleva dentro de la misma, los considerados más altos son:

Difusión de software dañino el cual tiene **un riesgo alto e impacto alto** por lo que se sugiere eliminar esta amenaza pudiendo tomar acciones como:

- Contar con seguridad en todos los segmentos de la red.
- Controlar la instalación de las aplicaciones nuevas, que estas se desenvuelvan enmarcado en la política de la institución.
- Todos los computadores y servidores deben contar con antivirus, evitar su propagación por la red.
- Actualizar periódicamente las bases de definiciones, de los antivirus.

Vulnerabilidades de los programas (software) es una amenaza con **riesgo alto e impacto alto** por lo que se sugiere eliminar la amenaza tomando acciones como:

- Hacer las actualizaciones pertinentes al software.

- Antes de hacer cambios al sistema se deben seguir reglas básicas de seguridad a la hora de escribir código, evitando el ingreso caracteres extraños.
- Evitar el uso de software no licenciado.
- Es necesario realizar pruebas del sistema antes de ponerlo en marcha, para evitar posibles fallas y la interrupción del servicio.

3.3.4. [A] ATAQUE INTENCIONADOS

Son aquellos que los causan personas generalmente de la institución con acceso al sistema de información, con el único afán de causar daños o de obtener un beneficio propio, entre estos los más relevantes son:

Suplantación de la identidad del usuario con un **riesgo alto e impacto Alto** por lo cual se sugiere eliminar la amenaza tomando acciones pertinentes como:

- Hacer conocer las políticas de seguridad de la empresa.
- Capacitar al personal antes de contratarlo para que conozca cómo identificar esta amenaza.
- Las claves, deben ser única por cada usuario y caducar periódicamente para que se realice su cambio.
- No abrir mensajes de correo que pidan datos de la persona o de la institución donde trabaja.

La **difusión de software dañino** de forma deliberada es una amenaza que pone en peligro no solo los procesos que se llevan en la institución sino también información que se maneja, causando demoras en la prestación de servicios y la pérdida parcial o total de la información con lo cual **riesgo alto e impacto alto** por lo que es necesario tomar medidas para eliminar la amenaza.

- Todos los computadores y servidores deben contar con antivirus, evitar su propagación por la red.
- Mantener actualizado el sistema operativo y las aplicaciones que se utilizan en la institución.
- Fomentar la cultura, de no participar en cadenas, y la instalación o abrir aplicaciones extrañas

Considerando que la **destrucción de información** es una amenaza de **riesgo muy alto e impacto alto** que causa grandes daños en la institución es necesario reducirla tomando acciones como:

- Hacer respaldos diarios de la información en forma física y lógica.
- Limitar el acceso de los empleados al sistema según la función que desempeñan.
- Capacitar al personal para que hagan uso adecuado de la información que se hospeda en el sistema.

Robo es una amenaza de que representa un **riesgo e impacto muy alto** por lo cual se considera necesario eliminarla:

- Instruir al personal, para que no libere información confidencial, ya sea de los empleados, socios o de la institución en general que pueda ser utilizada para cometer actos delictivos.
- Respaldar sus activos de información, con la cobertura de seguros para la institución.
- Limitar el acceso a las instalaciones sensibles de la institución, para evitar que se sustraigan objetos.
- Utilizar cámaras de vigilancia que les permita identificar acciones sospechosas dentro de la institución.

3.4. PROPUESTA DE SALVAGUARDAS

Con el análisis de riesgos realizado en la Cooperativa de ahorro y crédito Calceta limitada, se determinó la exposición al riesgo y el impacto que sufrirían en caso de que se materialice la amenaza, partiendo desde el punto que en la institución han adoptado medidas que les ayuden a mitigarlos se realizó una propuesta de salvaguardas, la cual fue realizada con el fin de que la institución sufra los menores daños posibles.

De acuerdo al proceso metodológico se determinan las salvaguardas a partir de los resultados de la exposición al riesgo, el proceso fue el siguiente:

1.- Calcular el valor del impacto, considerando el costo económico de los activos por cada amenaza y la degradación.

Impacto = Valor Activo * Degradación

2.- Calcular el valor del riesgo tomando en cuenta el resultado del impacto y la frecuencia.

Riesgo= Impacto * Frecuencia estimada

Luego calcular la exposición al riesgo y considerando los datos obtenidos de las matrices de riesgo – impacto se procedió a realizar una propuesta de salvaguardas para la institución, para en caso de materializarse las amenazas potenciales obtenidas, tomando en cuenta la frecuencia y la probabilidad de ocurrencia de cada una y siendo de prioridad las aquellas cuyos impacto y riesgo es medio, alto y muy alto; considerando que las amenazas de riesgo bajo y muy bajo no representan mayor daño a la institución y por ende la institución puede aceptarlas.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

El trabajo realizado en la Cooperativa de Ahorro y Crédito Calceta Limitada, dio como primer resultado el inventario del hardware actualizado de los activos más relevantes de la institución con sus respectivas valoraciones económicas, entre los cuales se encuentran estaciones de trabajo, servidores, equipos de impresión, computadores portátiles, equipos de comunicación, sistemas de administración de energía, y otros activos de hardware importantes (Anexo 2).

También se realizó la valoración de los activos de forma cualitativa, con el fin de saber la necesidad que se tiene de proteger determinado activo de acuerdo al papel que desempeña en los servicios que brinda la institución tomando en cuenta las dimensiones: Alta, Media, Baja.

Cuadro 4.01. Valoración cualitativa (Estación de trabajo)

Estaciones de Trabajo							
Item	Nombre del Activo	Tipo	Departamento Encargado	Responsable	Dimensiones		
					Confidencialidad	Disponibilidad	Integridad
1	Computador Intel Core I7-4770	Equipos Informáticos	Tecnología de Información	Walter Párraga	MEDIO	ALTO	MEDIO
2	Computador Core I7-4770 3.40 GHZ	Equipos Informáticos	Tecnología de Información	Javier Ormaza	MEDIO	ALTO	MEDIO
3	Computador Core I7-3770 3.4 GHZ	Equipos Informáticos	Tecnología de Información	Ramón Párraga	MEDIO	ALTO	MEDIO
4	Computador Intel Core I7-4770	Equipos Informáticos	Tecnología de Información	Carlos párraga	MEDIO	ALTO	MEDIO
5	Computador Intel Pentium IV 2.66 GHZ	Equipos Informáticos	Tecnología de Información	Sistemas	MEDIO	ALTO	MEDIO
6	Computador Intel Pentium IV 3.0 GHZ	Equipos Informáticos	Tecnología de Información	Sistemas	MEDIO	ALTO	MEDIO
7	Computador Core I7-3770 3.40 GHZ	Equipos Informáticos	Dirección Administrativa y de operaciones	Patricio Maya	MEDIO	ALTO	MEDIO
8	Computador Core I7-2600 3.40 GHZ	Equipos Informáticos	Captaciones	Gretty Sacón	MEDIO	ALTO	MEDIO
9	Computador Intel Core I7-2600 3.4 GHZ	Equipos Informáticos	Captaciones	Karol Velásquez	MEDIO	ALTO	MEDIO
10	Computador Untel Core I7-2600 3.4 GHZ	Equipos Informáticos	Captaciones	Karol Velásquez	MEDIO	ALTO	MEDIO
11	Compuador Intel Pentium 4 3.00 GHZ	Equipos Informáticos	Captaciones	Gretty Sacón	MEDIO	ALTO	MEDIO
12	Computador Core 2 DUO E4500 2.2 GHZ	Equipos Informáticos	Captaciones	Gretty Sacón	MEDIO	ALTO	MEDIO
13	Computador Core I7-2600 3.40 GHZ	Equipos Informáticos	Captaciones	Natathy Velásquez	MEDIO	ALTO	MEDIO
14	Computador Core I7-2600 3.40 GHZ	Equipos Informáticos	Captaciones	Martha Correa	MEDIO	ALTO	MEDIO
15	Computador Intel Pentium D 3.00 GHZ	Equipos Informáticos	Captaciones	Susana Proaño	MEDIO	ALTO	MEDIO
16	Computador Intel Pentium 3.00GHZ	Equipos Informáticos	Captaciones	Bono	MEDIO	ALTO	MEDIO
17	Computador Intel Celeron 1.7 GHZ	Equipos Informáticos	Captaciones	Bono	MEDIO	ALTO	MEDIO
18	Computador Intel Pentium D 1.6 GHZ E2140	Equipos Informáticos	Colocaciones	Anita Cedeño	MEDIO	ALTO	MEDIO
19	Computador Intel Core I3 3.07 GHZ	Equipos Informáticos	Colocaciones	Valeria Sanchez	MEDIO	ALTO	MEDIO
20	Computador Intel Core I3 540 3.07 GHZ	Equipos Informáticos	Colocaciones	Mariano Álava	MEDIO	ALTO	MEDIO
21	Computador Intel Core I7 3770 3.4 GHZ	Equipos Informáticos	Colocaciones	Johnny Velez	MEDIO	ALTO	MEDIO
22	Computador Intel Core 2 QUAD Q8400 2.66 GHZ	Equipos Informáticos	Colocaciones	Alejandro Cantos	MEDIO	ALTO	MEDIO
23	Computador Intel Core I7 870 2.93 GHZ	Equipos Informáticos	Colocaciones	Fernando Santana	MEDIO	ALTO	MEDIO
24	Computador Intel Core2 DUO E7500 2.94 GHZ	Equipos Informáticos	Colocaciones	Patricia Lucas	MEDIO	ALTO	MEDIO
25	Computador Core 2 QUAD Q8400 2.66 GHZ	Equipos Informáticos	Colocaciones	Katiuska Faubla	MEDIO	ALTO	MEDIO
26	Computador Core I7-3770 3.40 GHZ	Equipos Informáticos	Colocaciones	Álvarez Magdalena	MEDIO	ALTO	MEDIO
27	Computador Intel Dual Core E2160 1.80 GHZ	Equipos Informáticos	Secretaría	Yessie Gonzáles	MEDIO	ALTO	MEDIO
28	Computador CoreE I7 - 2600 3.40 GHz	Equipos Informáticos	Secretaría	Yessie Gonzáles	MEDIO	ALTO	MEDIO
29	Computador Core I7-2600 3.40 GHZ	Equipos Informáticos	Talento Hunamo	Angeles Vera	MEDIO	ALTO	MEDIO
30	Computador Core I7-3770 3.4 GHZ	Equipos Informáticos	Contabilidad	Maria Vidal	MEDIO	ALTO	MEDIO
31	Computador Core I7-870 2.93 GHZ	Equipos Informáticos	Contabilidad	Carmen Chávez	MEDIO	ALTO	MEDIO
32	Computador Core 2 QUAD Q6600 2.4 GHZ	Equipos Informáticos	Contabilidad	Victoria Zambrano	MEDIO	ALTO	MEDIO
33	Computador Core I7-4770 3.40 GHZ	Equipos Informáticos	Riesgos	Helen Bravo	MEDIO	ALTO	MEDIO
34	Computador Core I7-870 2.93 GHZ	Equipos Informáticos	Riesgos	Iván Caicedo	MEDIO	ALTO	MEDIO
35	Computador Core I7-870 2.93 GHZ	Equipos Informáticos	Auditoría	Amparo Vélez	MEDIO	ALTO	MEDIO
36	Computador Pentium D 2160 1.70 GHZ	Equipos Informáticos	Auditoría	Bono	MEDIO	ALTO	MEDIO

Fuente: Las autoras|

Cuadro 4.02. Valoración cualitativa (Servidores)

Servidores							
Item	Nombre del Activo	Tipo	Departamento Encargado	Responsable	Dimensiones		
					Confidencialidad	Disponibilidad	Integridad
1	Servidor de Base de Datos y Aplicaciones 2 Intel Xeon DE 2GHZ	Equipos Informáticos	Tecnología de Información	Sistemas	MUY ALTO	MUY ALTO	MUY ALTO
2	Servidor de Base de Datos y Aplicaciones 2 Intel Xeon DE 2GHZ	Equipos Informáticos	Tecnología de Información	Sistemas	MEDIO	MEDIO	MEDIO
3	Servidor de Respaldo Xeon E3-1225 V3 3.10GHZ	Equipos Informáticos	Tecnología de Información	Sistemas	MUY ALTO	MUY ALTO	MUY ALTO
4	Servidor de Cajero Automático y Ahorro Movil Xeon E3-1225 V3 3.10GHZ	Equipos Informáticos	Tecnología de Información	Sistemas	ALTO	ALTO	ALTO
5	Servidor Proxy Intel Xeon DE 2.4GHZ	Equipos Informáticos	Tecnología de Información	Sistemas	ALTO	ALTO	ALTO
6	Servidor de Riesgos 2 Intel Xeon de 3GHZ	Equipos Informáticos	Tecnología de Información	Sistemas	ALTO	ALTO	ALTO
7	Servidor Intel Xeon de 2.8GHZ	Equipos Informáticos	Tecnología de Información	Sistemas	MEDIO	MEDIO	MEDIO
8	Servidor de Antivirus Intel Pentium de 3 GHZ	Equipos Informáticos	Tecnología de Información	Sistemas	ALTO	ALTO	ALTO

Fuente: Las autoras

Cuadro 4.03. Valoración cualitativa (Computador portátil)

Computador Portatil							
Item	Nombre del Activo	Tipo	Departamento Encargado	Responsable	Dimensiones		
					Confidencialidad	Disponibilidad	Integridad
1	PortatilL Pavilon 2725LA, Capacidad 160GB, Ram 4GB	Equipos Informáticos	Tecnologia de Información	Gerencia	ALTO	ALTO	MEDIO

Fuente: Las autoras

Cuadro 4.04. Valoración cualitativa (Equipos de computación)

Equipos de Comunicación							
Item	Nombre del Activo	Tipo	Departamento Encargado	Responsable	Dimensiones		
					Confidencialidad	Disponibilidad	Integridad
1	Switch Hp GbE2c Layer 2/3 Ethernet Blade	Equipos Informáticos	Tecnología de Información	Sistemas	MUY ALTO	MUY ALTO	MUY ALTO
2	Switch Cisco SG500-52	Equipos Informáticos	Tecnología de Información	Sistemas	MUY ALTO	MUY ALTO	MUY ALTO
3	Switch Cisco SG500-52	Equipos Informáticos	Tecnología de Información	Sistemas	MUY ALTO	MUY ALTO	MUY ALTO
4	Central Telefónica Panasonic KX-TES824	Equipos Informáticos	Tecnología de Información	Sistemas	MUY ALTO	MUY ALTO	MUY ALTO

Fuente: Las autoras|

Cuadro 4.05. Valoración cualitativa (Sistema de administración de energía)

Sistemas de Administración de Energía							
Item	Nombre del Activo	Tipo	Departamento Encargado	Responsable	Dimensiones		
					Confidencialidad	Disponibilidad	Integridad
1	Ups Powerware Prestige 3000 20 KWA	Equipos Informáticos	CAPTACIONES	Cajero Automático	MUY ALTO	MUY ALTO	MUY ALTO

Fuente: Las autoras

Cuadro 4.05. Valoración cualitativa (Equipos de Impresión)

Equipos de Impresión							
Item	Nombre del Activo	Tipo	Departamento Encargado	Responsable	Dimensiones		
					Confidencialidad	Disponibilidad	Integridad
1	Impresora MG-2120	Equipos Informáticos	Tecnología de Información	Walter Párraga	BAJO	ALTO	MEDIO
2	Impresora MG-2120	Equipos Informáticos	Crédito	Kathiuska Faubla	BAJO	ALTO	MEDIO
3	Impresora MG-2120	Equipos Informáticos	Tecnología de Información	Javier Ormaza	BAJO	ALTO	MEDIO
4	Impresora ML-2010	Equipos Informáticos	Contabilidad	Carmen Chávez	BAJO	ALTO	MEDIO
5	Impresora ML-2010	Equipos Informáticos	Riesgos	Helen Bravo	BAJO	ALTO	MEDIO
6	Impresora TX410	Equipos Informáticos	Tecnología de Información	Ramón Párraga	BAJO	ALTO	MEDIO
7	Impresora MP-250	Equipos Informáticos	Direccion Administrativa y de operacioens	Patricio Maya	BAJO	ALTO	MEDIO
8	Impresora MP-250	Equipos Informáticos	Captaciones	Gretty Sacón	BAJO	ALTO	MEDIO
9	Impresora MP-250	Equipos Informáticos	Colocaciones	Magdalena Álvarez	BAJO	ALTO	MEDIO
10	Impresora MP-250	Equipos Informáticos	Colocaciones	Magdalena Álvarez	BAJO	ALTO	MEDIO
11	Impresora MP-250	Equipos Informáticos	Secretaria	Jessie González	BAJO	ALTO	MEDIO
12	Impresora MP-250	Equipos Informáticos	Auditoria	Amparo Vélez	BAJO	ALTO	MEDIO
13	Impresora MP-280	Equipos Informáticos	Captaciones	Karol Velásquez	BAJO	ALTO	MEDIO
14	Impresora FX-890	Equipos Informáticos	Captaciones	Karol Velásquez	BAJO	ALTO	MEDIO
15	Impresora FX-890	Equipos Informáticos	Captaciones	Gretty Sacón	BAJO	ALTO	MEDIO
16	Impresora TMU-950S	Equipos Informáticos	Captaciones	Gretty Sacón	BAJO	ALTO	MEDIO
17	Impresora TMU-950S	Equipos Informáticos	Captaciones	Natathy Velásquez	BAJO	ALTO	MEDIO
18	Impresora TMU-950S	Equipos Informáticos	Captaciones	Susana Proaño	BAJO	ALTO	MEDIO
19	Impresora ML-2165	Equipos Informáticos	Captaciones	Natathy Velásquez	BAJO	ALTO	MEDIO
20	Impresora MP-230	Equipos Informáticos	Captaciones	Martha Correa	BAJO	ALTO	MEDIO
21	Impresora MP-230	Equipos Informáticos	Talento Humano	Ángeles Bravo	BAJO	ALTO	MEDIO
22	Impresora P361A	Equipos Informáticos	Captaciones	Bono	BAJO	ALTO	MEDIO
23	Impresora FX-890	Equipos Informáticos	Colocaciones	Valeria Sánchez	BAJO	ALTO	MEDIO
24	Impresora LX-355	Equipos Informáticos	Colocaciones	Kathiuska Faubla	BAJO	ALTO	MEDIO
25	Impresora FX-890	Equipos Informáticos	Contaillidad	Victoria Zambrano	BAJO	ALTO	MEDIO
26	Impresora WC4118	Equipos Informáticos	Secretaria	Excio Espinel	BAJO	ALTO	MEDIO
27	Copiadora Aficio MP301	Equipos Informáticos	Colocaciones	Kathiuska Faubla	BAJO	ALTO	MEDIO
28	Copiadora Studio 2505	Equipos Informáticos	Secretaria	Jessie González	BAJO	ALTO	MEDIO
29	Fax KX-FT981LA	Equipos Informáticos	Contabilidad	Carmen Chávez	BAJO	ALTO	MEDIO
30	Fax KX-FT981LA	Equipos Informáticos	Colocaciones	Magdalena Álvarez	BAJO	ALTO	MEDIO

Fuente: Las autoras

Cuadro 4.06. Valoración cualitativa (Otros activos de hardware)

Otros Activos de Hardware							
Item	Nombre del Activo	Tipo	Departamento Encargado	Responsable	Dimensiones		
					Confidencialidad	Disponibilidad	Integridad
1	Cámara Digital DMC-LS80	Equipos Informáticos	Captaciones	Jessie González	MEDIO	MEDIO	MEDIO
2	Cámara Ip de Seguridad STC-165	Equipos Informáticos	Captaciones	Gretty Sacón	ALTO	ALTO	MEDIO
3	Lector de Firmas D-LBK460-HSDR	Equipos Informáticos	Captaciones	Karol Velásquez	MEDIO	ALTO	MEDIO
4	Reloj Biométrico Control de Entrada y Salida	Equipos Informáticos	Dirección Administrativa y de operaciones	Patricio Maya	ALTO	ALTO	MEDIO
5	Reloj Biométrico Control de Acceso	Equipos Informáticos	Dirección Administrativa y de operaciones	Patricio Maya	ALTO	ALTO	MEDIO

Fuente: Las autoras

Cuadro 4.07. Valoración cualitativa (Software)

Software							
Item	Nombre del Activo	Tipo	Departamento Encargado	Responsable	Dimensiones		
					Confidencialidad	Disponibilidad	Integridad
1	Base de Datos Oracle 2CC	Software	Tecnología de Información	Sistemas	MUY ALTO	MUY ALTO	MUY ALTO
2	Base de Datos Sql Server 2007	Software	Tecnología de Información	Sistemas	MUY ALTO	MUY ALTO	MUY ALTO
3	Core Financiero Softbank 2.16	Software	Tecnología de Información	Sistemas	MUY ALTO	MUY ALTO	MUY ALTO
4	Sistema Caefic	Software	Tecnología de Información	Sistemas	MUY ALTO	MUY ALTO	MUY ALTO
5	Powerbuilder 12.5	Software	Tecnología de Información	Sistemas	MEDIO	MEDIO	MEDIO
6	Antivirus Mcafee	Software	Tecnología de Información	Sistemas	MEDIO	ALTO	ALTO
7	Winrar	Software	Tecnología de Información	Sistemas	MEDIO	MEDIO	MEDIO
8	Microsoft Office 2010	Software	Tecnología de Información	Sistemas	MEDIO	MEDIO	MEDIO
9	Adobe Reader	Software	Tecnología de Información	Sistemas	MEDIO	MEDIO	MEDIO
10	Zero	Software	Tecnología de Información	Sistemas	MEDIO	MEDIO	MEDIO
11	Teamviewer	Software	Tecnología de Información	Sistemas	MEDIO	ALTO	MEDIO
12	Vnc	Software	Tecnología de Información	Sistemas	BAJO	MEDIO	MEDIO
13	Sistema de Correo Electrónico Outlook	Software	Tecnología de Información	Sistemas	ALTO	ALTO	ALTO
14	Sitio Web Empresarial	Software	Tecnología de Información	Sistemas	BAJO	ALTO	ALTO

Fuente: Las autoras

Luego de realizadas las matrices de riesgo, se obtuvo la estimación del impacto, cuyos datos se detallan en el siguiente cuadro:

Cuadro 4.08. Estimación del impacto

Código	Amenazas	Valor (dimensiones)		Degradación		Estimación del impacto	
		Valor	Siglas	Valor	Siglas	valor	siglas
[N.1]	Fuego	Muy Alto	MA	Alto	A	Muy Alto	MA
[N.2]	Daños por agua	Medio	M	Medio	M	Bajo	B
[N.*]	Desastres naturales	Alto	MA	Medio	M	Medio	MA
[I.1]	Fuego	Muy Alto	MA	Alto	A	Muy Alto	MA
[I.2]	Daños por agua	Medio	M	Alto	A	Medio	MA
[I.*]	Desastres industriales	Medio	M	Medio	M	Bajo	B
[I.3]	Contaminación mecánica	Media	M	Media	M	Bajo	B
[I.4]	Contaminación electromagnética	Media	M	Alto	A	Muy Bajo	MB
[I.5]	Avería de origen fisico o lógico	Muy Alto	MA	Medio	M	Alto	A
[I.6]	Corte del suministro eléctrico	Alto	A	Medio	M	Medio	M
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	Medio	M	Medio	M	Bajo	B
[I.8]	Fallo de servicios de comunicaciones	Muy Alto	A	Medio	M	Alto	A
[I.9]	Interrupción de otros servicios y suministros esenciales	Alto	A	Medio	M	Medio	M
[I.10]	Degradación de los soportes de almacenamiento de la información	Muy Alto	MA	Alto	A	Muy Alto	MA
[E.1]	Errores de los usuarios	Medio	A	Medio	M	Bajo	B
[E.2]	Errores del administrador	Alto	A	Medio	M	Medio	M
[E.4]	Errores de configuración	Alto	A	Medio	M	Medio	M
[E.7]	Deficiencias en la organización	Medio	M	Bajo	B	Muy Bajo	MB
[E.8]	Difusión de software dañino	Muy Alto	MA	Medio	M	Alto	A
[E.9]	Errores de [re-]encaminamiento	Muy Alto	M	Bajo	B	Medio	M
[E.10]	Errores de secuencia	Medio	M	Bajo	B	Muy Bajo	MB
[E.14]	Escapes de información	Muy Alto	MA	Bajo	B	Medio	M
[E.15]	Alteración accidental de la información	Alto	A	Medio	M	Medio	M
[E.18]	Destrucción de información	Alto	A	Alto	A	Alto	A
[E.19]	Fugas de información	Muy Alto	A	Medio	B	Alto	A
[E.20]	Vulnerabilidades de los programas (software)	Muy Alto	MA	Medio	M	Alto	A
[E.21]	Errores de mantenimiento / actualización de programas (software)	Alto	A	Medio	M	Medio	M
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Alto	A	Medio	M	Medio	M
[E.24]	Caída del sistema por agotamiento de recursos	Alto	A	Bajo	B	Bajo	B
[E.28]	Indisponibilidad del personal	Medio	M	Bajo	B	Muy Bajo	MB
[A.4]	Manipulación de la configuración	Muy Alto	MA	Medio	M	Alto	A
[A.5]	Suplantación de la identidad del usuario	Muy Alto	MA	Medio	M	Alto	A
[A.6]	Abuso de privilegios de acceso	Muy Alto	MA	Bajo	B	Medio	M
[A.7]	Uso no previsto	Alto	A	Bajo	B	Bajo	B
[A.8]	Difusión de software dañino	Muy Alto	MA	Medio	M	Alto	A
[A.11]	Acceso no autorizado	Alto	A	Bajo	B	Medio	M
[A.12]	Análisis de tráfico	Alto	A	Bajo	B	Bajo	B
[A.13]	Repudio	Alto	A	Bajo	B	Bajo	B
[A.14]	Interceptación de información	Alto	A	Bajo	B	Bajo	B
[A.15]	Modificación deliberada de la información	Alto	A	Medio	M	Medio	M
[A.18]	Destrucción de información	Muy Alto	MA	Alto	A	Muy Alto	MA
[A.19]	Revelación de información	Muy Alto	MA	Bajo	B	Medio	M
[A.22]	Manipulación de programas	Muy Alto	MA	Bajo	B	Medio	M
[A.25]	Robo	Muy Alto	MA	Alto	A	Muy Alto	MA
[A.26]	Ataque destructivo	Medio	M	Alto	A	Medio	M
[E.28]	Indisponibilidad del personal	Muy Alto	MA	Medio	B	Medio	M
[A.29]	Extorsión	Alto	M	Medio	M	Medio	M
[A.30]	Ingeniería social	Alto	A	Medio	M	Medio	M

Fuente: Las Autoras

Después de la estimación del impacto, se realizó la estimación del riesgo tomando en cuenta el resultado de cada impacto y la probabilidad de

ocurrencia por cada amenaza cuyos datos se detalla en el cuadro 4.09 a continuación:

Cuadro 4.09. Estimación del riesgo

Código amenaza	Amenaza	Estimacion de Impacto		Probabilidad de Ocurrencia		Estimación del Riesgo	
		Valor	Siglas	Valor	Siglas	Valor	Siglas
[N.1]	Fuego	Muy Alto	MA	Poco frecuente	PF	Alto	A
[N.2]	Daños por agua	Bajo	B	Frecuencia normal	PF	Bajo	B
[N.*]	Desastres naturales	Medio	MA	Frecuencia normal	FN	Medio	M
[I.1]	Fuego	Muy Alto	MA	Poco frecuente	PF	Alto	A
[I.2]	Daños por agua	Medio	MA	Poco frecuente	PF	Bajo	B
[I.*]	Desastres industriales	Bajo	B	Poco frecuente	PF	Muy Bajo	MB
[I.3]	Contaminación mecánica	Bajo	B	Muy Frecuente	MF	Alto	A
[I.4]	Contaminación electromagnética	Muy Bajo	MB	Poco frecuente	PF	Muy Bajo	MB
[I.5]	Avería de origen físico o lógico	Alto	A	Frecuencia normal	FN	Alto	A
[I.6]	Corte del suministro eléctrico	Medio	M	Frecuente	F	Alto	A
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	Bajo	B	Poco frecuente	PF	Muy Bajo	MB
[I.8]	Fallo de servicios de comunicaciones	Alto	A	Poco frecuente	PF	Alto	A
[I.9]	Interrupción de otros servicios y suministros esenciales	Medio	M	Frecuencia Normal	FN	Medio	M
[I.10]	Degradación de los soportes de almacenamiento de la información	Muy Alto	MA	Poco frecuente	PF	Alto	A
[E.1]	Errores de los usuarios	Bajo	B	Frecuencia normal	FN	Bajo	B
[E.2]	Errores del administrador	Medio	M	Frecuencia normal	FN	Medio	M
[E.4]	Errores de configuración	Medio	M	Frecuencia normal	FN	Medio	M
[E.7]	Deficiencias en la organización	Muy Bajo	MB	Frecuencia normal	FN	Muy Bajo	MB
[E.8]	Difusión de software dañino	Alto	A	Frecuencia normal	FN	Alto	A
[E.9]	Errores de [re-]encaminamiento	Medio	M	Poco frecuente	PF	Bajo	B
[E.10]	Errores de secuencia	Muy Bajo	MB	Poco frecuente	PF	Muy Bajo	MB
[E.14]	Escapes de información	Medio	M	Frecuencia normal	FN	Medio	M
[E.15]	Alteración accidental de la información	Medio	M	Poco frecuente	PF	Bajo	B
[E.18]	Destrucción de información	Alto	A	Poco frecuente	PF	Medio	M
[E.19]	Fugas de información	Alto	A	Poco frecuente	PF	Medio	M
[E.20]	Vulnerabilidades de los programas (software)	Alto	A	Frecuencia normal	FN	Alto	A
[E.21]	Errores de mantenimiento / actualización de programas (software)	Medio	M	Poco frecuente	PF	Medio	M
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Medio	M	Frecuencia normal	FN	Medio	M
[E.24]	Caída del sistema por agotamiento de recursos	Bajo	B	Frecuencia normal	PF	Bajo	B
[E.28]	Indisponibilidad del personal	Muy Bajo	MB	Frecuente	F	Bajo	B
[A.4]	Manipulación de la configuración	Alto	A	Poco frecuente	PF	Medio	M
[A.5]	Suplantación de la identidad del usuario	Alto	A	Frecuencia normal	FN	Alto	A
[A.6]	Abuso de privilegios de acceso	Medio	M	Frecuencia normal	FN	Medio	M
[A.7]	Uso no previsto	Bajo	B	Frecuencia normal	FN	Bajo	B
[A.8]	Difusión de software dañino	Alto	A	Frecuencia normal	FN	Alto	A
[A.11]	Acceso no autorizado	Medio	M	Frecuencia normal	FN	Medio	M
[A.12]	Análisis de tráfico	Bajo	B	Poco frecuente	PF	Muy Bajo	MB
[A.13]	Repudio	Bajo	B	Frecuencia normal	FN	Bajo	B
[A.14]	Interceptación de información	Bajo	B	Frecuencia normal	FN	Bajo	B
[A.15]	Modificación deliberada de la información	Medio	M	Poco frecuente	PF	Bajo	B
[A.18]	Destrucción de información	Muy Alto	MA	Poco frecuente	PF	Alto	A
[A.19]	Revelación de información	Medio	M	Frecuencia normal	FN	Medio	M
[A.22]	Manipulación de programas	Medio	M	Frecuencia normal	FN	Medio	M
[A.25]	Robo	Muy Alto	MA	Frecuencia normal	FN	Alto	A
[A.26]	Ataque destructivo	Medio	M	Poco frecuente	PF	Bajo	B
[E.28]	Indisponibilidad del personal	Medio	M	Poco frecuente	PF	Bajo	B
[A.29]	Extorsión	Medio	M	Frecuencia normal	FN	Medio	M
[A.30]	Ingeniería social	Medio	M	Frecuencia normal	FN	Medio	M

Fuente: Las autoras

Realizada la valoración cualitativa se pudo determinar el peso medio que representa cada tipo de amenaza en la institución, dando como resultado una media de 3 en los cuatro casos, lo cual significa que la institución tiene un

riesgo medio de que estas amenazas se materialicen en ella, como se evidencia en el cuadro 4.10, 4.11, 4.12 y 4.13:

Cuadro 4.10 Valoración cuantitativa amenazas naturales

Desastres Naturales		
Código	**Amenaza**	**valor cuantitativo**
[N.1]	Fuego	4
[N.2]	Daños por agua	2
[N.*]	Desastres naturales	3
	Total	**9**
	Media	**3**

Fuente: Las autoras|

Cuadro 4.11. Valoración cuantitativa amenazas de origen industrial

De origen industrial		
Código	**Amenaza**	**valor cuantitativo**
[I.1]	Fuego	4
[I.2]	Daños por agua	2
[I.*]	Desastres industriales	1
[I.3]	Contaminación mecánica	4
[I.4]	Contaminación electromagnética	1
[I.5]	Avería de origen físico o lógico	4
[I.6]	Corte del suministro eléctrico	4
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	1
[I.8]	Fallo de servicios de comunicaciones	4
[I.9]	Interrupción de otros servicios y suministros esenciales	3
[I.10]	Degradación de los soportes de almacenamiento de la información	4
	Total	**32**
	Media	**2,91**

Fuente: Las autoras

Cuadro 4.12. Valoración cuantitativa amenazas por errores y fallos no intencionados

Errores y fallos no intencionados		
Código	**Amenaza**	**valor cuantitativo**
[E.1]	Errores de los usuarios	2
[E.2]	Errores del administrador	3
[E.4]	Errores de configuración	3
[E.7]	Deficiencias en la organización	1
[E.8]	Difusión de software dañino	4
[E.9]	Errores de [re-]encaminamiento	2
[E.10]	Errores de secuencia	1
[E.14]	Escapes de información	3
[E.15]	Alteración accidental de la información	2
[E.18]	Destrucción de información	3
[E.19]	Fugas de información	3
[E.20]	Vulnerabilidades de los programas (software)	4
[E.21]	Errores de mantenimiento / actualización de programas (software)	3
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3
[E.24]	Caída del sistema por agotamiento de recursos	2
[E.28]	Indisponibilidad del personal	2
	Total	**41**
	Media	**2,56**

Fuente: Las autoras

Cuadro 13. Valoración cuantitativa amenazas por ataques intencionados

Ataques intencionados		
Código	**Amenaza**	**valor cuantitativo**
[A.4]	Manipulación de la configuración	3
[A.5]	Suplantación de la identidad del usuario	4
[A.6]	Abuso de privilegios de acceso	3
[A.7]	Uso no previsto	2
[A.8]	Difusión de software dañino	4
[A.11]	Acceso no autorizado	3
[A.12]	Análisis de tráfico	1
[A.13]	Repudio	2
[A.14]	Interceptación de información	2
[A.15]	Modificación deliberada de la información	2
[A.18]	Destrucción de información	4
[A.19]	Revelación de información	3
[A.22]	Manipulación de programas	3
[A.25]	Robo	4
[A.26]	Ataque destructivo	2
[E.28]	Indisponibilidad del personal	2
[A.29]	Extorsión	3
[A.30]	Ingeniería social	3
	Total	**50**
	Media	**2,78**

Fuente: Las autoras

Una vez realizadas las matrices de riesgo e impacto se logró determinar la exposición al riesgo, la frecuencia con la que se dan estas amenazas y las decisiones de tratamiento del riesgo como se muestra en el cuadro 4.14.

Cuadro 4.14. Decisiones de Tratamiento del Riesgo

Código Amenza	Amenaza	Nivel de impacto	Nivel de riesgo	Frecuencia	Tratamiento del riesgo
[N.1]	Fuego	Muy Alto	Alto	Poco frecuente	reduce
[N.2]	Daños por agua	Bajo	Bajo	Frecuencia normal	reduce
[N.*]	Desastres naturales	Medio	Medio	Frecuencia normal	reduce
[I.1]	Fuego	Muy Alto	Alto	Poco frecuente	reduce
[I.2]	Daños por agua	Medio	Bajo	Poco frecuente	reduce
[I.*]	Desastres industriales	Bajo	Muy Bajo	Poco frecuente	reduce
[I.3]	Contaminación mecánica	Bajo	Alto	Muy Frecuente	eliminar
[I.4]	Contaminación electromagnética	Muy Bajo	Muy Bajo	Poco frecuente	acepta
[I.5]	Avería de origen físico o lógico	Alto	Alto	Frecuencia normal	evita
[I.6]	Corte del suministro eléctrico	Medio	Alto	Frecuente	evita
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	Bajo	Muy Bajo	Poco frecuente	reduce
[I.8]	Fallo de servicios de comunicaciones	Alto	Alto	Poco frecuente	evita
[I.9]	Interrupción de otros servicios y suministros esenciales	Medio	Medio	Frecuencia Normal	reduce
[I.10]	Degradación de los soportes de almacenamiento de la información	Muy Alto	Alto	Poco frecuente	evita
[E.1]	Errores de los usuarios	Bajo	Bajo	Frecuencia normal	reduce
[E.2]	Errores del administrador	Medio	Medio	Frecuencia normal	reduce
[E.4]	Errores de configuración	Medio	Medio	Frecuencia normal	evita
[E.7]	Deficiencias en la organización	Muy Bajo	Muy Bajo	Frecuencia normal	acepta
[E.8]	Difusión de software dañino	Alto	Alto	Frecuencia normal	eliminar
[E.9]	Errores de [re-]encaminamiento	Medio	Bajo	Poco frecuente	reduce
[E.10]	Errores de secuencia	Muy Bajo	Muy Bajo	Poco frecuente	acepta
[E.14]	Escapes de información	Medio	Medio	Frecuencia normal	reduce
[E.15]	Alteración accidental de la información	Medio	Bajo	Poco frecuente	reduce
[E.18]	Destrucción de información	Alto	Medio	Poco frecuente	reduce
[E.19]	Fugas de información	Alto	Medio	Poco frecuente	reduce
[E.20]	Vulnerabilidades de los programas (software)	Alto	Alto	Frecuencia normal	eliminar
[E.21]	Errores de mantenimiento / actualización de programas (software)	Medio	Medio	Poco frecuente	reduce
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Medio	Medio	Frecuencia normal	evita
[E.24]	Caída del sistema por agotamiento de recursos	Bajo	Bajo	Frecuencia normal	evita
[E.28]	Indisponibilidad del personal	Muy Bajo	Bajo	Frecuente	acepta
[A.4]	Manipulación de la configuración	Alto	Medio	Poco frecuente	reduce
[A.5]	Suplantación de la identidad del usuario	Alto	Alto	Frecuencia normal	eliminar
[A.6]	Abuso de privilegios de acceso	Medio	Medio	Frecuencia normal	reduce
[A.7]	Uso no previsto	Bajo	Bajo	Frecuencia normal	acepta
[A.8]	Difusión de software dañino	Alto	Alto	Frecuencia normal	eliminar
[A.11]	Acceso no autorizado	Medio	Medio	Frecuencia normal	reduce
[A.12]	Análisis de tráfico	Bajo	Muy Bajo	Poco frecuente	acepta
[A.13]	Repudio	Bajo	Bajo	Frecuencia normal	acepta
[A.14]	Interceptación de información	Bajo	Bajo	Frecuencia normal	acepta
[A.15]	Modificación deliberada de la información	Medio	Bajo	Poco frecuente	reduce
[A.18]	Destrucción de información	Muy Alto	Alto	Poco frecuente	reduce
[A.19]	Revelación de información	Medio	Medio	Frecuencia normal	reduce
[A.22]	Manipulación de programas	Medio	Medio	Frecuencia normal	reduce
[A.25]	Robo	Muy Alto	Muy Alto	Frecuencia normal	eliminar
[A.26]	Ataque destructivo	Muy Alto	Alto	Poco frecuente	reduce
[E.28]	Indisponibilidad del personal	Medio	Bajo	Poco frecuente	reduce
[A.29]	Extorsión	Medio	Medio	Frecuencia normal	reduce
[A.30]	Ingeniería social	Medio	Medio	Frecuencia normal	reduce

Fuente: Las autoras

Después de identificar las amenazas y tomando en cuenta datos importantes como: la susceptibilidad al riesgo y el impacto que causaría se realizó la propuesta de salvaguardas a la institución, la cual se detalla desde el cuadro 4.15 hasta el cuadro 4.40:

Cuadro 4.15. Determinación de Salvaguardas – Fuego

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[I.1]	Fuego	$ 1315,40	• [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [L] instalaciones • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	• [D] Disponibilidad
Salvaguarda				
Tipo de salvaguarda			**Valor $**	**Costo Estimado**
Evitar el almacenamiento de productos inflamables dentro de la institución.			0,00	0,00
Que las redes eléctricas, estén diseñada de tal forma que no estén propensas a riesgos, por sobre carga de equipos.			0,00	
No fumar dentro de la institución.			0,00	

Fuente: Las autoras

Cuadro 4.16. Determinación de Salvaguardas – Daños por agua

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[I.2]	Daños por agua	$ 1315,40	• [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [L] instalaciones • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	• [D] Disponibilidad
Salvaguarda				
Tipo de salvaguarda			**Valor $**	**Costo Estimado**
Dar mantenimiento a las instalaciones de agua, ya que estas se pueden averiar con el paso del tiempo.			$ 300,00	$ 300,00

Fuente: Las autoras

Cuadro 4.17. Determinación de Salvaguardas – Contaminación mecánica

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[I.3]	Contaminación mecánica	$ 12570,26	• [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	• [D] Disponibilidad

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Mantener las puertas y ventanas de las oficinas cerradas para evitar la entrada de polvo y suciedad.	0,00	$ 1920,00
Se debe de realizar el mantenimiento preventivo a los equipos, de acuerdo a las recomendaciones técnicas de cada uno de ellos.	$ 1920,00	

Fuente: Las autoras

Cuadro 4.18. Determinación de Salvaguardas – Avería de origen físico o lógico

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[I.5]	Avería de origen físico o lógico	$ 2020,85	• [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [SW] aplicaciones (software) • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	• [D] Disponibilidad

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Realizar mantenimiento preventivo, de acuerdo a lo planificado para los equipos, con la finalidad de evitar daño físico que comprometa el buen funcionamiento del sistema.	$ 1920,00	$ 1920,00
Instalar solamente el software requerido dentro de las estaciones de trabajo, para evitar la lentitud del equipo con la funcionalidad del mismo.	0,00	

Fuente: Las autoras

Cuadro 4.19. Determinación de Salvaguardas – Corte del suministro eléctrico

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[I.6]	Corte del suministro eléctrico	$ 419,01	• [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	• [D] Disponibilidad
Salvaguarda				
Tipo de salvaguarda		**Valor $**		**Costo Estimado**
Hacer mantenimiento periódico a la planta generadora para evitar su deterioro.		$ 750		$ 2250
Disponer de la continuidad de la energía con un sistema de UPS		$ 1500		

Fuente: Las autoras

Cuadro 4.20. Determinación de Salvaguardas – Condiciones inadecuadas de temperatura y/o humedad

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	$ 34,92	• [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	• [D] Disponibilidad
Salvaguarda				
Tipo de salvaguarda		**Valor $**		**Costo Estimado**
Realizar mantenimiento a los quipos climatizador de toda la institución, especialmente a los del data center para evitar el mal funcionamiento de los mismos.		$ 1800		$ 1800

Fuente: Las autoras

Cuadro 4.21. Determinación de Salvaguardas – Fallo de servicios de comunicaciones

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[I.8]	Fallo de servicios de comunicaciones	$ 3,79	• [COM] redes de comunicaciones	• [D] Disponibilidad

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Contar con enlaces redundantes	0,00	0,00
Hacer mantenimiento a las redes de datos periódicamente para evitar fallos de comunicaciones.	0,00	

Fuente: Las autoras

Cuadro 4.22. Determinación de Salvaguardas – Degradación de los soportes de almacenamiento de la información

Amenazas			Activo	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[I.10]	Degradación de los soportes de almacenamiento de la información	$ 200,12	• [AUX] equipamiento auxiliar	• [D] Disponibilidad

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Almacenar los soportes de almacenamiento de información en un lugar libre de polvo, humedad y otros que puedan deteriorarlos.	0,00	$500
Contar con un sistema de respaldo de información en más de un medio físico, con el fin de evitar pérdidas de información.	$500	

Fuente: Las autoras

Cuadro 4.23. Determinación de Salvaguardas – Errores de los usuarios

Amenazas			Activo	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[E.1]	Errores de los usuarios	$ 3526,58	• [MEDIA] soporte de información • [S] servicios • [D] datos/información	• [C] Confidencialidad • [I] Integridad • [D] Disponibilidad

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Sistemas de capacitación continua	$ 500	$ 250

Fuente: Las autoras

Cuadro 4.24. Determinación de Salvaguardas – Errores del administrador

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[E.2]	Errores del administrador	$ 3640,42	• [MEDIA] soporte de información • [S] servicios • [D] datos/información • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	• [C] Confidencialidad • [I] Integridad • [D] Disponibilidad • [A_S] Autenticidad del servicio • [A_D] Autenticidad de los datos

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Dar capacitaciones a los responsables de administrar información y que tienen personal a su cargo, como jefes de departamentos.	$ 800	$ 800
Hacer conocer las políticas de seguridad y privacidad a todos los empleados de la institución.	0,00	

Fuente: Las autoras

Cuadro 4.25. Determinación de Salvaguardas – Errores de configuración

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[E.4]	Errores de configuración	$ 4613,75	• [D] datos/información • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	• [C] Confidencialidad • [D] Disponibilidad • [I] Integridad • [A_S] Autenticidad del servicio • [A_D] Autenticidad de los datos

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Se debe contar con un personal capacitado para que no tenga inconvenientes al momento de operar.	0,00	0,00
Mantener registros de cada equipo que permitirá conocer parámetros al momento de realizar la configuración como: la persona responsable, el tipo de soporte, el tipo de información que contiene, entre otros.	0,00	

Fuente: Las autoras

Cuadro 4.26. Determinación de Salvaguardas – Difusión de software dañino

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[E.8]	Difusión de software dañino	$ 973,33	• [SW] aplicaciones (software)	• [C] Confidencialidad • [D] Disponibilidad • [I] Integridad

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Contar con seguridad en todos los segmentos de la red.	0,00	$ 2300
Controlar la instalación de las aplicaciones nuevas, que estas se desenvuelvan enmarcado en la política de la institución.	0,00	
Todos los computadores y servidores deben contar con antivirus, evitar su propagación por la red.	$ 2300	
Actualizar periódicamente las bases de definiciones, de los antivirus.	0,00	

Fuente: Las autoras

Cuadro 4.27. Determinación de Salvaguardas – Errores de [re-]encaminamiento

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[E.9]	Errores de [re-]encaminamiento	$ 8,87	• [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	• [C] Confidencialidad • [I] Integridad

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Capacitar a los usuarios de la institución sobre el uso adecuado de la red datos y envió de información.	$ 200	

Fuente: Las autoras

Cuadro 4.28. Determinación de Salvaguardas – Alteración accidental de la información

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[E.15]	Alteración accidental de la información	$ 45,08	• [D] datos/información	• [C] Confidencialidad
Salvaguarda				
Tipo de salvaguarda		**Valor $**		**Costo Estimado**
Capacitar al personal en el uso de los privilegios que se le han dado en el sistema, para evitar confusiones en el manejo de los datos del cliente, entendiendo que la información que manejan no pertenece a la institución sino a sus socios.		$ 300		$ 300
Contar con un perfil de usuario por empleado, así se puede determinar quién y cuándo hizo modificaciones en la información y con qué fin.		0,00		

Fuente: Las autoras

Cuadro 4.29. Determinación de Salvaguardas – Destrucción de información

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[E.18]	Destrucción de información	$ 450,85	• [D] datos/información	• [C] Confidencialidad
Salvaguarda				
Tipo de salvaguarda		**Valor $**		**Costo Estimado**
Se debe contar con soportes de información actualizados, para evitar la pérdida parcial o total de la información de la institución.		$ 0,00		$ 0,00

Fuente: Las autoras

Cuadro 4.30. Determinación de Salvaguardas – Fugas de información

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[E.19]	Fugas de información	$ 4,51	• [D] datos/información	• [C] Confidencialidad
Salvaguarda				
Tipo de salvaguarda		**Valor $**		**Costo Estimado**
Contar con sistemas de perdida de información.		0,00		$ 100
Capacitar a los empleados los cuales tienen perfiles de acceso al sistema de la institución sobre el valor que tiene la información y el peligro que representa la fuga de la misma		$ 100		

Fuente: Las autoras

Cuadro 4.31. Determinación de Salvaguardas – Vulnerabilidades de los programas (software)

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[E.20]	Vulnerabilidades de los programas (software)	$ 973,33	• [SW] aplicaciones (software)	• [I] Integridad • [C] Confidencialidad • [D] Disponibilidad
Salvaguarda				
Tipo de salvaguarda		**Valor $**		**Costo Estimado**
Es necesario realizar pruebas del sistema antes de ponerlo en marcha, para evitar posibles fallas y la interrupción del servicio.		0,00		0,00
Hacer las actualizaciones pertinentes al software.		0,00		
Evitar el uso de software no licenciado.		0,00		

Fuente: Las autoras

Cuadro 4.32. Determinación de Salvaguardas – Errores de mantenimiento / actualización de equipos (hardware)

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	$ 600,35	• [HW] equipos informáticos (hardware) • [MEDIA] soporte de información	• [D] Disponibilidad
Salvaguarda				
Tipo de salvaguarda		**Valor $**		**Costo Estimado**
Toda actualización se debe realizar en ambiente de calidad, previa a la liberación en productivo, con el fin de certificar su funcionamiento.		0,00		0,00
Los equipos informáticos deben estar protegidos contra cualquier fallo, para evitar la pérdida de datos.		$ 0,00		

Fuente: Las autoras

Cuadro 4.33. Determinación de Salvaguardas – Manipulación de la configuración

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[A.4]	Manipulación de la configuración	$ 153,79	• [COM] redes de comunicaciones • [HW] equipos informáticos (hardware) • [SW] aplicaciones (software) • [S] servicios • [D] datos/información	• [C] Confidencialidad • [D] Disponibilidad • [I] Integridad • [A_S] Autenticidad del servicio • [A_D] Autenticidad de los datos
Salvaguarda				
Tipo de salvaguarda		**Valor $**		**Costo Estimado**
El administrador debe estar atento a los cambios que realice en el sistema, y dar privilegios de usuario según el rol de cada empleado en la institución.		0,00		0,00
Debe existir bitácora de todo cambio que realice, identificando la responsabilidad de los usuarios y las acciones de cambios realizada.		0,00		

Fuente: Las autoras

Cuadro 4.34. Determinación de Salvaguardas – Suplantación de la identidad del usuario

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[A.5]	Suplantación de la identidad del usuario	$ 3899,56	• [D] datos/información • [S] servicios • [SW] aplicaciones (software)	• [C] Confidencialidad • [D] Disponibilidad • [A_S] Autenticidad del servicio • [A_D] Autenticidad de los datos

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Hacer conocer las políticas de seguridad de la empresa.	0,00	0,00
Capacitar al personal antes de contratarlo para que conozca cómo identificar esta amenaza.	0,00	
Las claves, deben ser única por cada usuario y caducar periódicamente para que se realice su cambio.	0,00	
No abrir mensajes de correo que pidan datos de la persona o de la institución donde trabaja.	0,00	

Fuente: Las autoras

Cuadro 4.35. Determinación de Salvaguardas – Abuso de privilegios de acceso

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[A.6]	Abuso de privilegios de acceso	$ 364,04	• [D] datos/información • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	• [C] Confidencialidad • [D] Disponibilidad • [A_S] Autenticidad del servicio • [A_D] Autenticidad de los datos

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Es importante crear un perfil de acuerdo a la función de cada usuario del sistema dando acceso únicamente a los datos que necesita conocer para desempeñar sus funciones.	0,00	0,00

Fuente: Las autoras

Cuadro 4.36. Determinación de Salvaguardas – Difusión de software dañino

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[A.8]	Difusión de software dañino	$ 973,33	• [SW] aplicaciones (software)	• [C] Confidencialidad • [D] Disponibilidad • [I] Integridad • [A_S] Autenticidad del servicio • [A_D] Autenticidad de los datos

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Todos los computadores y servidores deben contar con antivirus, evitar su propagación por la red**.**	0,00	$ 700
Mantener actualizado el sistema operativo y las aplicaciones que se utilizan en la institución.	$ 700	
Fomentar la cultura, de no participar en cadenas, y la instalación o abrir aplicaciones extrañas	0,00	

Fuente: Las autoras

Cuadro 4.37. Determinación de Salvaguardas – Acceso no autorizado

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[A.11]	Acceso no autorizado	$ 786,38	• [D] datos/información • [S] servicios • [HW] equipos informáticos (hardware) • [SW] aplicaciones (software) • [MEDIA] soporte de información • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar • [L] instalaciones	• [C] Confidencialidad • [I] Integridad • [A_S] Autenticidad del servicio

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Crear políticas de acceso al sistema, para que cada usuario según su perfil y su rol acceda a información necesaria para realizar su trabajo.	0,00	0,00
Monitorear las redes de datos del sistema para detectar usos de los recursos del software en horarios no autorizados para evitar daños.	0,00	

Fuente: Las autoras

Cuadro 4.38. Determinación de Salvaguardas – Destrucción de información

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[A.18]	Destrucción de información	$ 450,85	• [D] datos/información	• [D] Disponibilidad
Salvaguarda				
Tipo de salvaguarda		**Valor $**		**Costo Estimado**
Hacer respaldos diarios de la información en forma física y lógica**.**		0,00		$ 150
Limitar el acceso de los empleados al sistema según la función que desempeñan.		0,00		
Capacitar al personal para que hagan uso adecuado de la información que se hospeda en el sistema.		$ 150		

Fuente: Las autoras

Cuadro 4.39. Determinación de Salvaguardas – Manipulación de programas

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[A.22]	Manipulación de programas	$ 97,33	• [D] datos/información	• [C] confidencialidad • [I] Integridad • [A_S] Autenticidad del servicio • [A_D]Autenticidad de los datos • [T_D] Trazabilidad de los datos
Salvaguarda				
Tipo de salvaguarda		**Valor $**		**Costo Estimado**
Todas las aplicaciones o sistemas, deben contar con tareas de auditoria, con el fin de monitorear las acciones realizadas por cada uno de ellos y tomar medidas.		0,00		0,00

Fuente: Las autoras

Cuadro 4.40. Determinación de Salvaguardas – Manipulación de programas

Amenazas			**Activo**	
Código	**Amenaza**	**Valor Riesgo**	**Tipo activo a proteger**	**Dimensiones**
[A.25]	Robo	$ 9336,88	• [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [AUX] equipamiento auxiliar	• [C] Confidencialidad • [D] Disponibilidad

Salvaguarda		
Tipo de salvaguarda	**Valor $**	**Costo Estimado**
Instruir al personal, para que no libere información confidencial, ya sea de los empleados, socios o de la institución en general que pueda ser utilizada para cometer actos delictivos.	0,00	$ 7500
Respaldar sus activos de información, con la cobertura de seguros para la institución.	$ 5000	
Limitar el acceso a las instalaciones sensibles de la institución, para evitar que se sustraigan objetos.	0,00	
Utilizar cámaras de vigilancia que les permita identificar acciones sospechosas dentro de la institución.	$ 2500	

Fuente: Las autoras

El desarrollo de un análisis de riesgos tecnológicos en la cooperativa calceta sirvió para determinar el grado de exposición de eventos no deseados en la infraestructura de Tecnologías de Información, el cual como resultado global se determinó que tiene un riesgo medio, del cual se puede dar pautas para mitigar estos riesgos y proponer salvaguardas que ayuden a la toma de decisiones para reducir, aceptar o trasladar sus riesgos a fin de mantener su operatividad sin daños en los activos.

4.2. DISCUSIÓN

El análisis de riesgos de la infraestructura tecnología realizado en la cooperativa de ahorro y crédito Calceta limitada permitió conocer el valor real de los activos con los que cuenta la organización para realizar sus actividades, así mismo los riesgos a los que están expuestos, la susceptibilidad a ellos y el impacto que causaría en la institución en caso de materializarse, de igual manera permitió dar medidas preventivas y finalmente una propuesta de salvaguardas a la institución para brindar apoyo a la empresa y tener idea de cómo actuar ante un desastre precautelando lo más importante para la institución como lo es la información y los servicios que se brindan. Este tipo de trabajos han adquirido gran importancia dentro de la sociedad, pero antes no

se realizaban con frecuencia, por lo que era difícil encontrarlos disponibles en los repositorios de universidades y si habían eran limitados a áreas de negocio especificas enfocadas únicamente a los activos y no a los servicios que brindan las instituciones a las cuales se aplica.

Lo mencionado anteriormente se evidencia con el trabajo titulado: **ANÁLISIS DE RIESGOS PARA EL PROCESO ADMINISTRATIVO: DEPARTAMENTO DE INFORMÁTICA EN LA EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE PEREIRA S.A E.S.P, BASADOS EN LA NORMA ISO 27005**, se aplicó al hardware, software y servicios de la institución, con el fin de evidenciar las amenazas a las cuales están expuestas y las salvaguardas óptimas para la inmediata recuperación de las actividades de la empresa (Angarita *et al.,* 2012).

También la investigación titulada **PLAN DE CONTINGENCIA DE LOS EQUIPOS Y SISTEMAS INFORMÁTICOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN JUNÍN** realizada por estudiantes de la ESPAM MFL sirvió de referencia para las autoras en el desarrollo de la investigación para la organización del trabajo y los lineamientos a seguir en cuanto a la metodología aplicada (Palacios *et al*., 2013).

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Una vez terminado el trabajo realizado en la Cooperativa de Ahorro y Crédito Calceta Limitada se puede concluir que:

- Es necesario realizar un inventario de activos con sus valores económicos actualizados, ya que como todo bien material éstos van perdiendo valor económico, pero su funcionalidad es necesaria para el tratamiento de la información almacenada en ellos, la cual va adquiriendo a través del tiempo más valor para la institución.

- Realizando una identificación de las amenazas potenciales a las que están expuestos los activos se pueden determinar qué tan vulnerable al riesgo es la institución y tener una idea aproximada del impacto que tendrá en ella, para evitar la pérdida de los mismos.

- Es necesario tener una ruta que seguir ante las potenciales amenazas que puedan darse dentro de la institución para salvaguardar los recursos tecnológicos con los que cuenta para la realización de sus actividades.

- El uso de las salvaguardas establecidas para mitigar los riesgos es una herramienta que servirá de apoyo para los directivos de la institución en la toma de decisiones en caso de la materialización de las amenazas.

5.2. RECOMENDACIONES

- Evaluar constantemente el estado en el que se encuentran los activos de la institución, ya que éstos son los encargados de administrar un gran flujo de datos los cuales son la razón de ser de la institución y en caso de deterioro pueden representar grandes pérdidas dentro de la misma.

- Es primordial para la institución, determinar a tiempo los factores o elementos que pueden representarles peligro, con el fin de evitar daños o pérdida de los activos.

- Con el fin de asegurar una buena gestión al riesgo, es necesario tomar medidas preventivas invirtiendo cierta cantidad de dinero a tiempo para mitigar posibles fallas futuras que pueden resultar más costosas.

- De manera continua se debe actualizar periódicamente el análisis de riesgos para mantenerlo acorde a las necesidades de la institución, ya que todos estamos susceptibles a amenazas las que deben ser identificadas a tiempo para mitigar os riesgos y el impacto al que se está expuesto, siendo necesario la utilización de las salvaguardas más idóneas según sea el caso.

BIBLIOGRAFÍA

Abril, A; Pulido, J; Bohada, J. 2013. Análisis de riesgos en seguridad de la información. Tunja. Col. Revista Ciencia, Innovación y Tecnología. Vol. 1. p 43

Andrade, K; Jiménez, J; Valencia, O. 2013. Análisis para la detección de vulnerabilidades en la aplicación web Colibrí II. Aragua, VE. Revista de tecnología e información. Vol. 1. p 1-2.

Angarita, A y Tabares, C. 2012. Análisis de riesgos para el proceso administrativo: departamento de informática en la empresa de acueducto y alcantarillado de Pereira s.a e.s.p. Colombia. Formato PDF. Disponible en http://repositorio.utp.edu.co

Cooperativa de ahorro y crédito calceta limitada. 2014. Misión, visión, organigrama estructural. (En Línea). EC. Consultado, 03 de nov. 2014. Formato PDF. Disponible en http://www.coopcalcetaltda.fin.ec

Cobo, J. 2009. El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento. MEX. ZER. Vol. 14. p 312

Cordones, P y Piedra, M. 2011. Análisis de riesgos informáticos y elaboración de un plan de contingencia T.I para la empresa Eléctrica Quito S.A. (En Línea). EC. Consultado, 18 de ene. 2015. Formato PDF. Disponible en http://bibdigital.epn.edu.ec

Departamento Administrativo de la Función Pública. 2011. Guía para la administración de riesgos. (En Línea). COL. Consultado, 20 de ene. 2015. Formato PDF. Disponible en http://portal.dafp.gov.co

De la Fuente, H y Díaz, I. 2013. Análisis de los factores determinantes de la calidad percibida del servicio prestado por una cooperativa de ahorro y crédito: una aplicación basada en modelos de ecuaciones estructurales. CH. Revista Chilena de Ingeniería. Vol. 21. p 233.

Dirección General de Modernización Administrativa. 2012a. MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: libro I - Método. 3ed. España. NIPO. p 22-35

_____. 2012b. MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: libro II – Catalogo de elementos. 3ed. España. NIPO. p 19-56.

_____. 2012c. MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: libro III – Guía de Técnicas. 3ed. España. NIPO. p 19-56.

Espinoza, F. 2009. Importancia de las tecnologías de información en las organizaciones. COL. Revista de investigación académica sin fronteras. Vol. 1. p 1-116

Gaona, K. 2013. Aplicación de la metodología Magerit para el análisis y gestión de la seguridad de la información aplicado a la empresa pesquera e industrial bravito S.A en la ciudad de Machala. (En Línea). EC. Consultado, 16 de ene. 2015. Formato PDF. Disponible en http://dspace.ups.edu.ec

Gómez, R; Hernán, D; Donoso, Y; Herrera, A. 2010. Metodología y gobierno de la gestión de riesgos de tecnologías de la información. COL. Revista de Ingeniería. Vol. 31. P 110-111

Gómez, G. 2001. Los activos de la empresa y los recursos empresariales. (En Línea). COL. Consultado, 25 de may. 2015. Formato HTML. Disponible en http://www.gestiopolis.com

Gonzales, D; Martínez, A; Pérez, T; Zárate, J. 2010. Modelo de seguridad para la prevención de perdida de datos en las organizaciones. (En Línea). MEX. Consultado, 16 de ene. 2015. Formato PDF. Disponible en http://tesis.ipn.mx

Jiménez, L. 2008. Por qué necesitamos el Análisis de Riesgo en T.I. (En Línea). CR. Consultado, 13 de ener. 2014. Formato PDF. Disponible en http://ci.ucr.ac.cr

Marcotrigiano, L. 2011. Discusión del concepto de “activo” dentro del Actualidad Contable FACES. (En Línea). VEN. Consultado, 20 de Agosto. 2015. Formato PDF. Disponible en http://www.saber.ula.ve

Montesino, R; Baluja, W; Porvén, J. 2013. Gestión automatizada e integrada de controles de seguridad informática. La Habana, CUB. Revista de ingeniería electrónica automática y comunicaciones. Vol. 34. p 1-19

Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2014. Tecnologías de la información y comunicaciones para el desarrollo. (En Línea). EC. Consultado, 16 de may. 2015. Formato PDF. Disponible en http://www.industrias.ec

Meliá, J; García, J; Herrera J. 2010. Clasificación de las Amenazas a la Seguridad en Sistemas RFID-EPC Gen2. (En Línea). ES. Consultado, 25 de may. 2015. Formato PDF. Disponible en http://citeseerx.ist.psu.edu

Pandini, P y Pallero, M. 2013. Vulnerabilidades, amenazas y riesgo en “texto claro”. (En Línea). MEX. Consultado, 16 de ene. 2015. Formato HTML. Disponible en http://www.magazcitum.com.mx

Palacios, R; Quiroz, J; Buenaventura, J; Morales, J. 2013. Plan de contingencia de equipos y sistemas informático en el municipio de Junín. Tesis. Ing. Informática. ESPAM MFL. Calceta – Manabí, Ec. Pág. 129.

Pérez, M; Contreras Y; Amador, S. 2009. Características de los sistemas de información que permiten la gestión oportuna de la información y el conocimiento institucional. La Habana, CUB. ACIMED. Vol. 20. p 66-67

Ramírez, O. 2009. Riesgos de origen tecnológico: apuntes conceptuales para una definición, caracterización y reconocimiento de las perspectivas de estudio del riesgo tecnológico. Manizales, COL. Luna Azul. Vol. 29. p 1-2.

Revilla, A. 2012. Un modelo para la gestión de los recursos intangibles de tipo tecnológico. ¿Qué diferencia a los sectores intensivos en innovación? Madrid, ESP. Universia Business Review. Vol. 1. p 2

Rodríguez, I. 2015. ¿Qué es el riesgo, riesgo inherente y riesgo residual? (En Línea). Consultado, 16 de may. 2015. Formato HTML. Disponible en http://www.auditool.org

Suarez y Menéndez. 2011. Análisis y Gestión de Riesgo en Tecnología de la Información. (En Línea).AR. Consultado, 25 de may. 2015. Formato PDF. Disponible en http://www.suarez-menendez.com/

Ojeda, J; Rincón, F; Arias, M; Daza, L. 2010. Delitos informáticos y entorno jurídico vigente en Colombia. Bogotá, COL. Cuadernos de Contabilidad. Vol. 11. p 41-66.

Vásquez, R. 2010. Gestión integral de riesgos de tecnologías de información. (En Línea). MEX. Consultado, 25 de may. 2015. Formato PDF. Disponible en http://www.convencion-colac.com

Vergara, A. 2011. Análisis de las carteras de créditos orientados a la microempresa de los bancos privados del ecuador 2009-2010. (En Línea). EC. Consultado, 02 de nov. 2014. Formato PDF. Disponible en http://repositorio.ug.edu.ec

Villegas, M; Meza, M; León, P. 2011. Las métricas, elemento fundamental en la construcción de modelos de madurez de la seguridad informática. Zulia, VEN. Revista electrónica de estudios temáticos. Vol. 10. p 1-16

Voutssas, J. 2010. Preservación documental digital y seguridad informática. MEX. Investigación bibliotecológica. Vol. 24. p 129-132

ANEXOS

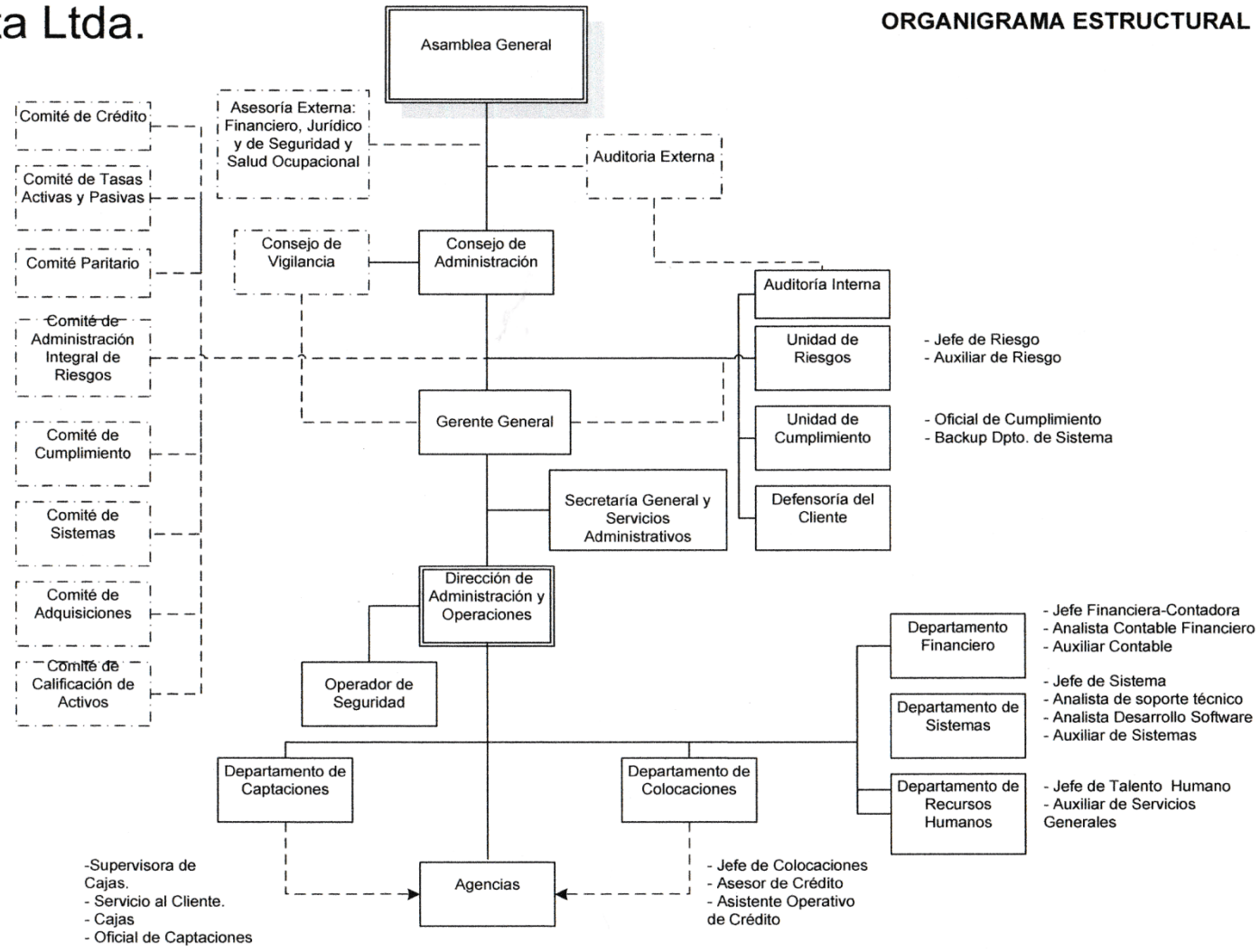
ANEXO 1

ORGANIGRAMA ESTRUCTURAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO CALCETA LIMITADA

COAC Calceta Ltda.

21/04/2015

ORGANIGRAMA ESTRUCTURAL



ANEXO 2

INVENTARIO DEL HARDWARE DE LOS ACTIVOS DE LA COOPERATIVA DE AHORRO Y CRÉDITO CALCETA LIMITADA

Estaciones de Trabajo											
Items	Detalle	Cantidad	Precio Unitario	Precio Total	Fecha de adquisición	Tiempo de uso (meses)	Depreciación anual	Depreciación mensual	Depreciación total	Valor actual del activo	Valor unitario del activo
1	Computador Intel Core I7-4770	1	1550,00	1550,00	feb-15	11	170,48	42,63	468,93	1081,07	1081,07
2	Computador Core I7-4770 3.40 GHZ	1	1550,00	1550,00	abr-15	9	170,48	42,64	383,76	1166,24	1166,24
3	Computador Core I7-3770 3.4 GHZ	1	1550,00	1550,00	ene-14	24	170,48	42,65	1023,60	526,40	526,40
4	Computador Intel Core I7-4770	1	1550,00	1550,00	feb-15	10	170,48	42,66	426,60	1123,40	1123,40
5	Computador Intel Pentium IV 2.66 GHZ	1	1200,00	1200,00	jun-06	114	170,48	33,00	3762,00	688,55	688,55
6	Computador Intel Pentium IV 3.0 GHZ	1	1200,00	1200,00	jul-06	113	170,48	33,00	3729,00	688,55	688,55
7	Computador Core I7-3770 3.40 GHZ	1	1550,00	1550,00	ene-14	24	170,48	42,66	1023,84	526,16	526,16
8	Computador Core I7-2600 3.40 GHZ	1	1400,00	1400,00	may-11	55	170,48	38,50	2117,50	888,55	888,55
9	Computador Intel Core I7-2600 3.4 GHZ	1	1550,00	1550,00	sep-12	39	170,48	42,66	1663,74	1038,55	1038,55
10	Computador Untel Core I7-2600 3.4 GHZ	1	1550,00	1550,00	sep-12	39	170,48	42,66	1663,74	1038,55	1038,55
11	Compuador Intel Pentium 4 3.00 GHZ	1	1200,00	1200,00	ene-06	108	170,48	33,00	3564,00	688,55	688,55
12	Computador Core 2 DUO E4500 2.2 GHZ	1	1200,00	1200,00	sep-08	87	170,48	33,00	2871,00	688,55	688,55
13	Computador Core I7-2600 3.40 GHZ	1	1400,00	1400,00	may-11	55	170,48	38,50	2117,50	888,55	888,55
14	Computador Core I7-2600 3.40 GHZ	1	1550,00	1550,00	oct-12	38	170,48	42,63	1619,94	1038,55	1038,55
15	Computador Intel Pentium D 3.00 GHZ	1	1200,00	1200,00	dic-08	84	170,48	33,00	2772,00	688,55	688,55
16	Computador Intel Pentium 3.00GHZ	1	1200,00	1200,00	feb-07	106	170,48	33,00	3498,00	688,55	688,55
17	Computador Intel Celeron 1.7 GHZ	1	1200,00	1200,00	feb-07	106	170,48	33,00	3498,00	688,55	688,55
18	Computador Intel Pentium D 1.6 GHZ E2140	1	1550,00	1550,00	oct-12	38	170,48	42,63	1619,94	1038,55	1038,55
19	Computador Intel Core I3 3.07 GHZ	1	1200,00	1200,00	ago-10	64	170,48	33,00	2112,00	688,55	688,55
20	Computador Intel Core I3 540 3.07 GHZ	1	1200,00	1200,00	ago-10	64	170,48	33,00	2112,00	688,55	688,55
21	Computador Intel Core I7 3770 3.4 GHZ	1	1550,00	1550,00	dic-12	36	170,48	42,63	1534,68	1038,55	1038,55
22	Computador Intel Core 2 QUAD Q8400 2.66 GHZ	1	1200,00	1200,00	jun-10	66	170,48	33,00	2178,00	688,55	688,55
23	Computador Intel Core I7 870 2.93 GHZ	1	1400,00	1400,00	dic-11	48	170,48	38,50	1848,00	888,55	888,55
24	Computador Intel Core2 DUO E7500 2.94 GHZ	1	1200,00	1200,00	oct-07	98	170,48	33,00	3234,00	688,55	688,55
25	Computador Core 2 QUAD Q8400 2.66 GHZ	1	1200,00	1200,00	jun-10	66	170,48	33,00	2178,00	688,55	688,55
26	Computador Core I7-3770 3.40 GHZ	1	1400,00	1400,00	dic-11	48	170,48	38,50	1848,00	888,55	888,55
27	Computador Intel Dual Core E2160 1.80 GHZ	1	1200,00	1200,00	dic-07	96	170,48	33,00	3168,00	688,55	688,55
28	Computador CoreE I7 - 2600 3.40 GHz	1	1400,00	1400,00	mar-11	57	170,48	38,50	2194,50	888,55	888,55
29	Computador Core I7-2600 3.40 GHZ	1	1400,00	1400,00	mar-11	57	170,48	38,50	2194,50	888,55	888,55
30	Computador Core I7-3770 3.4 GHZ	1	1550,00	1550,00	feb-14	22	170,48	42,63	937,86	612,14	612,14
31	Computador Core I7-870 2.93 GHZ	1	1550,00	1550,00	nov-12	37	170,48	42,63	1577,31	1038,55	1038,55
32	Computador Core 2 QUAD Q6600 2.4 GHZ	1	1200,00	1200,00	jun-10	66	170,48	33,00	2178,00	688,55	688,55
33	Computador Core I7-4770 3.40 GHZ	1	1550,00	1550,00	abr-15	8	170,48	42,63	341,04	1208,96	1208,96
34	Computador Core I7-870 2.93 GHZ	1	1550,00	1550,00	nov-12	13	170,48	42,63	554,19	995,81	995,81
35	Computador Core I7-870 2.93 GHZ	1	1550,00	1550,00	nov-12	13	170,48	42,63	554,19	995,81	995,81
36	Computador Pentium D 2160 1.70 GHZ	1	1200,00	1200,00	dic-08	84	170,48	33,00	2772,00	688,55	688,55
									total	30126,8711	

Anexo 2-A. Depreciación de Activos (Estaciones de Trabajo)

Servidores											
Items	Detalle	Cantidad	Precio Unitario	Precio Total	Fecha de adquisición	Meses en uso	Depreciación anual	Depreciacion mensual	Depreciacion total	Valor actual del activo	Valor unitario del activo
1	Servidor de Base de Datos y Aplicaciones 2 Intel Xeon DE 2GHZ	1	22500,00	22500,00	ago-13	28	7499,25	624,94	17498,25	5001,75	5001,75
2	Servidor de Base de Datos y Aplicaciones 2 Intel Xeon DE 2GHZ	1	22500,00	22500,00	ago-13	28	7499,25	624,94	17498,25	5001,75	5001,75
3	Servidor de Respaldo Xeon E3-1225 V3 3.10GHZ	1	2000,00	2000,00	jun-14	18	666,60	55,55	999,90	1000,10	1000,10
4	Servidor de Cajero Automático y Ahorro Movil Xeon E3-1225 V3 3.10GHZ	1	2000,00	2000,00	jun-14	18	666,60	55,55	999,90	1000,10	1000,10
5	Servidor Proxy Intel Xeon DE 2.4GHZ	1	2000,00	2000,00	ago-11	52	666,60	55,55	2888,60	0,20	0,20
6	Servidor de Riesgos 2 Intel Xeon de 3GHZ	1	2000,00	2000,00	dic-10	60	666,60	55,55	3333,00	0,20	0,20
7	Servidor Intel Xeon de 2.8GHZ	1	2000,00	2000,00	ene-07	108	666,60	55,55	5999,40	0,20	0,20
8	Servidor de Antivirus Intel Pentium de 3 GHZ	2	2000,00	2000,00	oct-08	86	666,60	55,55	4777,30	0,20	0,10
									TOTAL	12004,5	

Anexo 2-B. Depreciación de Activos (Servidores)

Equipos de comunicación											
Items	Detalle	Cantidad	Precio Unitario	Precio Total	Fecha de adquisición	Meses en uso	Depreciación anual	Depreciaclón mensual	Depreciación total	Valor actual del activo	Valor unitario del activo
1	Switch GbE2c Layer 2/3 Ethernet Blade	1	3200	3200	mar-13	33	1066,56	88,88	2933,04	266,96	266,96
2	Switch SG500-52	1	2500	2500	mar-14	21	833,25	69,4375	1458,1875	1041,8125	1041,8125
3	Switch SG500-52	1	3400	3400	abr-14	20	1133,22	94,435	1888,7	1511,3	1511,3
4	Central Telefonica KX-TES824	2	1200	2400	feb-08	94	799,92	66,66	6266,04	0,24	0,12
									TOTAL	2820,3125	

Anexo 2-C. Depreciación de Activos (Equipos de Comunicación)

Equipos de Impresión											
Items	Detalle	Cantidad	Precio Unitario	Precio Total	Fecha de adquisición	Meses en uso	Depreciación anual	Depreciación mensual	Depreciación total	Valor actual del activo	Valor unitario del activo
1	Impresora MG-2120	2	300	600	feb-14	22	199,98	16,67	366,63	233,37	116,69
2	Impresora ML-2010	3	800	2400	ene-14	24	799,92	66,66	1599,84	800,16	266,72
3	Impresora TX410	1	850	850	feb-14	22	283,31	23,61	519,39	330,61	330,61
4	Impresora MP-250	6	180	1080	sep-08	87	359,96	30,00	2609,74	0,11	0,02
5	Impresora MP-280	1	180	180	ene-07	108	59,99	5,00	539,95	0,02	0,02
6	Impresora FX-890	2	900	1800	nov-12	37	599,94	50,00	1849,82	0,18	0,00
7	Impresora TMU-950S	3	1000	3000	ene-14	24	999,90	83,33	1999,80	1000,20	333,40
8	Impresora ML-2165	1	250	250	feb-14	22	83,33	6,94	152,76	97,24	97,24
9	Impresora MP-230	2	150	300	dic-11	49	99,99	8,33	408,29	0,03	0,02
10	Impresora P361A	1	350	350	feb-07	106	116,66	9,72	1030,45	0,03	0,03
11	Impresora FX-890	1	900	900	feb-15	10	299,97	25,00	249,98	650,03	650,03
12	Impresora LX-355	1	750	750	feb-14	22	249,98	20,83	458,29	291,71	291,71
13	Impresora FX-890	1	900	900	feb-15	11	299,97	25,00	274,97	625,03	625,03
14	Impresora WC4118	1	3500	3500	ene-14	24	1166,55	97,21	2333,10	1166,90	1166,90
15	Copiadora Aficio MP301	1	3800	3800	feb-14	22	1266,54	105,55	2321,99	1478,01	1478,01
16	Copiadora Studio 2505	1	3800	3800	ago-10	64	1266,54	105,55	6754,88	0,38	0,38
17	Fax KX-FT981LA	1	3400	3400	ene-14	24	1133,22	94,44	2266,44	1133,56	1133,56
									TOTAL	25736,315	

Anexo 2-D. Depreciación de Activos (Equipos de impresión)

Computador Portatil											
Items	Detalle	Cantidad	Precio Unitario	Precio Total	Fecha de adquisición	Meses en uso	Depreciación anual	Depreciación mensual	Depreciación total	Valor actual del activo	Valor unitario del activo
1	PORTATIL PAVILON 2725LA, CAPACIDAD 160GB, RAM 4GB	1	950	950	sep-08	87	316,635	26,38625	2295,60375	0,095	0,095

Anexo 2-E. Depreciación de Activos (Computador Portátil)

Sistemas de Administración de Energía											
Items	Detalle	Cantidad	Precio Unitario	Precio Total	Fecha de adquisición	Meses en uso	Depreciación anual	Depreciación mensual	Depreciación total	Valor actual del activo	Valor unitario del activo
1	Ups Prestige 3000 20 KWA	1	15000	15000	mar-13	33	4999,5	416,625	13748,625	1251,375	1251,375

Anexo 2-F. Depreciación de Activos (Sistema de administración de energía)

Otros Activos de Hardware											
Items	Detalle	Cantidad	Precio Unitario	Precio Total	Fecha de adquisición	Meses en uso	Depreciación anual	Depreciación mensual	Depreciación total	Valor actual del activo	Valor unitario del activo
1	Cámara Digital DMC-LS80	1	600	600	ago-08	88	199,98	16,665	1466,52	0,06	0,06
2	Cámara IP de Seguridad STC-165	3	200	600	ago-08	88	199,98	16,665	1466,52	0,06	0,02
3	Lector de firmas D-LBK460-HSDR	1	450	450	ago-08	88	149,985	12,50	1099,89	0,05	0,05
4	Reloj biometrico de control de entrada y salida	1	350	350	feb-13	34	116,655	9,72	330,5225	19,48	19,48
5	Reloj biométrico de control de acceso	5	300	1500	feb-13	34	499,95	41,66	1416,525	83,47	16,70
									TOTAL	103,1175	

Anexo 2-G. Depreciación de Activos (Otros activos e hardware)

ANEXO 3

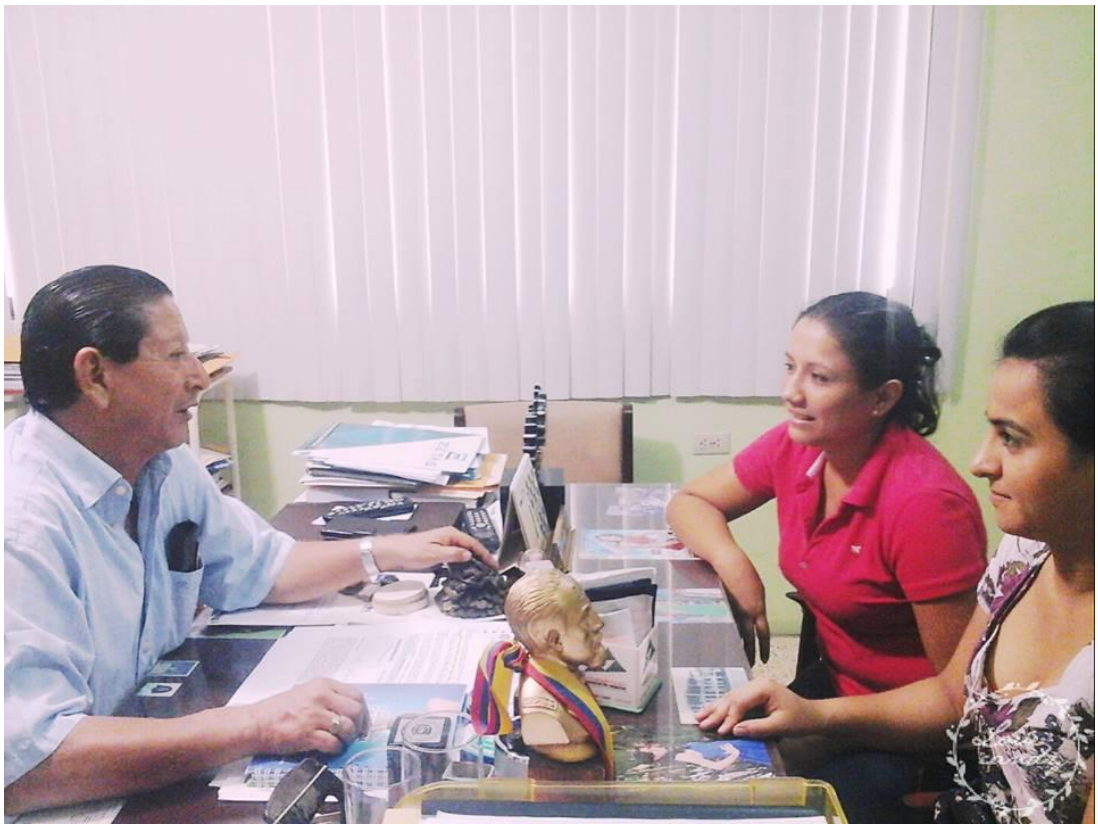
VALORACIÓN ECONÓMICA DE LAS SALVAGUARDAS

Código	Amenaza	Valor salvaguarda	Detalle
[I.2]	Daños por agua	$ 300	Por mantenimiento a las instalaciones de agua se estima un pago por hora de $15, trabajando 4 horas diaria por cinco días, esta salvaguarda se hace una vez al año
[I.3]	Contaminación mecánica	$1920	El mantenimiento de equipos se lo realiza 2 veces al año, teniendo la institución un total de 80 equipos pagando $12,00 por cada uno.
[I.5]	Avería de origen físico o lógico	$1920	El mantenimiento preventivo de equipos se lo realiza 2 veces al año, teniendo la institución un total de 80 equipos pagando $12,00 por cada uno.
[I.6]	Corte del suministro eléctrico	$ 750	El mantenimiento a la planta generadora se realizara tres veces al año, pagando por cada mantenimiento $250.
[I.6]	Corte del suministro eléctrico	$ 1500	La adquisición del sistema de UPS tiene un valor total de $ 1500
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	$ 4800	El mantenimiento de los equipos de climatización se realizara una vez al año, trabajando 4 horas diarias por tres días, pagando la institución por hora de trabajo $150
[I.8]	Fallo de servicios de comunicaciones	$ 3000	La implementación de enlace redundante se la realiza por un monto en total de $ 3000
[I.8]	Fallo de servicios de comunicaciones	$ 400	El mantenimiento a las redes de comunicación se las realiza una vez al año, trabajando 2 horas por 8 días, cancelando $50 la hora
[I.10]	Degradación de los soportes de almacenamiento de la información	$ 500	El respaldo se la puede realizar en discos duros extraíbles, cd y flash memory, estimando un costo de adquisición de los mismos de $500.
[E.1]	Errores de los usuarios	$ 500	Se capacitara a los usuarios 2 veces al año, el cual se cancelara a la persona un valor de $250 por capacitación.
[E.2]	Errores del administrador	$ 800	Se capacitara a los administradores de la institución dos veces al año, el cual se cancelara a la persona un valor de $400 por capacitación.
[E.8]	Difusión de software dañino	$2300	La adquisición del antivirus para implementar a los computadores de la institución tuvo un costo de $ 2300

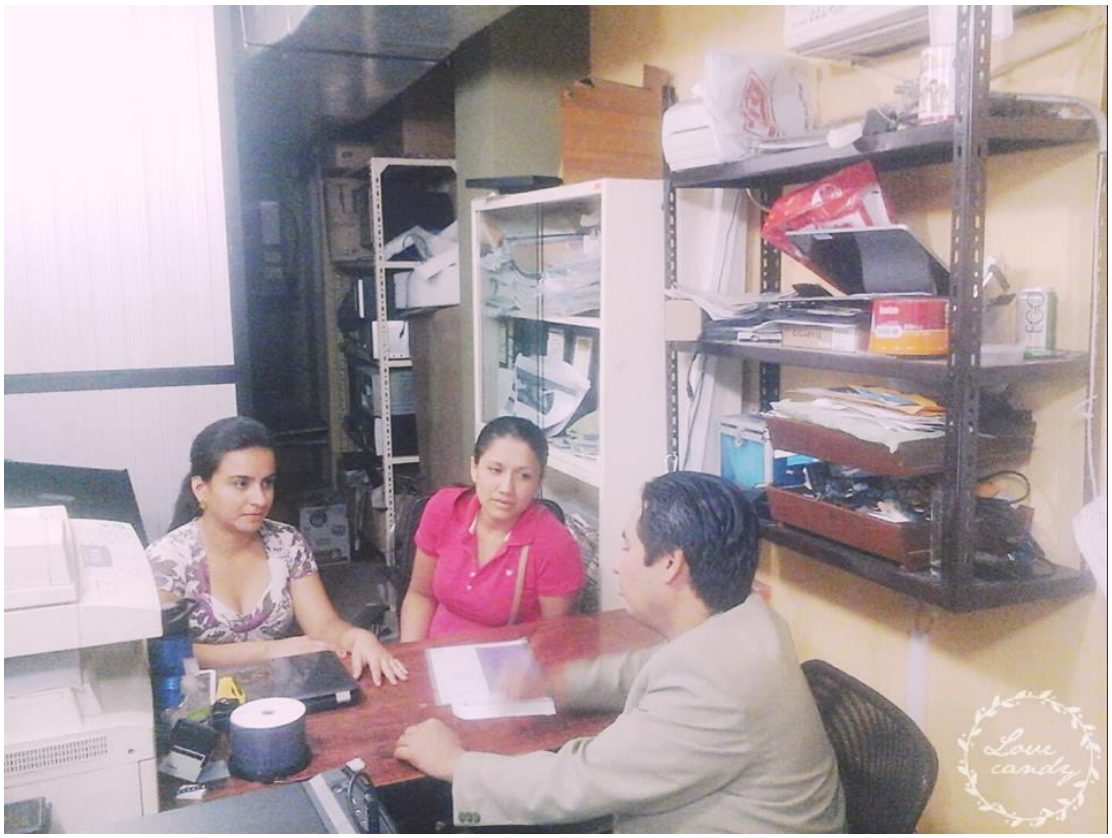
[E.9]	Errores de [re-]encaminamiento	$ 200	La capacitación a los usuarios se realizara una vez al año, el cual se cancelara a la persona un valor de $200.
[E.15]	Alteración accidental de la información	$ 300	La capacitación al personal se la realizara dos veces al año, el cual se cancelara a la persona un valor de $150 por capacitación.
[E.18]	Destrucción de información	$ 400	Se estima que el costo por adquisición de soportes de información es de $ 400
[E.19]	Fugas de información	$ 100	La capacitación al personal se la realizara una vez al año, el cual se cancelara a la persona un valor de $100.
[E.19]	Fugas de información	$ 600	Se estima que la adquisición de un sistema de perdida de información es de $ 600
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	$ 400	Para evitar la pérdida de datos, se debe realizar mantenimiento preventivo a los equipos por un costo de $ 400
[A.5]	Suplantación de la identidad del usuario	$ 50	La capacitación del personal antes de ser contratado se la realiza una hora por un valor de $ 50
[A.8]	Difusión de software dañino	$ 700	Se estima que el costo de actualización del software de la institución es de $700
[A.18]	Destrucción de información	$ 150	Se capacitara al 2 veces al año, pagando a la persona un valor de $150 por capacitación.
[A.22]	Manipulación de programas	$ 500	La auditoría a las aplicaciones la realiza la misma institución pero esta puede generar un cargo de $ 500 por el trabajo.
[A.25]	Robo	$ 100	Las capacitaciones al personal para que no libere información confidencial de la institución tiene un costo de $ 100
[A.25]	Robo	$ 5000	Se estima que la institución debe pagar por un seguro que ampare sus activos un valor de $5000 por año.
[A.25]	Robo	$ 2500	La implementación de cámaras en las instalaciones de la institución tienen un costo de $2500

ANEXO 4

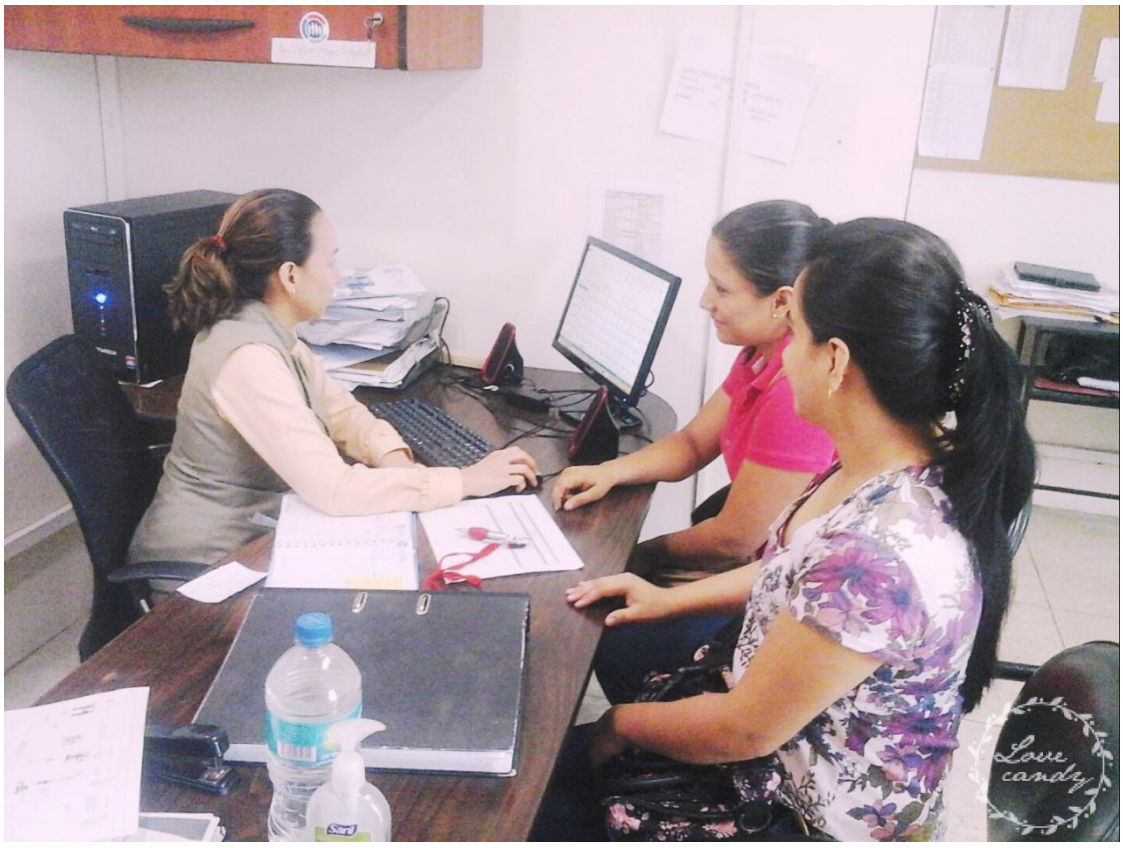
ACTIVIDADES REALIZADAS DENTRO DE LA COOPERATIVA DE AHORRO Y CRÉDITO CALCETA LIMITADA POR LAS AUTORAS



Anexo 3-A. Conversación con el Gerente de la Cooperativa Calceta Ltda.



Anexo 3-B. Conversación con el jefe del departamento Tecnológico de la Cooperativa Calceta Ltda.



Anexo 3-C. Conversación con la encargada del departamento de riesgo de la Cooperativa Calceta Ltda.

Anexo 3-D. Data Center de la Cooperativa Calceta Ltda.

ANEXO 5

DOCUMENTOS DE LA INSTITUCIÓN

COOPERATIVA
DE AHORRO Y CRÉDITO
CALCETA LTDA.

Desde 1966
CRECIENDO JUNTO A USTED

Oficio No.COAC-GG-2014-273

Calceta, 12 de noviembre de 2014

Señoritas
Gema Párraga Andrade, y
Mayra Dávila Muñoz
Ciudad

De mi consideración:

En atención a la solicitud presentada por ustedes, en la que requieren la autorización para realizar la tesis para terminación de su Carrera de Informática en la Escuela Superior Politécnica Agropecuaria de Manabí MFL, tengo el agrado de comunicar nuestra aceptación y por ende la autorización para que den inicio a los trabajos de investigación.

Atentamente,

COOPERATIVA DE AHORRO Y CRÉDITO "CALCETA LTDA."

Ing. Gustavo Navarrete Castillo
GERENTE GENERAL

jg

COOPERATIVA
DE AHORRO Y CRÉDITO
CALCETA LTDA.

Desde 1966
CRECIENDO JUNTO A USTED

Oficio No.COAC-GG-2015-294

Calceta, 05 de noviembre de 2015

Ingeniera
Jessica Morales Carrillo
DIRECTORA DE LA CARRERA INFORMATICA
ESCUELA SUPERIOR POLITECNICA AGROPECUARIA ESPAM MFL
Ciudad

De mi consideración:

Para los fines pertinentes me permito CERTIFICAR: Que las Señoras Mayra Alexandra Dávila Muñoz y Gema Vanessa Párraga Andrade, egresadas de la Carrera de Ingeniería Informática de la Escuela Superior Politécnica Agropecuaria de Manabí ESPAM MFL, realizaron el trabajo de campo para elaboración de su tesis, en mi representada, en el periodo de marzo a julio del 2015, tiempo durante el cual mostraron respeto, responsabilidad y sigilo en el manejo de la información, culminando con éxito el trabajo de tesis antes mencionado.

Es todo cuanto puedo certificar en honor a la verdad.

Atentamente,

Ing. Gustavo Navarrete C.
GERENTE GENERAL
jg