DISEÑO DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE TECNOLOGÍA DE LA CÁMARA DE COMERCIO DE CÚCUTA

MARIA CAROLINA DUARTE MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CÚCUTA
2019

DISEÑO DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE TECNOLOGÍA DE LA CÁMARA DE COMERCIO DE CÚCUTA

MARIA CAROLINA DUARTE MARTINEZ

Trabajo de grado presentado como requisito para optar al título de:

Especialista en Seguridad Informática

Msc. Katerine Marceles Villalba

Directora de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CÚCUTA

2019

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Ciudad y Fecha de entrega

DEDICATORIA

Dedico este proyecto de grado a mis maravillosos y amados padres, quienes siempre me han apoyado en todas las etapas de la vida. Soy muy afortunada de tenerlos como mis padres. A mis hermanos Edgar José, Cecilia Stella y Oscar David, quienes han sido los compañeros inseparables de la infancia y grandes amigos en la adultez, dispuestos siempre a escucharme y darme una mano. Sin el apoyo de mi familia no sería quien soy ahora. A mis grandes amigos, que me han comprendido y apoyado en la consecución de este nuevo logro. Y al universo por formar parte de él y ser consciente de todas las maravillas que me rodean.

AGRADECIMIENTOS

A la Cámara de Comercio de Cúcuta por brindarme la oportunidad de desarrollar este proyecto en sus instalaciones.

A los integrantes de la Dirección de Tecnología de la Cámara de Comercio de Cúcuta, por disponer de su tiempo para obtener la información necesaria para el desarrollo de este proyecto.

A la Ingeniera Marianela Olivares, Directora de Tecnología de la Cámara de Comercio de Cúcuta, por el apoyo brindado como líder del equipo en la orientación de este proyecto.

A la Ingeniera Katerine Marceles, Directora de proyecto en la UNAD, por el acompañamiento y su invaluable apoyo en el desarrollo de este proyecto.

A la Universidad Nacional Abierta y a Distancia por el apoyo brindado a través de los tutores de las diferentes asignaturas cursadas para obtener el título de Especialista en Seguridad Informática, pues gracias a la modalidad de estudio virtual es mucho más fácil poder acceder a una formación especializada. A mis compañeros de estudio, con quienes gracias al trabajo colaborativo pude desarrollar satisfactoriamente los contenidos de las asignaturas y tener un mejor aprendizaje.

CONTENIDO

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

El presente proyecto presenta el diseño de las Políticas de Seguridad de la Información para la Dirección de Tecnología de la Cámara de Comercio de Cúcuta, como respuesta a la necesidad de disminuir el impacto de las amenazas sobre los activos de información. Para llegar a estas políticas se hace inicialmente una evaluación del nivel de madurez de la Cámara de Comercio de Cúcuta con respecto a los controles de seguridad definidos por la ISO 27001:2013. Posteriormente se plantean una serie de fases de acuerdo a la metodología de análisis de riesgos seleccionada como la más adecuada de acuerdo a las características de la organización. Se realiza la identificación de los activos de información, se valoran en sus dimensiones de seguridad y se identifican los riesgos a los que están expuestos aplicando los criterios de valoración por probabilidad de impacto. Se definen las Políticas de Seguridad teniendo en cuenta el análisis previo realizado a la organización que contribuyan a minimizar las probabilidades de materialización de riesgos de seguridad de la información.

Palabras clave: Riesgos de seguridad, metodología de análisis de riesgos, ISO 27001, controles de seguridad, Políticas de Seguridad.

ABSTRACT

This project presents the design of the Information Security Policies for the Technology Department of the Cámara de Comercio de Cúcuta, in response to the need to reduce the impact of threats on information assets. To reach these policies, an evaluation of the maturity level of the Cámara de Comercio de Cúcuta is initially made with respect to the security controls defined by ISO 27001: 2013. Subsequently, a series of phases are proposed according to the risk analysis methodology selected as the most appropriate according to the characteristics of the organization. The identification of the information assets is carried out, they are valued in their security dimensions and the risks to which they are exposed are applied by applying the criteria of valuation by impact probability. The Security Policies are defined taking into account the previous analysis made to the organization that contribute to minimizing the probabilities of materialization of information security risks.

Keywords: Security risks, risk analysis methodology, ISO 27001, security controls, Security Policies.

INTRODUCCIÓN

En la actualidad las Cámaras de Comercio en Colombia, además de ser entidades gremiales privadas que cumple con la obligación legal de llevar los registros públicos, se han convertido en entidades de apoyo con programas y planes que propenden el mejoramiento de todas las actividades que incidan en el progreso socioeconómico de las regiones donde tienen su jurisdicción. Para alcanzar exitosamente todas sus metas y cumplir con sus obligaciones, la Entidad se apoya internamente en todas sus áreas misionales, operativas y de apoyo.

La Dirección de Tecnología es la unidad organizacional que apoya a la Cámara de Comercio de Cúcuta en la consecución de sus objetivos corporativos, implementando tecnologías de punta que sirvan de soporte a la operación diaria. La implementación de toda esta infraestructura tecnológica, que trae muchos beneficios y mejoras en la prestación de servicios a los usuarios, también implica la posibilidad de que se materialicen riesgos de seguridad al no contar con los controles y mecanismos que permitan garantizar la continuidad del servicio.

Es por esta razón que se propone realizar un diagnóstico preliminar donde se pueda detectar el grado de madurez que tiene la Cámara de Comercio de Cúcuta con respecto a los controles que se deben tener implementados al interior de la Entidad, con el fin de garantizar la integridad, disponibilidad y confidencialidad de la información.

Identificado el nivel de madurez, se procederá a identificar los activos de información críticos para la Dirección de Tecnología, que es el área encargada de administrar toda la plataforma tecnológica y eje central de este proyecto. Identificados los activos, se procede a valorarlos en términos de confidencialidad integridad y disponibilidad, con el fin de poder de esta manera realizar un análisis de riesgos y determinar cuáles son aquellos a los que se encuentran expuestos los activos.

Lo que se busca es llegar al diseño de unas políticas de seguridad de la información para la Dirección de Tecnología que se encuentren alineadas a sus necesidades y de esta manera disminuir el impacto en los activos frente a alguna amenaza.

1. GENERALIDADES DEL PROYECTO

1.1 PLANTEAMIENTO DEL PROBLEMA

La Unidad de Tecnología de la Cámara de Comercio de Cúcuta, como responsable de los procesos de gestión y administración de los recursos informáticos de la Entidad, ha implementado a lo largo de los años diversos controles de seguridad con el fin de poder garantizar un nivel de seguridad confiable en el desarrollo de la operación, que es soportada en los sistemas de información y las plataformas informáticas. Estos controles se han configurado para evitar la materialización de los riesgos de seguridad que son más comunes en el contexto en el que se encuentra la Entidad y han demostrado una efectividad a lo largo del tiempo.

Sin embargo, a pesar de que existen controles informáticos implementados, estos no han sido por el resultado de la identificación de éstos mediante la realización de un análisis de riesgos que le permita a la Entidad conocer cuáles son sus activos de información y determinar para cada uno de ellos los riesgos a los que están expuestos y el impacto que tendría para la Entidad la materialización de estos riesgos.

El no tener identificados claramente cuáles son los activos de información y establecido el impacto en el caso de que se materialice un riesgo de seguridad, se hace mucho más difícil la toma de decisiones en el momento de tener que invertir en controles que por su naturaleza pueden requerir una inversión económica alta. Esto ha ocasionado que en varias ocasiones se postergue la compra de soluciones que podrían beneficiar la seguridad de la información, pues no se puede demostrar a la Presidencia y Junta Directiva el impacto negativo en el caso de no realizarse. Es por esta razón que algunos de los sistemas de información que son administrados por el área de Tecnología de la Cámara de Comercio no cuentan con las últimas versiones disponibles, la red de datos tiene dispositivos de marcas que ya no se encuentran en el mercado y los dispositivos móviles no cuentan con una gestión claramente establecida sobre su finalidad de uso y seguridad de la información que allí se almacena.

Por último, esta falta de un análisis detallado a nivel de seguridad de la información ha llevado que se adopte un modelo de Política de Seguridad de la Información planteado por Confecámaras, quien en su momento envía este documento para revisión y adopción por parte de las Cámaras de Comercio del país. La Cámara de Comercio de Cúcuta adopta este documento y lo formaliza, pero que a la fecha no ha sido revisada y adaptada a las necesidades de la

Cámara de Comercio, ni tampoco existen unas políticas de seguridad de la información específicas para el área de Tecnología, que es el área que vela por la disponibilidad, integridad y confidencialidad de los sistemas informáticos de la Entidad.

1.2 FORMULACION DEL PROBLEMA

¿Es necesaria la definición de unas Políticas de Seguridad de la Información alineadas a las necesidades de la Unidad de Tecnología de la Cámara de Comercio de Cúcuta para disminuir el impacto de los activos frente alguna amenaza?

1.3 JUSTIFICACION

El diseño de las Políticas de Seguridad de la Información para la Unidad de Tecnología de la Cámara de Comercio de Cúcuta permitirá que la información sea valorada desde el punto de vista de la seguridad y de acuerdo a esto determinar los controles y mecanismos de protección adecuados que ayuden a minimizar los riesgos asociados a la administración de la plataforma tecnológica que soporta la operación de la Entidad.

Se realizará una evaluación de los controles que comprende la ISO/IEC 27001:2013 a la Unidad de Tecnología, para obtener un diagnóstico de la efectividad de las medidas de seguridad implementadas por la Cámara de Comercio de Cúcuta hasta el momento. Este documento le permitirá a la Entidad conocer el estado actual de la seguridad de la información.

La realización del análisis de riesgos dará a conocer a la Unidad de Tecnología cuales son sus activos de información y de esta manera contar con un inventario y poder sobre ellos aplicar los controles necesarios. Así mismo se brindará una herramienta que de forma sistemática le permita conocer los riesgos a los que están expuestos los activos de información y el impacto en el caso de que se llegaran a materializar.

Teniendo identificados los riesgos a los que están expuestos los activos de información será mucho más eficiente la toma de decisiones sobre la implementación de mecanismos de seguridad que se requieran implementar alineados a las políticas de seguridad atendiendo a las necesidades de la Unidad de Tecnología.

1.4 ALCANCE Y DELIMITACION DEL PROYECTO

El presente proyecto tiene como alcance el planteamiento de las Políticas de Seguridad de la Información para la Unidad de Tecnología de la Cámara de Comercio de Cúcuta, definidas con base a la realización de un análisis de riesgos a los activos de información.

1.5 OBJETIVOS

1.5.1 Objetivo general. Diseñar las políticas de seguridad de la información aplicables a la Unidad de Tecnología de la Cámara de Comercio de Cúcuta.

1.5.2 Objetivos específicos. Evaluar la seguridad de la información teniendo en cuenta los distintos controles que tiene la ISO 27001:2013 para que sirva como un componente de planificación para la implementación de medidas de seguridad de la información en la cámara de comercio de Cúcuta.

Identificar los activos de información críticos para la Unidad de Tecnología de la Cámara de Comercio de Cúcuta, aplicando los criterios de valoración en términos de confidencialidad integridad y disponibilidad.

Determinar los riesgos que afectan la seguridad de la información en los activos críticos de la Unidad de Tecnología de la Cámara de Comercio de Cúcuta, aplicando los criterios de valoración de probabilidad por impacto.

Estructurar las políticas de seguridad de la información aplicables para la Unidad de Tecnología de la Cámara de Comercio de Cúcuta.

2. MARCO TEORICO

2.1 ANTECEDENTES

Para el desarrollo de este proyecto se tomaron como referencia trabajos similares relacionados con el análisis y gestión de riesgos de Seguridad de la Información y su aplicación para la mejora de los procesos al interior de las organizaciones en cuanto a la seguridad de la información.

Proyecto “Análisis de los riesgos de Seguridad de la Información de un aplicativo de gestión documental líder en el mercado colombiano”, trabajo de grado presentado por Carmen Elizabeth Fajardo Díaz a la Institución Universitaria Politécnico Grancolombiano en el año 2017 para optar al título de Especialista en Seguridad de la Información[1]. En este proyecto se aplica una metodología de análisis de riesgos al aplicativo de gestión documental, permitiendo identificar las deficiencias y vulnerabilidades a nivel de seguridad de la Información para brindar a la organización un plan de tratamiento de riesgos para el mejoramiento del aplicativo. Los aplicativos de gestión documental son utilizados por la Cámara de Comercio de Cúcuta desde el año 2004, y sirve de referencia este análisis para el realizado en el presente proyecto.

Proyecto “Análisis y evaluación de riesgos de Seguridad Informática para la Cámara de Comercio de la Dorada, Puerto Boyacá, Puerto Salgar y municipios de Oriente de Caldas” presentado por José Nayid Cardona Castañeda y Willis Alberto Salcedo Ruiz a la Universidad Nacional Abierta y a Distancia en el año 2017 para optar al título de Especialistas en Seguridad Informática. Este proyecto al ser aplicado en una Cámara de Comercio en Colombia permite tener una visión de un contexto similar al del presente proyecto en aspectos tales como legales, organizacionales y procedimentales. La aplicación de una metodología para identificar los riesgos a los que se encuentra expuesta la Cámara de Comercio de la Dorada, Puerto Boyacá, Puerto Salgar y municipios de Oriente de Caldas a nivel de seguridad informática orienta esta misma actividad a ser aplicada en la Cámara de Comercio de Cúcuta.[2]

[1] FAJARDO, Carmen Elizabeth. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano. Trabajo de grado. Bogota: Instituto Universitaria Politecnico Gran Colombiano, Facultad de Ingenierias, Departamento de Seguridad, 2017. 73 p.

[2] CARDONA, Jose Nayid y SALCEDO Willis Alberto. Análisis y evaluación de riesgos de seguridad informática Para la cámara de comercio de la dorada, puerto boyacá, puerto salgar y municipios de

Proyecto “Guía de Auditoria basada en el Análisis de Riesgos a un Centro de Datos aplicando la metodología Magerit 3” presentado por Jair Hernando Vanegas Garzón a la Universidad Católica de Colombia en el año 2017 para optar al título de Especialista en Auditoría de Sistemas de Información. En este proyecto se elabora una guía de auditoría para evaluar los controles implementados para mitigar los riesgos asociados a las tecnologías de la información en un centro de datos, basada en la metodología de análisis de riesgos Magerit, encontrando un uso especial a este tipo de metodologías para mejorar los procesos al interior de una organización, como es en este caso en la creación de una guía de auditorías.[3] Las fases de desarrollo del proyecto aplicando la metodología de análisis de riesgos constituyen una guía para armar la estructura del presente proyecto.

Proyecto “Diseño de un SGSI basado en la norma ISO 27001 para la empresa MA Peñalosa cía. S.A.S. sede principal Cúcuta” presentado por Johanna Carolina Ararat Muñoz a la Universidad Nacional Abierta y a Distancia en el año 2018 para optar al título de Especialista en Seguridad Informática[4]. Este proyecto plantea la importancia que tiene, para la organización donde fue aplicado, la seguridad de la información que considera una prioridad. Se evalúa la situación actual de seguridad de la información y se presenta una propuesta que servirá de apoyo a la organización para la implementación de un Sistema de Gestión de Seguridad de la Información. Aplica la metodología Magerit para la creación del inventario de activos informáticos y el análisis de riesgos a los que están expuestos. Al ser una organización ubicada en el mismo contexto geográfico al del presente proyecto sirve de referencia en cuanto a la naturaleza de las amenazas del entorno que pueden afectar a la seguridad de la información.

2.2 MARCO CONCEPTUAL

2.2.1 Sistemas de gestión de seguridad de la información. Un sistema de gestión de seguridad de la información, abreviado como SGSI, es un grupo de políticas y procedimientos que permiten organizar y administrar de manera sistemática los datos sensibles de una organización, el principal objetivo de este sistema es minimizar el riesgo y asegurar la continuidad del negocio, limitando el riesgo que puedan tener las brechas de seguridad, de una manera proactiva.

---

oriente de caldas. Tesis de grado. Universidad Nacional Abierta, Facultad de Ciencias Basicas, Departamento de Seguridad, 2017. 176 p.

[3] VANEGAS, Fair Hernando. Guia de auditoria basada en el análisis de riesgos a un centro de datos aplicando la metodologia Magerit 3. Tesis de grado. Universidad Católica de Colombia, Facultad de Ingeniería, programa de especialista en sistemas, 2017. 168 p.

[4] ARARAT MUÑOZ, Johanna Carolina. Diseño de un sgsi basado en la norma iso 27001 para la empresa ma Peñalosa Cía. S.A.S. sede principal Cúcuta. Tesis de grado. Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería, Programa de Especialización de Seguridad Informática,2018. 153 p.

Usualmente un SGSI regula y orienta el comportamiento de los empleados, los procesos, los datos y la tecnología. Puede implementarse para enfocarse en un elemento particular como, por ejemplo, los datos de los clientes, o puede implementarse de manera más general para que forme parte de la cultura organizacional del ente[5]. Esto requiere que se haga una apropiada identificación de activos y una correcta evaluación de los mismos en base a su confidencialidad, integridad y disponibilidad. Existen especificaciones que orientan la creación de un SGSI, por ejemplo, la ISO 27001 de la que se hablará más adelante, estas especificaciones usualmente no obligan a tomar acciones específicas, pero si incluyen sugerencias para documentación, auditorias, mejora continua y acciones correctivas y preventivas.[6]

2.2.2 Seguridad de la información e informática. Se define como seguridad de la información[7] a un conjunto de estrategias para crear e implementar procesos, herramientas y políticas orientadas a prevenir, detectar, documentar y cuantificar amenazas sobre la información digital y no digital de una organización. La seguridad de la información se construye alrededor de 3 objetivos claves, mantener la confidencialidad, integridad y disponibilidad de los datos del negocio (CIA por sus siglas en inglés). Estos objetivos deben asegurar que la información sensible sólo será mostrada a los actores autorizados (confidencialidad), prevenir la modificación no autorizada de los datos (integridad) y garantizar que los datos pueden ser accedidos por los autores autorizados cuando estos lo requieran (disponibilidad).

No debe confundirse el concepto de seguridad de la información con el de seguridad informática, la seguridad de la información se refiere a todos los ámbitos donde se gestione la información mientras que la seguridad informática se refiere solo al manejo de la información en el medio informático.

Por tanto, la seguridad informática es un conjunto de procesos para prevenir y detectar usos no autorizados de un sistema informático, esto incluye la protección contra daños (intencionales o no), robos o hurto del hardware o software, así como protección contra la interrupción de los servicios que estos elementos proveen. Entran en los alcances de esta definición los procesos de control de acceso físico

[5] ISO 27000.ES. El portal de ISO 27001 en Español. (En línea) (Citado el 16 de Mayo del 2018). Disponible en: http://www.iso27000.es/iso27000.html

[6] ROUSE, Margaret. information security management system (ISMS). (En línea) (Citado el 14 de Julio del 2018). Disponible en: https://whatis.techtarget.com/definition/information-security-management-system-ISMS

[7] ESTÁNDAR INTERNACIONAL ISO/IEC 17779. Tecnología de la información - Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información [en línea]. (citado s.n., 2011). Disponible en: https://mmujica.files.wordpress.com/2007/07/iso17799-2005-castellano.pdf

al hardware, la protección de amenazas que puedan ingresar vía red e incluso las debidas a malas prácticas de un operador, sean accidentales o no y que pudiesen afectar la seguridad de la información. [8]

2.2.3 Metodología de análisis de riesgos. La metodología de análisis de riesgos es un marco de trabajo que define la forma en que se analizan y evalúan los riesgos que están presentes en el ámbito computacional y de información en una organización. Esto representa un verdadero reto para los profesionales de tecnologías de la información debido a los rápidos cambios en la tecnología y a la realidad de que evaluar riesgos es una tarea difícil. Por ello, estos marcos de trabajo no se enfocan en plantear directivas, sino que sugieren métodos que permiten orientar el análisis y tabularlo en función de su importancia específica para ese negocio en particular, evaluándolo cualitativa y cuantitativamente, identificando activos y sus vulnerabilidades y asignando una importancia a cada uno de esos aspectos, para luego estimar la forma de prevenirlos o mitigarlos. Todo ello con la debida documentación, de tal forma de que múltiples actores de la organización puedan colaborar en el análisis.

Existen, una gran variedad de metodologías de análisis de riesgo, dependiendo del tipo de negocio, la cantidad de activos, si es pertinente o no hacer valoraciones cualitativas o cuantitativas, si es necesario generar políticas o solo evaluar los riesgos, si el análisis se va a realizar por un ente externo o por elementos de la misma organización con conocimiento de los procesos, etc. Más adelante en este documento se verán las características de las metodologías más utilizadas, sus ventajas y desventajas, y las diferencias entre ellas.

2.2.4 Serie de normas ISO/IEC 27000. Son una serie de normas publicadas por la *International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC*) las cuales proporcionan un conjunto de recomendaciones y lineamientos para el manejo de la seguridad de la información. Son similares en su diseño a las normas de otros sistemas de gestión como el de aseguramiento de calidad (la serie ISO 9000) y las normas de protección ambiental (serie ISO 14000). Esta serie de normas incluye un conjunto de guías y documentos organizados según la oficina internacional de estandarización con rangos de numeración reservados que van de 27000 a 27019 y de 27030 a 27044.

[8] BUENAS TAREAS. Guía de estudios ETS seguridad informática. (En línea) (Citado el 16 de Mayo del 2019). Disponible en: http://www.buenastareas.com/ensayos/Horario-Voca-8-Segundo-Semestre/1513007.html

Siendo los más importantes la ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002 y la ISO/IEC 27003.[9]

2.2.5 Norma ISO/IEC 27000. Brinda una visión completa de las normas que incluyen la serie, detallando su alcance y propósito. Da además justificación para comprender porque es necesaria la implementación de un SGSI, una breve descripción de los pasos para su implementación, monitorización, mantenimiento y mejora. Constituye la introducción necesaria para que todos los elementos de la organización involucrados, entiendan la importancia de estas normas. Fue publicada en su primera versión en mayo de 2009 y actualmente está vigente su cuarta revisión que data de febrero de 2016.

2.2.6 Norma ISO/IEC 27001. Es la norma principal de la serie, contiene un detalle de los principales requisitos con que debe contar un sistema de gestión de seguridad de la información, organizados de una manera formal, estructurada y concisa. Cabe resaltar que la ISO/IEC 27001 establece requisitos, si una organización quiere certificar su sistema de gestión de seguridad de la información debe cumplir por completo todos los requisitos que se expresan en la norma. La revisión más reciente de esta norma fue publicada en 2015 y ahora su nombre completo es ISO/IEC 27001:2015. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

2.2.7 Norma ISO/IEC 27002. Constituye una guía de buenas prácticas y describe más en detalle los objetivos de control y los controles recomendables orientado a seguridad de la información. Dentro de 11 dominios se agrupan 39 objetivos de control y 133 controles. Ésta no es certificable, por lo tanto, no es obligatoria, aunque las organizaciones pueden usarla como guía para implementar los requerimientos de la ISO/IEC 27001. La ISO/EIC 27001 establece que se debe hacer, pero no cómo, la ISO/EIC 27002 da una guía de cómo hacerlo, considerando que su implementación depende del contexto de la organización. Fue publicada inicialmente en julio de 2007 sustituyendo a la guía anterior, llamada ISO 17799:2005.

2.2.8 Norma ISO/IEC 27003. Esta norma es una guía de implementación para los sistemas de gestión de seguridad de la información. Detalla todo el proceso desde la concepción hasta la puesta en marcha de un SGSI, enfocándose principalmente en los aspectos más importantes de estas tareas. Fue liberada inicialmente en

[9] Ibid., p. 2

febrero de 2010 y la versión actual data de abril de 2017. Por considerarse una guía, no es certificable.[10]

2.2.9 Serie de normas ISO/IEC 27000 en Colombia. En Colombia la entidad que emite la certificación ISO/IEC 27001 es ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación). Esta institución es también la encargada de realizar las auditorias de seguimiento, reactivaciones y renovaciones de los certificados. En cuanto a las estadísticas de certificación, según el informe emitido por ISO[11] el número de certificados ISO/IEC 27001 mantenidos a nivel mundial a fines del 2017 asciende a 39.501, observándose un crecimiento del 20% desde el año 2014. Japón es el país que más certificados emitidos posee con 9.161. En América Latina México lidera la región con 315 certificados emitidos, seguido de Brasil con 170 y Colombia en un tercer lugar con 148, siendo, de los 29 países con certificaciones que integran la región de centro y sur América, el que acumuló hasta 2017 casi un cuarto de todos los certificados activos (23.87%), muy por delante del cuarto de la lista, Chile, con 64 certificados.

Una posible manera de comprender la cultura de la certificación de las empresas en Colombia es revisar los números de certificaciones de una de las normas más populares, la ISO 9001. Colombia ocupa en la certificación de la norma el segundo lugar de la región con 11471 luego de Brasil con 17165 y por delante de México que tiene 7184 lo cual muestra que las empresas colombianas han estado atentas a la importancia de las certificaciones y aunque no pareciera haber una marcada tendencia de las organizaciones a certificarse en seguridad de la información, se observa una tendencia creciente en las solicitudes para esta norma.[12]

2.3 MARCO LEGAL

Con referencia a los sistemas informáticos, existen leyes en Colombia que hacen referencia a la seguridad de la información y sistemas informáticos, entre las cuales las siguientes rigen a las Cámaras de Comercio del país:

Ley 1273 de 2009. **Ley de delitos informáticos en Colombia.** Se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los

[10] Op. cit., p. 2
[11] ISO/IEC 27001. Information Technology - Security Techniques - Information Security Management Systems–Requirements. 2018 [En línea]. (Citado el 24 de mayo del 2018). Disponible en https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1
[12] Ibid., p. 1

datos"[13] y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Con esta ley en Colombia se establecen castigos para aquellos que incurran en delitos que atenten contra la seguridad de los sistemas informáticos.

Ley 1581 de 2012. Ley de protección de datos personales. Constituye el marco general de la protección de los datos personales en Colombia. Tiene por objeto "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma."[14] Las entidades como las Cámaras de Comercio deben tener establecida una Política de protección de datos personales para dar cumplimiento a esta ley. La Cámara de Comercio de Cúcuta define un manual de políticas y procedimientos de protección de datos personales bajo esta reglamentación.[15]

Decreto 1377 de 2013. Con este decreto se busca facilitar la implementación de la Ley 1581 de 2012**.** Este decreto reglamenta aspectos relacionados con titular de la información, las políticas de tratamiento de datos personales de los responsables y encargados, la transferencia, transmisión y la responsabilidad demostrada frente al tratamiento de datos personales. Define la relación contractual entre el responsable y el encargado del tratamiento de los datos personales. Regula la manera de obtener la autorización del tratamiento de datos personales, entre otros aspectos que permiten el cumplimiento de la ley 1521 de 2012.[16]

Ley 527 de 1999. Ley de comercio electrónico. Con esta ley se reglamenta el uso de mensajes de datos para todas las organizaciones privadas o públicas, indicando que no se negarán efectos jurídicos, validez o fuerza obligatoria por el

[13] COLOMBIA. CONGRESO DE LA REPUBLICA. ley 1273 de 2009.(enero 5). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado. Diario Oficial. Bogota: El Congreso, 2009. 2 p.

[14] COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. DECRETO NÚMERO 1317 DE 2013. "Por el cual se reglamenta parcialmente la Ley 1581 de 2012" Bogota: El Ministerio, 2013. 2 p.

[15]MARRUGO,RIVERA & ASOCIADOS. Manual de políticas y procedimientos de protección de datos personales. (En línea) (Citado el 16 de Octubre del 2016). Disponible en: http://www.cccucuta.org.co/media/habeas_data/manual_de_politicas_y_procedimientos_de_proteccion_de_datos_personales.pdf

[16] Op. cit., p. 2

hecho de que los datos estén en formato electrónico.[17] Con esta ley se define el concepto de firma digital, comercio electrónico, entidades de certificación e intercambio electrónico de datos. Su importancia radica en el hecho de que otorga la misma validez a los datos en medios físicos como a los que se encuentran en medios electrónicos.

Ley 1712 de 2014. Ley de Transparencia y del Derecho de acceso a la Información pública. Reglamenta el derecho que tienen todas las personas a conocer la existencia de información pública que se encuentre bajo control de cualquier institución. Las Cámaras de Comercio prestan la función pública de llevar los registros de comercio, siendo ante la ley sujetos obligados a suministrar este tipo de datos.

Ley 1341 de 2009. Ley sobre la sociedad de la información y la organización de las Tecnologías de la información y las comunicaciones. Con esta ley el Estado colombiano determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones. Entre los principios orientadores está la masificación del Gobierno en línea, que busca que la prestación de servicios a los ciudadanos se haga de forma eficiente, debiendo adoptar las entidades públicas todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones en el desarrollo de sus funciones. Las Cámaras de Comercio del país prestan la función pública de llevar los registros de comercio, y participan activamente en proyectos liderados por el Ministerio de Tecnologías de la Información y las Comunicaciones para facilitar a los empresarios el acceso a las tecnologías de Información, como los Centros de Transformación Digital Empresarial CTDE."[18]

Ley 1266 de 2008. Habeas Data. Ley que regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.[19] La Cámara de Comercio de Cúcuta en el ejercicio de la función pública delegada por el gobierno maneja datos públicos, y a la vez trata datos personales que no son de naturaleza

[17]COLOMBIA. CONGRESO DE LA REPUBLICA. ley 527 de 1999 (agosto 18). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Diario Oficial. Bogota: El Congreso, 1999. 21 p.

[18] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley .1341 (30 de Julio 2009). por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de lastecnologías de la información y las comunicaciones. Bogota: El Congreso, 2009. 21 p.

[19] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley estatutaria 1266 de 2008 (diciembre 31). por la cual se dictan las disposiciones generales del hábeas data. Bogota: El Congreso, 2008. 24 p.

pública, con el fin de llevar a cabo el desarrollo de sus funciones de carácter privado.[20]

2.4 MARCO CONTEXTUAL

2.4.1 Reseña histórica. La Cámara de Comercio de Cúcuta fue fundada el 25 de noviembre de 1915 cuando el Gobierno nacional expidió el decreto 1807 de 1915, mediante el cual se ordenó la creación de las Cámaras de Comercio de Cúcuta, Cartagena, Cali y Bucaramanga, como entidades sin ánimo de lucro.

En esa época a la Cámara de Comercio de Cúcuta se le delegaron algunas funciones entre las que se encuentran servir de órgano oficial del comercio y el empresariado ante el Gobierno Nacional, presentando iniciativas de desarrollo regional. Fue a partir del año 1931 que se delegó a la Cámara de Comercio de Cúcuta la función de llevar el registro mercantil de su jurisdicción.

Actualmente la Cámara de Comercio de Cúcuta cumple con la obligación legal de llevar los registros públicos, promover el desarrollo regional y de ser vocera del sector privado ante el Gobierno Nacional como gestora de proyectos y programas de beneficio para el empresariado y la comunidad de la región[21].

Existen 5 oficinas distribuidas en el área metropolitana de Cúcuta y el Municipio de Tibú:

- Oficina Principal, en la ciudad de Cúcuta.
- Centro de Atención Avenida Cero, en la Ciudad de Cúcuta.
- Centro de Atención Los Patios, en el Municipio de Los Patios.
- Centro de Atención Villa del Rosario, en el Municipio de Villa del Rosario.
- Centro de Atención Tibú, en el Municipio de Tibú.

[20] CAMARA DE COMERCIO DE CUCUTA. Información General Habeas Data, (En línea) (Citado el 16 de Octubre del 2013). Disponible en: http://www.cccucuta.org.co/secciones-128-s/informacion-general-habeas-data.htm

[21] Ibid., p. 2

2.4.2 Mega. La Cámara de Comercio de Cúcuta la define como “Mega: Para el año 2028, seremos más que una Cámara de Comercio, integrando servicios que transforman retos en oportunidades para los empresarios de la región.”[22]

2.4.3 La Cámara de Comercio de Cúcuta la define como “Propósito superior: Nuestro propósito es maximizar la generación de valor como agentes de cambio, aliados del tejido empresarial, con innovación, transparencia y compromiso social.”[23]

2.4.4 Política de Calidad. “Es política de LA CAMARA DE COMERCIO DE CÚCUTA, la prestación de los servicios delegados por el Estado y el fortalecimiento empresarial, promoviendo la formalidad en nuestra zona de influencia, bajo principios de calidad, compromiso, innovación y desarrollo; cumpliendo las especificaciones técnicas y legales, con sentido de participación y representación institucional.

Mejorando constantemente los procesos y servicios, para lograr eficiencia y sostenibilidad financiera, con el fin de ofrecer a nuestros grupos de interés, una Entidad competitiva y gestora de confianza; actuando como líderes multiplicadores del Desarrollo Productivo Regional y la Transformación Digital, con sistemas de operación de clase mundial.” [24]

2.4.5 Funciones. De acuerdo con la Ley, la Cámara de Comercio de Cúcuta ejerce las siguientes funciones:[25]

Sirven de órgano de los intereses generales del comercio ante el Gobierno y ante los comerciantes mismos.

- Llevan el Registro Mercantil y certifican sobre los actos y documentos en él escritos.
- Entregar noticias en sus boletines y órganos de publicidad de las inscripciones hechas en el Registro Mercantil y de toda modificación, cancelación o alteración que se haga de dichas inscripciones.
- Recopilan las costumbres mercantiles de los lugares correspondientes a su jurisdicción y certifican sobre la existencia de las recopiladas.

[22] Ibid., p. 2
[23] Ibid., p. 3
[24] Ibid., p. 4
[25] Ibid., p. 5

- Designan el árbitro o árbitros o los amigables componedores cuando los particulares se lo solicitan.
- Organizan conferencias, editan o imprimen estudios o informes relacionados con sus objetivos, y con los intereses de la región.
- Adelantan actividades cívicas e investigaciones económicas sobre aspectos o ramos específicos del comercio interior y exterior y formulan recomendaciones a los organismos estatales y semioficiales encargados de la ejecución de los planos respectivos.
- Colaboran dentro del interés común de fomentar los planes y programas que cada uno de los diferentes gremios regionales se propongan.
- Desempeñar veedurías cívicas y ciudadanas.
- Promoción de la educación, la cultura, la recreación y el turismo.
- Promoción y desarrollo institucional, regional, nacional e internacional mediante planes, programas y proyectos, que permita el crecimiento regional y la integración fronteriza dentro de un marco de bienestar social.
- Gestionar recursos de cooperación internacional para el desarrollo de sus actividades.
- Prestar los servicios de certificación previstos en la ley 527 de 1999.
- Promover la capacitación de los empresarios.
- Prestar servicios de información comercial y documentación empresarial.
- Facilitar los mecanismos alternos de solución de conflictos.
- Mantener servicios especiales para sus afiliados.

2.4.6 Organigrama. En la siguiente figura se presenta la estructura organizacional de la Cámara de Comercio de Cúcuta.

Figura 1. Organigrama

Fuente: CAMARA DE COMERCIO DE CUCUTA. Información General Habeas Data, (En línea) (Citado el 14 de Febrero del 2013). Disponible en: http://www.cccucuta.org.co/secciones-70-s/organigrama.htm

Se presenta una modificación con respecto a la Unidad de Tecnología, que pasó de pertenecer a la Gerencia Administrativa y Financiera a formar parte de la Presidencia Ejecutiva, manteniendo las mismas funciones y procedimientos, cambiando su nombre a Dirección de Tecnología.

3. MARCO METODOLOGICO

El tipo de investigación del proyecto propuesto es de tipo aplicada, ya que se plantea identificar los principales riesgos de seguridad que tienen los activos de información de la Dirección de Tecnología de la Cámara de Comercio de Cúcuta, y a su vez aplicar los conocimientos adquiridos durante la Especialización en Seguridad Informática generando como producto el Diseño de Políticas de Seguridad de la Información.

El Área General de conocimiento del proyecto propuesto es Gestión de la Seguridad Informática.
El Área de Conocimiento Específica del proyecto es desarrollo de políticas de Seguridad informática SGSI basado en el estándar ISO/IEC27001.

3.1 POBLACION Y MUESTRA

Se determina como población el personal que conforma la Dirección de Tecnología de la Cámara de Comercio de Cúcuta, determinado como muestra el 100% de la población. En total son 13 personas distribuidas en los siguientes cargos:

- Cargo: Director de TI. Cantidad personas: 1
- Cargo: Profesional de Tecnología. Cantidad personas: 1
- Cargo: Profesional Junior de Redes y seguridad. Cantidad personas: 1
- Cargo: Profesional Junior de Tecnología. Cantidad personas: 1
- Cargo: Asistente de Tecnología. Cantidad personas: 1
- Cargo: Ingeniera de Desarrollo. Cantidad personas: 1
- Cargo: Auxiliar de Tecnología. Cantidad personas: 1
- Cargo: Auxiliar Operativo. Cantidad personas: 1
- Cargo: Programador. Cantidad personas: 1
- Cargo: Coordinador de la Mesa de Ayuda. Cantidad personas: 1
- Cargo: Técnicos de sistemas. Cantidad personas: 3

3.2 FUENTES DE INFORMACION

Las fuentes de información tomadas para la recolección de información son:

3.2.1 Fuentes de información primaria. Para el desarrollo de este proyecto se consideró como información primaria aquella información suministrada por el personal de la Dirección de Tecnología de la Cámara de Comercio de Cúcuta, quienes cuentan con el conocimiento directo producto del desempeño propio de sus funciones laborales.

3.2.2 Fuentes de información secundaria. Documentación interna de la Cámara de Comercio de Cúcuta que hace referencia a Seguridad de la Información: Documento Políticas de seguridad de la información AF-GIT-06 v.2

Información documental sobre encaminada al análisis y evaluación de la seguridad de la Información.

3.3 TECNICAS DE RECOLECCION DE INFORMACION

Para la recolección de la información, se utilizan técnicas como la observación con el fin de registrar patrones de conducta de los usuarios y funcionarios que hacen parte la Dirección de Tecnología, adicionalmente se realizan la entrevista no estructurada o diálogo con el personal con el fin de obtener la opinión personalizada de los funcionarios que forman parte de la Dirección de Tecnología.

3.4 FASES DE TRABAJO

Las fases a seguir se establecen en función de los objetivos propuestos así:

3.4.1 Fase 1. Evaluación de la seguridad de la información teniendo en cuenta los distintos controles que tiene la ISO 27001:2013 para que sirva como un componente de planificación para la implementación de medidas de seguridad de la información en la cámara de comercio de Cúcuta.

Actividad 1: Realizar una evaluación de los controles que comprende la ISO/IEC 27001:2013, para tener un diagnóstico en cuanto a la efectividad de las medidas de seguridad implementadas por la CCC.

Teniendo en cuenta que la Cámara de Comercio de Cúcuta es una Entidad privada sin ánimo de lucro, que presta la función pública de llevar el Registro Mercantil, entre otras funciones, se toma como guía algunos elementos que el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC ha desarrollado en el marco del Fortalecimiento de la Gestión TI en el Estado.

Para realizar un diagnóstico inicial del estado de la gestión de la Seguridad de la Información se utilizó el "Instrumento de Evaluación MSPI" que fue desarrollado por el MinTIC con el objetivo de que las Entidades Estatales puedan identificar el nivel de madurez de la implementación de un Modelo de Seguridad y Privacidad de la Información. En el caso del presente proyecto, se hizo esta evaluación utilizando los componentes de pruebas administrativas y técnicas, que incluyen los controles dados en la Norma ISO 27001:2013.

Una vez aplicado el instrumento de Evaluación MSPI se obtuvo como resultado el siguiente cuadro y gráfica, donde se observa el nivel alcanzado en la evaluación de efectividad de cada dominio de control de la Norma ISO 27001:2013:

Tabla 1. Evaluación de efectividad de controles

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	**INICIAL**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	12	100	**INICIAL**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	13	100	**INICIAL**
A.8	GESTIÓN DE ACTIVOS	11	100	**INICIAL**
A.9	CONTROL DE ACCESO	63	100	**GESTIONADO**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	46	100	**EFECTIVO**
A.12	SEGURIDAD DE LAS OPERACIONES	40	100	**REPETIBLE**
A.13	SEGURIDAD DE LAS COMUNICACIONES	34	100	**REPETIBLE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	7	100	**INICIAL**
A.15	RELACIONES CON LOS PROVEEDORES	0	100	**INEXISTENTE**

Tabla 1. (Continuación)

No.	Evaluación de Efectividad de controles			
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	**INEXISTENTE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	47	100	**EFECTIVO**
A.18	CUMPLIMIENTO	27,5	100	**REPETIBLE**
	PROMEDIO EVALUACIÓN DE CONTROLES	**23**	**100**	**REPETIBLE**

Fuente: Elaboración propia

Figura 2. Brecha anexo A ISO 27001:2013

Fuente: Elaboración propia

Análisis de resultados:

Al analizar los resultados se puede observar que la Cámara de Comercio de Cúcuta a la fecha de este proyecto se encuentra en una fase inicial en la mayoría de los dominios de control de la ISO 27001:2013. Esto debido a que la Entidad a pesar de tener controles de seguridad en operación, hay muchos aspectos de la seguridad en los cuales no se ha trabajo aún. Actualmente no se cuenta con un inventario de activos y no se ha realizado un análisis de riesgos que les permita establecer claramente los riesgos a los que se encuentra expuesta la información, y por esta razón, los controles existentes no han sido definidos de una manera sistemática para garantizar la integridad, disponibilidad y privacidad de la información.

A continuación se detallarán los puntos más fuertes que tiene la Entidad que son los correspondientes a Control de Acceso, que en la evaluación obtuvo un nivel de efectividad Gestionado, y Aspectos de Seguridad de la Información de la Gestión de la Continuidad del negocio que obtuvo un nivel de Efectivo.

- Dominio Control de Acceso: La Cámara de Comercio de Cúcuta tiene implementado varios controles que han demostrado efectividad. Como base de este control se tiene que el proceso de solicitud de acceso a la red y a los sistemas se encuentra formalizado a través de una ruta en el Sistema de Gestión Documental Mercurio. De esta manera se tiene siempre una autorización por parte del Gerente encargado del área para asignar credenciales de acceso.
- Se tiene configurado un servidor de directorio activo que permite mantener un control en el acceso a la red, a la vez que le presenta al usuario una política de uso correcto de los recursos asignados. La clave es única y el sistema obliga a cambiarla automáticamente cada 42 días y maneja un alto grado de complejidad. Esta misma clave es usada en varios sistemas, pues algunos sistemas se comunican con protocolos como LDAP para la autenticación contra el directorio activo, lo que ayuda a que el cambio de una contraseña se aplica para varios sistemas.
- Cuando se entregan las credenciales del dominio por primera vez, el sistema obliga a realizar un cambio inmediato de la clave y por políticas no permite que se utilicen contraseñas previas.
- Este mismo directorio permite controlar la instalación de software en los equipos, pues solo lo pueden realizar perfiles administradores.
- En cuanto al acceso a la red, se tienen controles de seguridad a nivel del servidor DHCP (filtros de denegación o permitir), asociación de dirección MAC con la IP asignada al dispositivo, y a nivel de los switches se asocia también la dirección MAC con el puerto, para que no se pueda conectar ningún otro

dispositivo en ese puerto, pues de lo contrario el puerto se bloquea automáticamente.

- En cada sistema se maneja el control de acceso con la creación de los usuarios según llegan las solicitudes por el Sistema de Gestión Documental. Igualmente se aplica el mismo procedimiento para la desactivación por finalización de contrato, vacaciones o incapacidades.
- Se debe mejorar el control de acceso en cuanto a la revisión periódica de permisos concedidos, ya que no se ha definido una periodicidad formal para esto, y los sistemas no tienen una manera de programar estas desactivaciones, depende del administrador realizarlas. También se deben formalizar procedimientos de acceso a la red wifi, que a la fecha no existen.
- También es importante que toda la Entidad conozca y comprenda la importancia de los controles definidos, para que al momento de solicitar un acceso lo realicen rápidamente por los canales establecidos, y que al momento de presentarse una incapacidad también se informe de la eventualidad y proceder a desactivar los usuarios.
- Dominio Aspectos de Seguridad de la Información de la Gestión de la Continuidad del negocio. La Cámara de Comercio de Cúcuta cuenta con una arquitectura redundante en sus centros de datos principales, contando con dos sitios alternos donde se almacena la información de manera asíncrona cada 5 minutos con el sitio alterno 2, y en forma de copias de seguridad en un tercer sitio en una ubicación externa, en la Sede Avenida Cero. Esto le brinda a la Entidad la posibilidad de levantar servicios en cuestión de minutos, y también le permite en caso de una falla que afecte todo el centro de datos principal, tener toda la información disponible.
- En la Dirección de Tecnología se tiene un documento Plan de Recuperación de Desastres (DRP por sus siglas en inglés *Disaster Recovery* Plan) entregado por el proveedor que implementó la solución SAN de Alta disponibilidad que establece la manera en que se pueden levantar servicios o todo el centro de datos en el centro alterno.
- En cuanto a este dominio falta que se defina un BCP (*Business Continuity* Plan), involucrando a todas las partes de la Entidad, no solo la Dirección de Tecnología. También se debe realizar periódicamente las pruebas de la solución SAN de Alta Disponibilidad.

A continuación se detallarán aquello que es más relevante que se detectó en cada uno de los dominios que no permitió obtener un resultado más alto en la evaluación:

- Políticas de Seguridad de la información: Existe una Política de Seguridad de la Información, pero no ha sido debidamente socializada. No existe aún una asignación de responsabilidades. La política ha tenido algunas revisiones y están pendientes algunos ajustes ya detectados por la Dirección de

Tecnología, pero no han sido el resultado de un análisis de seguridad de la información.

- Adicionalmente no existen varios de los documentos planteados en la política como el manual de políticas y los procedimientos en materia de protección.
- Organización de la seguridad de la información: No hay una definición de roles y responsabilidades con respecto a la seguridad de la información. Hay un Comité de Seguridad de la Información y Protección de datos que cuenta con el aval de Presidencia Ejecutiva, que apenas está iniciando.
- Aún no existe un inventario de activos con asignación de responsables o propietario. Existe un pequeño presupuesto para capacitaciones que se realizarán apenas este año 2019.
- No hay una comunicación con autoridades en el tema, tampoco existen procedimientos para reportar eventos o incidentes de seguridad de la información.
- No existe un Sistema de Gestión de Seguridad de la Información formalizado como tal.
- Seguridad de los recursos humanos: No existen a la fecha una definición de responsabilidades en cuanto a la seguridad de la información, así como tampoco se ha iniciado con capacitaciones en temas relacionados a todos los empleados para la toma de conciencia en temas de seguridad de la información.
- Existe para el caso de algunos empleados la firma de un acuerdo de confidencialidad de la información, pero es algo que sólo se ha hecho firmar a los empleados más nuevos. Los contratos más antiguos se mantienen sin esa cláusula de confidencialidad.
- No existe aún un proceso disciplinario en el caso de incurrir en alguna violación a la seguridad de la información.
- Gestión de activos: No existe un inventario de activos de información y tampoco se ha definido la propiedad de estos activos.
- Criptografía: No existe una política sobre el uso de controles criptográficos para la protección de la información. Es un punto débil también el hecho que no se utiliza la encriptación para que información transportada o almacenada en dispositivos móviles o externos se encuentre encriptada, o cuando se envía a través de los medios de comunicación electrónicos.
- Seguridad física y del entorno: Existen centros de datos delimitados a parte de las oficinas, pero falta definir controles de acceso más efectivos, sólo cuentan con una cerradura para controlar el acceso y no se hace un registro de acceso a estos sitios. También es inexistente políticas que controlen el uso de dispositivos de grabación o fotográficos en los centros de datos y telecomunicaciones.
- Hay un programa de mantenimientos para equipos e impresoras, pero para los dispositivos de la red no existe el mismo programa, se debe solicitar anualmente su aprobación y en varios años no ha sido aprobado este mantenimiento.

- Seguridad de las operaciones: No existe control de cambios a nivel de seguridad de la información, no hay un procedimiento formal para la aprobación de cambios. No hay procedimientos formales para optimizar los recursos en los sistemas.
- Algunos sistemas cuentan con ambiente de pruebas, pero no todos. En lo referente a actualizaciones de sistemas operativos, estas se hacen en las máquinas de producción y no en un ambiente de pruebas y es responsabilidad del administrador. No hay un procedimiento formal.
- Falta la definición de una política de retención de registros o logs de los sistemas.
- Seguridad de las comunicaciones: No existe una definición de acuerdos de nivel de servicio. Tampoco existen procedimientos formales que regulen las comunicaciones y la transferencia de la información.
- No se han definido directrices formales para la mensajería electrónica.
- Adquisición, desarrollo y mantenimiento de sistemas: La Entidad no cuenta con procedimientos definidos formalmente para exigir el cumplimiento de requisitos de seguridad de la información en los nuevos sistemas de información. Se solicita a los proveedores ciertos parámetros a cumplir sobre controles de acceso, registro de logs, etc., pero dentro del marco de algo formal.
- Relaciones con los proveedores: Al no existir un inventario de activos, no existe tampoco acuerdos donde se indique el acceso a la información. Se hace firmar un acuerdo de confidencialidad en algunos casos específicos a los proveedores, pero no en todas las modalidades de contratación.
- En el caso de proveedores de servicio en la nube, no se realiza un análisis de riesgos asociados a este tipo de servicios, ni se custodia la cadena de suministro en el caso de que el proveedor tercerice el servicio, como sucede con Confecámaras y el Sistema Integrado de Información SII.
- Gestión de incidentes de seguridad de la información: La Cámara de Comercio de Cúcuta no realiza gestión de incidentes de seguridad de la información.
- Cumplimiento: La Dirección de TI tiene un inventario del software licenciado y se verifica periódicamente comparando con las licencias adquiridas. Falta documentar estos procesos de verificación y su periodicidad.
- La entidad no tiene una política publicada sobre el cumplimiento de propiedad intelectual.

3.3.2 Fase 2. Identificación de los activos de información críticos para la Unidad de Tecnología de la cámara de comercio de Cúcuta, aplicando los criterios de valoración en términos de confidencialidad integridad y disponibilidad.

- Actividad 1: Selección de la metodología adecuada para realizar el análisis de riesgos

Para realizar el análisis de riesgos de seguridad de la información se hizo una revisión previa de algunas de las metodologías existentes, para seleccionar aquella que se adapte mejor a los requerimientos de la Entidad.

Una metodología de análisis de riesgos en Seguridad de la Información es una guía paso a paso que nos permite a través de la aplicación de técnicas, obtener resultados para la toma de decisiones en el momento de implementar controles que mitiguen el riesgo al que están expuestos los activos de información para una empresa.

Las metodologías que se analizaron fueron las siguientes:

Octave: Llamada así por ser el acrónimo en inglés de *Operationally Critical Threat, Asset, and Vulnerability Evaluation,* es una metodología de evaluación de riesgos desarrollada por el *Software Engineering Institute* (SEI) de la *Carnegie Mellon University de Pensilvania* en conjunto con el *Telemedicine and Advanced Technology Research Center* (TATRC), en Estados Unidos. Es la metodología de uso oficial de algunos organismos norteamericanos tal como el Departamento de Defensa. Se enfoca en estudiar los riesgos considerando el principio de la confidencialidad, la integridad y la disponibilidad.

Las actividades que esta metodología define son las siguientes:

- Identificar los activos críticos y las amenazas a las que están expuestos
- Identificar las vulnerabilidades, tanto tecnológicas como organizacionales que originan estos riesgos.
- Desarrollar una estrategia de protección basada en buenas prácticas, así como planes para la mitigación de los riesgos.

Octave busca entre otras cosas concientizar que la seguridad de la información no solamente es una responsabilidad del área técnica sino de toda la organización.

Octave ha evolucionado en diferentes versiones[26]:

Octave: La primera versión de su marco conceptual se liberó en septiembre de 1999 impulsada por la necesidad de enfrentar los retos de seguridad que

[26] CARALLI Richard, et al. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. USA: Carnegie Mellon University, 2007. 154 p.

generaba la aplicación de la Ley de Transferencia y Responsabilidad de Seguro Médico (*Health Insurance Portability and Accountability* Act, HIPAA por sus siglas en inglés) en las áreas de privacidad y seguridad de la información sobre la salud de las personas. Luego en 2001 y 2002 se hicieron modificaciones a su marco conceptual y criterios que son los que se aplican actualmente bajo el nombre del Método Octave.

Octave-S: En marzo de 2005, se liberó la versión de Octave-S v1.0, este enfoque está diseñado específicamente para su aplicación en organizaciones pequeñas (100 personas o menos), consta de 3 fases similares al Método Octave, pero la idea es que el análisis sea realizado por un equipo de personas que pertenezcan a la organización y que tengan un amplio conocimiento de cómo funciona esta, cuáles son sus activos importantes, las necesidades de seguridad y las amenazas. Al estar pensado para ser aplicado en organizaciones pequeñas por personal interno está más estructurado y se han incorporado los conceptos de seguridad a las hojas de trabajo y las guías de aplicación.

Octave Allegro: Liberado en su versión 1.0 en junio de 2007, el enfoque de Octave Allegro está centrado en lograr una evaluación más amplia de los riesgos operacionales de la organización, pero centrado principalmente en los activos de información en el contexto de cómo se utilizan, almacenan, transportan y procesan. Se podría considerar que es una versión simplificada del Método Octave.

MEHARI: Nombre derivado de las siglas en inglés de *Method for Harmonized Analysis of Risk* (Método para el análisis armonizado del riesgo), fue creada por el CLUSIF (Club francés de la seguridad de la información) a mediados de los años 90 y ha venido evolucionando desde entonces con el objetivo principal de ayudar a los encargados de la seguridad de la información de las organizaciones (CISO por sus siglas en inglés, *Chief Information Security Officers*) a gestionar todo lo referente a las actividades de seguridad informática, aunque pueden utilizarlo otros actores del proceso como los auditores y gestores de riesgo.

Esta metodología fue liberada bajo la licencia de uso libre *Creative Commons* lo cual permite su uso gratuito y el desarrollo de aplicaciones y herramientas adicionales basados en los mismos principios.

La intención principal de esta metodología es lograr diseñar un modelo de riesgo, valorar y simular los niveles de ese riesgo y evaluar la eficiencia de las políticas de seguridad previamente implementadas en la organización y a partir de ese basamento realizar un análisis de las deficiencias e inconvenientes encontrados.

Se apoya en tres elementos principales, el análisis y evaluación de los riesgos, evaluación de la seguridad usando el análisis de vulnerabilidades y el análisis de amenazas y con eso se construyen posteriormente los planes de acción que permitan mantener la seguridad de la información.

MAGERIT: (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), desarrollada por el Ministerio de Hacienda y Administraciones Públicas de España. Esta metodología se encuentra explicada en tres libros: Método, Catálogo de Elementos y Guía de Técnicas, y plantea dentro del análisis de riegos la identificación de los activos de información, las salvaguardas, las amenazas y vulnerabilidades de un sistema de información. También incluye la gestión de riesgos y cómo definir planes de seguridad.

- El método: Es la guía donde se detalla la metodología de análisis de riesgos.
- Catálogo de Elementos: Incluye listados de elementos tales como activos, dimensiones de seguridad, criterios de valoración de los activos, amenazas típicas y salvaguardas.
- Guía de Técnicas: Contiene algunas técnicas útiles para el análisis de riesgos, tales como tablas, análisis costo-beneficio, histogramas, árboles de tanque, entre otras.

NIST SP 800 – 30: (*National Institute of Standards and Technology*). Metodología de análisis de riesgos desarrollada por el Instituto Nacional de Estándares y Tecnología NIST, agencia federal para la Administración de Tecnología de Departamento de Comercio de los Estados Unidos. La NIST SP 800-30 forma parte de una serie de publicaciones (serie SP 800) orientada a la Seguridad de la Información.

El análisis de riesgos en la Metodología NIST SP 800-30 se plantea realizarse en 9 pasos:

- Caracterización del sistema.
- Identificación de amenaza.
- Identificación de vulnerabilidades.
- Control de análisis.
- Determinación del riesgo.
- Análisis de impacto.
- Determinación del riesgo.
- Recomendaciones de control.
- Resultado de la implementación o documentación.

Se listan las ventajas y desventajas de cada una de las principales metodologías a fin de encontrar los aspectos y características que más se alinean con la aplicación específica en la Cámara de Comercio de Cúcuta.

Tabla 2. Ventajas y desventajas de metodologías de análisis de riesgos

Nombre	Ventajas/Desventajas
OCTAVE Aplica a: Pymes, organizaciones públicas y privadas.	Ventajas: Un equipo multidisciplinario de la misma organización puede implementarla. Construcción de los perfiles de amenazas basados en activos. Identificación de la infraestructura de vulnerabilidades. Desarrollo de planes y estrategias de seguridad. Comprende las etapas de análisis y gestión de riesgos. Involucra procesos, activos, dependencias, recursos, vulnerabilidades, amenazas y salvaguardas. Relaciona amenazas y vulnerabilidades. Gratuito para uso interno. Desventajas: Utiliza gran cantidad de documentos en el proceso de análisis de riesgos. Se requiere amplios conocimientos técnicos. No define claramente los activos de información. Para uso externo se debe comprar una licencia.
MAGERIT	Ventajas:

Tabla 2. (Continuación)

Nombre	Ventajas/Desventajas
Aplica a: Gobierno, compañías grandes comerciales y no comerciales, Pymes.	Alcance completo en el análisis y gestión de riesgos. Está bien documentada en cuanto a recursos de información, amenazas y tipos de activos. Utiliza análisis de riesgo cuantitativo y cualitativo. De uso libre y gratuito. Divide los activos de la organización en diferentes grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier riesgo. Se centra en tres objetivos: Concientizar sobre la existencia de los riesgos y de la necesidad de atajarlos a tiempo, ofrecer un método sistemático para analizar tales riesgos, ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación. Permite que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión de riegos efectiva. Buena documentación y guías. Posee herramienta de software para el análisis de riesgo (PILAR). Desventajas: En su modelo no involucra los procesos, recursos, ni vulnerabilidades. Posee falencias en el inventario de políticas. Se considera una metodología costosa en su aplicación.
MEHARI Aplica a: Gobierno, organismos, empresas grandes y medianas, compañías comerciales sin ánimo de lucro.	Ventajas: Utiliza modelos cuantitativos y cualitativos para el análisis de riesgo. Posee bases de datos de conocimientos con manuales, guías y herramientas que permiten realizar el análisis de riesgos cuando sea necesario. Complementa y se acopla a las necesidades de la norma ISO 27001, 27002 y 27005 para definir los SGSI y la gestión de riesgos. Combina análisis y evaluación de riesgos; particularmente, se especifica un módulo de evaluación rápida y uno de evaluación detallada.

Tabla 2. (Continuación)

Nombre	Ventajas/Desventajas
NIST SP 800-30 Aplica a: Organizaciones gubernamentales y no gubernamentales	Desventajas: Se enfoca solo en los principios de integridad, confidencialidad y disponibilidad, olvidando el no repudio. La recomendación de los controles no se incluye dentro del análisis sino dentro de la gestión de los riesgos. El impacto de los riesgos se estima en el proceso de gestión y evaluación. Ventajas: Bajo costo relacionado con el riesgo analizado y solventado. Proporciona una guía para evaluación de riesgos de seguridad en las infraestructuras de TI. Presenta un resumen de los elementos clave de las pruebas de seguridad técnica y la evaluación con énfasis en técnicas específicas, sus beneficios, limitaciones y recomendaciones para su uso. La guía provee herramientas para la valoración y mitigación de riesgos. Asegura los sistemas informáticos que almacenan, procesan y transmiten información. Desventajas: En su modelo no tiene contemplados elementos como los procesos, los activos ni las dependencias.

Fuente: ALEMAN Helena y RODRIGUEZ Claudia. Metodologías Para el Análisis de Riesgos en los SGSI. En: Publicaciones e investigaciones, Mayo, 2015. vol. 9, No. 2, p. 23-29.

Basados en las ventajas y desventajas reflejadas en la tabla anterior se seleccionan las siguientes características descriptivas comunes que permiten analizar y comparar la aplicación de cada metodología a este caso en específico.

- Ámbito de aplicación: Corresponde al tipo de empresa a la cual está especialmente dirigida la metodología.
- Costo de Implementación: Considera si la metodología implica altos costos a la empresa para su implementación.

- Disponibilidad de profesionales entrenados: Hace referencia a la facilidad de conseguir documentación, profesionales entrenados y proyectos similares en Colombia.
- Licenciamiento: Si la metodología implica la adquisición de una licencia para su utilización.
- Incluye recomendaciones para los controles de seguridad: La metodología incluye recomendaciones de controles o salvaguardas de los activos de información.
- Incluye análisis cuantitativo: La metodología permite un análisis tanto cuantitativo como cualitativo.

Para la evaluación se asignó un peso a estas características, siendo 3 la ponderación más alta, y 1 la más baja. Analizando estas características para las metodologías seleccionadas, se obtiene el siguiente cuadro:

Tabla 3. Evaluación de metodologías de análisis de riesgos

		Metodología (de 1 a 3 / 3 es mejor)			
Característica	Importancia (1 a 3 / 3 es mayor peso)	Octave	Magerit	Mehari	NISP 800-30
Ámbito de aplicación	3 x	3	3	3	2
Costo de implementación	3 x	2	3	3	3
Simplicidad en la documentación	2 x	1	2	2	2
Disponibilidad de profesionales entrenados	3 x	1	3	2	2
Licenciamiento	3 x	1	3	3	3
Incluye recomendaciones para los controles	2 x	3	3	1	3
Incluye análisis cuantitativo	2 x	3	3	3	3
Total:		35	52	45	46

Fuente: Elaboración propia

La puntuación más alta, que se obtiene de la sumatoria del puntaje de cada característica multiplicado por la importancia de la misma, la obtiene la metodología Magerit, y se selecciona Magerit como la metodología para hacer el

análisis de riesgos para la Dirección de Tecnología de la Cámara de Comercio de Cúcuta.

- Actividad 2: Realizar el inventario de los activos de información: La identificación de los activos de información se realizó teniendo como base la clasificación propuesta por Magerit, y se obtuvo la lista gracias al acompañamiento del personal de Ingenieros de la Dirección de Tecnología, que a través de entrevistas y reuniones grupales se llegó al siguiente listado:

Tabla 4. Identificación y clasificación de los activos

Nombre del Activo	Cantidad	Responsable
Tipo: [D] Datos		
Base de datos Mercurio	1	Profesional Junior de Tecnología
Base de datos Worfkflow	1	Profesional Junior de Tecnología
Base de datos Docuware	1	Profesional Junior de Tecnología
Base de datos BPM	1	Asistente de Tecnología
Base de datos SGD	1	Asistente de Tecnología
Base de datos SII	1	Profesional de Tecnología
Base de datos Censo	1	Programador
Base de datos SIREP	1	Profesional de Tecnología
Base de datos Helpdesk	1	Auxiliar de Tecnología
Base de datos Página Web	1	Profesional Junior de Redes y Seguridad
Backups de Máquinas virtuales	1	Auxiliar de Tecnología
Backups de bases de datos	1	Cada administrador, Programador
Manuales de contingencia	NA	Cada administrador
Manuales de los sistemas	NA	Cada administrador, Profesional Junior de Tecnología
Logs de los sistemas	NA	Cada administrador
Tipo: [K] Claves criptográficas		
Firma Electrónica Secretaria General	1	Profesional de Tecnología, Secretaría general
Firma electrónica Persona Jurídica	1	Profesional de Tecnología, Secretaría general

Tabla 4. (Continuación)

Firma de la sic	1	Gerente Administrativa y Financiera
Código QR de BPM	1	Asistente de Tecnología
Tipo: [SW] Servicios		
Directorio Activo - Autenticación	1	Auxiliar de Tecnología
Telefonía IP	1	Auxiliar de Tecnología
Página web	1	Profesional Junior de Redes y Seguridad
Mesa de ayuda	1	Auxiliar de Tecnología
Intranet	1	Profesional Junior de Tecnología
Correo electrónico	1	Auxiliar de Tecnología
DNS	1	Profesional Junior de Redes y Seguridad
DHCP	1	Profesional Junior de Redes y Seguridad
Proxy	1	Profesional Junior de Redes y Seguridad
Sistema de Gestión Documental	1	Auxiliar de Tecnología
Sistema de Gestión Documental registros públicos	1	Profesional Junior de Tecnología
Sistema de Registros Públicos	1	Profesional de Tecnología
Sistema de Gestión Administrativa y Financiera	1	Profesional de Tecnología
Almacenamiento en la nube Amazon	1	Profesional de Tecnología
Almacenamiento en la nube Azure	1	Auxiliar de Tecnología
Almacenamiento en la nube Onedrive	1	Profesional Junior de Tecnología
Tipo: [SW] Software		
Sistemas operativos	20	Director TI, Auxiliar de Tecnología
Software de gestión y administración Bases de datos	1	Profesional Junior de Tecnología
Software de gestión y administración Bases de datos nuevo	1	Asistente de Tecnología
Antivirus	1	Auxiliar de Tecnología
Software de gestión y administración de backups	1	Auxiliar de Tecnología
Software de administración Plataforma Tecnológica	1	Asistente de Tecnología
Software de virtualización	1	Asistente de Tecnología
Software Actualizaciones sistemas operativos PC	1	Auxiliar de Tecnología

Tabla 4. (Continuación)

Plataforma OFFICE 365	1	Auxiliar de Tecnología
Software de sincronización usuarios office 365	1	Auxiliar de Tecnología
Firewall Seguridad perimetral	1	Profesional Junior de Redes y Seguridad
Monitoreo de Red	1	Profesional Junior de Redes y Seguridad
Tipo: [HW] Hardware		
Servidores	5	Asistente de Tecnología
Almacenamientos	3	Asistente de Tecnología
Computadores	7	Coordinador de Mesa de Ayuda
Portátiles	6	Coordinador de Mesa de Ayuda
Impresora	1	Coordinador de Mesa de Ayuda
Switches	25	Profesional Junior de Redes y Seguridad
Access Point	16	Profesional Junior de Redes y Seguridad
Tipo: [COM] Redes de comunicaciones		
Red LAN	1	Profesional Junior de Redes y Seguridad
Red Wifi	1	Profesional Junior de Redes y Seguridad
Red LAN extendida (sedes)	4	Profesional Junior de Redes y Seguridad
Internet	2	Profesional Junior de Redes y Seguridad
Canal SIP Telefonía IP	1	Auxiliar de Tecnología
Tipo: [Media] Soportes de información		
Discos Duros Externos	6	Programador
Tipo: [AUX] Elementos auxiliares		
UPS en Centros datos	20	Coordinador de Mesa de Ayuda
Inversores	4	Coordinador de Mesa de Ayuda
Cableado estructurado	1	Profesional Junior de Redes y Seguridad
Tipo: [L] Instalaciones físicas		
Centros de Datos	14	Gerente Administrativa y Financiera, Directora TI
Oficinas	1	Gerente Administrativa y Financiera
Tipo: [P] Personal		
Director TI	1	Presidente Ejecutivo
Profesional de Tecnología	1	Director TI
Profesional Junior de Redes y seguridad	1	Director TI
Profesional Junior de Tecnología	1	Director TI
Asistente de Tecnología	1	Director TI
Ingeniera de Desarrollo	1	Director TI
Auxiliar de Tecnología	1	Director TI

Tabla 4. (Continuación)

Auxiliar Operativo	1	Director TI
Programador	1	Director TI
Coordinador de la Mesa de Ayuda	1	Director TI
Técnicos de sistemas	3	Director TI

Fuente: Elaboración propia

- Actividad 3: Valorar las tres dimensiones de la seguridad para cada activo.

Para cada uno de los activos de información de la Dirección de Tecnología se establecieron la disponibilidad, la confidencialidad y la integridad como las dimensiones a valorar. Estas dimensiones son aquellas características de la información que pueden verse disminuidas en su valor en el caso de la materialización de una amenaza.

Para el caso de los activos de información de la Dirección de Tecnología de la Cámara de Comercio de Cúcuta se definieron las siguientes tablas de valoración para cada una de las dimensiones de seguridad:

Confidencialidad: es aquella característica de la información que hace referencia a que el activo sólo es accesible para las personas o sistemas que están autorizados. Se tiene en cuenta la clasificación de la información en pública, clasificada o reservada, Ley 1712 de 2014.

Tabla 5. Tabla de valoración de la confidencialidad

Valor Cuantitativo	Valor Cualitativo	Descripción
1	Bajo	Información Pública / La divulgación no autorizada del activo no afecta a la Entidad.
2	Medio	Información clasificada / La divulgación no autorizada del activo incumple políticas de manejo de la información.
3	Alto	Información reservada / la divulgación no autorizada del activo afecta a la Entidad en su imagen o se incurre en incumplimientos legales.

Fuente: Elaboración propia

Tabla 6. Tabla de valoración de la disponibilidad

Valor Cuantitativo	Valor Cualitativo	Descripción
1	Bajo	El activo puede estar indisponible un día.
2	Medio	Si el activo está indisponible por 8 horas, se generan retrasos en el cumplimiento de algunos objetivos.
3	Alto	Si el activo esta indisponible una hora, seria crítico para la entidad.

Fuente: Elaboración propia

Tabla 7. Tabla de valoración de la Integridad

Valor Cuantitativo	Valor Cualitativo	Descripción
1	Bajo	Si se modifica el activo no sería muy relevante para la Entidad.
2	Medio	Si se modifica el activo esto tiene un impacto medio para la Entidad.
3	Alto	Si se modifica el activo sería crítico para la Entidad.

Fuente: Elaboración propia

Del Activo: Esta corresponde al cálculo que se realiza promediando la valoración a cada una de las dimensiones de seguridad y permite determinar la escala de importancia en la cual se encuentra el activo para la Dirección de Tecnología. Se utiliza la escala bajo, medio y alto de acuerdo a la criticidad que supondría la ocurrencia de un incidente de seguridad para la Entidad. Los activos que obtengan una valoración media y alta serán los seleccionados posteriormente para el análisis de riesgos.

Tabla 8. Tabla de criticidad de los activos

Valor Cuantitativo	Valor Cualitativo	Descripción
1	Bajo	Al sucederle algo a este activo su impacto es bajo o poco crítico para la Entidad.
2	Medio	Al sucederle algo a este activo su impacto es medio o medianamente crítico para la Entidad.
3	Alto	Al sucederle algo a este activo su impacto es alto o crítico para la Entidad.

Fuente: Elaboración propia

La metodología Magerit da una clasificación de los activos con el objetivo de poder tipificar las amenazas que pueden ser más comunes para cada tipo, además de permitir realizar la relación de dependencia entre ellos.

Las categorías que propone Magerit son:

- Datos [D]: Es la información que es almacenada dentro de otros activos tales como equipos, soporte de información, bases de datos, etc. En el caso de la Dirección de Tecnología de la Cámara de Comercio de Cúcuta se analizaron datos almacenados en medios físicos y digitales.
- Claves criptográficas [K]: Es aquello que se utiliza para proteger la información para que no pueda ser leída por personas no autorizadas. En el caso de la Dirección de Tecnología se tuvieron en cuenta las firmas electrónicas que son utilizadas en varios de los sistemas de información a cargo de la Dirección de Tecnología.
- Servicios [S]: Son aquellas funciones que permiten satisfacer una necesidad de los usuarios. Para este caso se tuvieron en cuenta servicios prestados por la

Dirección de Tecnología a través de los Sistemas de Información y algunos otros como servicios en la nube y servicios relacionados con la red de datos.

- Software [S]: Corresponde a todo aquel programa con el que se ha automatizado alguna tarea y que funciona sobre un equipo informático tipo hardware. Para la Dirección de Tecnología se incluyeron aquellos aplicativos que forman parte de soluciones informáticas compradas a terceros, algunos desarrollos propios, aplicaciones de seguridad, etc.
- Hardware [H]: Es todo aquel dispositivo que soporta la ejecución de las aplicaciones y en general servicios que presta una organización. Para la Dirección de Tecnología se incluyen servidores, computadores, portátiles, equipos de almacenamiento, etc.
- Redes de comunicaciones [COM]: Son aquellas instalaciones, dispositivos y medios de comunicación que permite la transferencia de datos de un sistema a otro. Para el presente caso, se tienen en cuenta redes LAN, redes contratadas con terceros como Internet y MPLS y canal de Telefonía IP.
- Soportes de información [Media]: Son los dispositivos físicos que permiten almacenar información en ellos. Para la Dirección de Tecnología es importante el manejo que se le da los discos duros externos para el transporte y almacenamiento de Backups en un lugar remoto por lo que se incluyen en este inventario.
- Elementos auxiliares [AUX]: Son dispositivos que también soportan a los sistemas sin estar relacionados con los datos, sino a su disponibilidad. Para la Dirección de Tecnología son importantes los sistemas de alimentación ininterrumpida y demás elementos de protección eléctrica, así como el cableado estructurado.
- Instalaciones físicas [L]: Son lugares en la organización donde se ubican los equipos y sistemas de información. Para este proyecto se analizan las oficinas de la Dirección de Tecnología y los Centros de datos.
- Personal [P]: Son aquellas personas que interactúan con los sistemas de información. Se tienen en cuenta los profesionales de la Dirección de Tecnología.

A continuación se presentan los resultados de la valoración de los activos de información de la Dirección de Tecnología de la Cámara de Comercio de Cúcuta.

Tabla 9. Valoración de dimensiones de los activos de información.

Nombre del Activo	Valoración de Dimensiones			Valor Cualitativo (Criticidad)	Valor Cuantitativo (Criticidad)
	D	I	C		
Tipo: [D] Datos					
Base de datos Mercurio	2	3	3	3	Alto
Base de datos Worfkflow	3	3	3	3	Alto
Base de datos Docuware	3	3	3	3	Alto
Base de datos BPM	2	3	3	3	Alto
Base de datos SGD	2	3	3	3	Alto
Base de datos SII	3	3	3	3	Alto
Base de datos Censo	2	3	3	3	Alto
Base de datos SIREP	1	3	3	2	Medio
Base de datos Helpdesk	2	3	3	3	Alto
Base de datos Página Web	3	3	3	3	Alto
Backups de Máquinas virtuales	1	3	3	2	Medio
Backups de bases de datos	1	3	3	2	Medio
Manuales de contingencia	1	3	2	2	Medio
Manuales de los sistemas	1	3	2	2	Medio
Documentos estandarizados TI	1	3	2	2	Medio
Logs de los sistemas	1	3	2	2	Medio
Tipo: [K] Claves criptográficas					
Firma Electrónica Secretaria General	2	3	3	3	Alto
Firma electrónica Persona Jurídica	2	3	3	3	Alto
Firma electrónica DIAN	2	3	3	3	Alto
Firma de la sic	2	3	3	3	Alto
Código QR de BPM	2	3	3	3	Alto
Tipo: [SW] Servicios					
Directorio Activo - Autenticación	3	2	2	2	Medio
Telefonía IP	2	2	2	2	Medio
Página web	3	2	2	2	Medio
Mesa de ayuda	2	2	2	2	Medio
Intranet	2	2	2	2	Medio
Correo electrónico	2	3	2	2	Medio
DNS	3	3	1	2	Medio
DHCP	2	2	1	2	Medio

Tabla 9. (Continuación)

Nombre del Activo	Valoración de Dimensiones			Valor Cualitativo (Criticidad)	Valor Cuantitativo (Criticidad)
Proxy	2	1	1	1	Bajo
Sistema de Gestión Documental	2	3	3	3	Alto
Sistema de Gestión Documental registros públicos	2	3	3	3	Alto
Sistema de Registros Públicos	3	3	3	3	Alto
Sistema de Gestión Administrativa y Financiera	2	3	3	3	Alto
Almacenamiento en la nube Amazon	3	3	3	3	Alto
Almacenamiento en la nube Azure	1	3	3	2	Medio
Almacenamiento en la nube Onedrive	2	3	3	3	Alto
Tipo: [SW] Software					
Sistemas operativos	3	1	2	2	Medio
Software de gestión y administración Bases de datos	3	3	2	3	Alto
Software de gestión y administración Bases de datos nuevo	1	1	2	1	Bajo
Antivirus	2	2	1	2	Medio
Software de gestión y administración de backups	1	3	2	2	Medio
Software de administración Plataforma Tecnológica	2	2	2	2	Medio
Software de virtualización	3	1	2	2	Medio
Software Actualizaciones sistemas operativos PC	1	1	2	1	Bajo
Plataforma OFFICE 365	1	2	2	2	Medio
Software de sincronización usuarios office 365	1	2	2	2	Medio
Firewall Seguridad perimetral	3	2	2	2	Medio
Monitoreo de Red	1	1	1	1	Bajo
Tipo: [HW] Hardware					
Servidores	3	3	3	3	Alto
Almacenamientos	3	3	3	3	Alto

Tabla 9. (Continuación)

Nombre del Activo	Valoración de Dimensiones			Valor Cualitativo (Criticidad)	Valor Cuantitativo (Criticidad)
Computadores	1	1	2	1	Bajo
Portátiles	2	2	2	2	Medio
Impresora	1	1	1	1	Bajo
Switches	3	3	1	2	Medio
Access Point	1	1	1	1	Bajo
Tipo: [COM] Redes de comunicaciones					
Red LAN	3	3	2	3	Alto
Red Wifi	2	1	2	2	Medio
Red LAN extendida (sedes)	3	2	3	3	Alto
Internet	3	1	1	2	Medio
Canal SIP Telefonía IP	3	1	1	2	Medio
Tipo: [Media] Soportes de información					
Discos Duros Externos	1	3	3	2	Medio
Tipo: [AUX] Elementos auxiliares					
UPS en Centros datos	3	1	1	2	Medio
Inversores	1	1	1	1	Bajo
Cableado estructurado	3	1	1	2	Medio
Tipo: [L] Instalaciones físicas					
Centros de Datos	3	3	3	3	Alto
Oficinas	1	1	1	1	Bajo
Tipo: [P] Personal					
Director TI	2	1	3	2	Medio
Profesional de Tecnología	2	1	3	2	Medio
Profesional Junior de Redes y seguridad	2	1	3	2	Medio
Profesional Junior de Tecnología	2	1	3	2	Medio
Asistente de Tecnología	2	1	3	2	Medio
Ingeniera de Desarrollo	2	1	3	2	Medio
Auxiliar de Tecnología	2	1	3	2	Medio
Auxiliar Operativo	2	1	3	2	Medio
Programador	1	1	3	2	Medio
Coordinador de la Mesa de Ayuda	2	1	3	2	Medio
Técnicos de sistemas	1	1	3	2	Medio

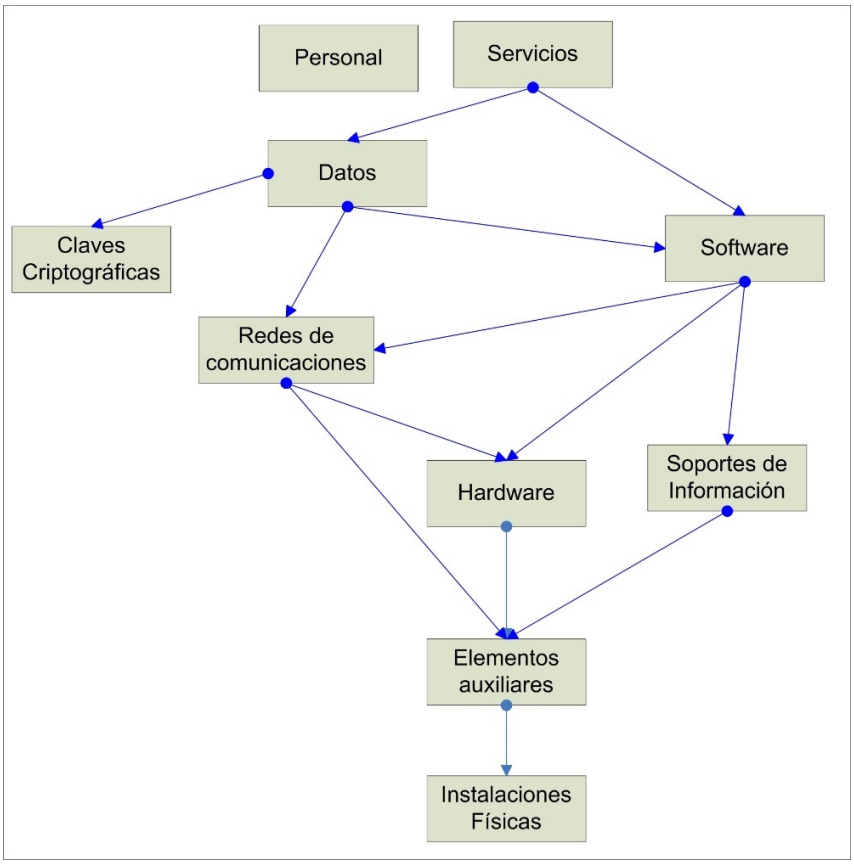
Fuente: Elaboración propia

La metodología Magerit propone que se identifique la dependencia entre activos, es decir, la relación existente entre activos que dependen unos de otros. De acuerdo a lo identificado todos se encuentra muy estrechamente ligados entre sí. Esto indica que cualquier vulnerabilidad de un activo que sea atacada repercutirá en mayor o menor medida en muchos de los demás activos.

En este caso sobre todo lo referente a los equipos servidores, SAN y conexiones de red que soportan toda la infraestructura tecnológica, que es la base del normal desarrollo de los demás sistemas.

En la siguiente figura se puede observar la jerarquía existente entre los activos de información de la Dirección de Tecnología de la Cámara de Comercio de Cúcuta.

Figura 3. Árbol de dependencia de activos



Fuente: Elaboración propia

3.3.3 Fase 3. Determinación de los riesgos que afectan la seguridad de la información en los activos críticos de la Unidad de Tecnología de la cámara de comercio de Cúcuta, aplicando los criterios de valoración de probabilidad por impacto.

La metodología Magerit propone realizar el análisis de riesgos siguiendo cinco pasos:

- Identificar los activos de información que son más relevantes para la organización
- Identificar las amenazas a las que están expuestos los activos.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.
- Determinar las salvaguardas o controles existentes para afrontar riesgos. 27

Actividad 1. Identificar los activos de información que son más relevantes para la organización

Los activos de información de la Dirección de Tecnología a seleccionar para el análisis de riesgos son aquellos que tienen nivel de criticidad medio y alto. También se realiza una agrupación de los activos de acuerdo a su funcionalidad, quedando el listado de activos para análisis de riesgos como se observa en la siguiente tabla:

[27] GOBIERNO DE ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Catálogo de Elementos. Madrid: El Ministerio. 2012. 127 p.

Tabla 10. Listado de Activos más relevantes

Nombre del Activo	Activo de información seleccionado para el Análisis de riesgos	Valor Cuantitativo
Tipo: [D] Datos		
Base de datos Mercurio	Bases de datos	Alto
Base de datos Worfkflow		Alto
Base de datos Docuware		Alto
Base de datos BPM		Alto
Base de datos SGD		Alto
Base de datos SII		Alto
Base de datos Censo		Alto
Base de datos SIREP		Medio
Base de datos Helpdesk		Alto
Base de datos Página Web		Alto
Backups de Máquinas virtuales	Backups	Medio
Backups de bases de datos		Medio
Manuales de contingencia	Documentación de los sistemas	Medio
Manuales de los sistemas		Medio
Documentos estandarizados TI		Medio
Logs de los sistemas	Logs de los sistemas	Medio
Tipo: [K] Claves criptográficas		
Firma Electrónica Secretaria General	Claves criptográficas	Alto
Firma electrónica Persona Jurídica		Alto
Firma electrónica DIAN		Alto
Firma de la sic		Alto
Código QR de BPM		Alto
Tipo: [SW] Servicios		
Directorio Activo - Autenticación	Directorio Activo - Autenticación	Medio
Telefonía IP	Telefonía IP	Medio
Página web	Página web	Medio
Mesa de ayuda	Mesa de ayuda	Medio
Intranet	Intranet	Medio
Correo electrónico	Correo electrónico	Medio
DNS	DNS	Medio

Tabla 10. (Continuación)

Nombre del Activo	Activo de información seleccionado para el Análisis de riesgos	Valor Cuantitativo
DHCP	DHCP	Medio
Sistema de Gestión Documental	Sistema de Gestión Documental	Alto
Sistema de Gestión Documental registros públicos	Sistema de Gestión Documental registros públicos	Alto
Sistema de Registros Públicos	Sistema de Registros Públicos	Alto
Sistema de Gestión Administrativa y Financiera	Sistema de Gestión Administrativa y Financiera	Alto
Almacenamiento en la nube Amazon		Alto
Almacenamiento en la nube Azure	Almacenamientos en la nube	Medio
Almacenamiento en la nube Onedrive		Alto
Tipo: [SW] Software		
Sistemas operativos	Sistemas operativos	Medio
Software de gestión y administración Bases de datos	Software de gestión y administración Bases de datos	Alto
Antivirus	Antivirus	Medio
Software de gestión y administración de backups	Software de gestión y administración de backups	Medio
Software de administración Plataforma Tecnológica	Software de administración Plataforma Tecnológica	Medio
Software de virtualización	Software de virtualización	Medio
Plataforma OFFICE 365	Plataforma OFFICE 365	Medio
Software de sincronización usuarios office 365	Software de sincronización usuarios office 365	Medio
Firewall Seguridad perimetral	Firewall Seguridad perimetral	Medio
Tipo: [HW] Hardware		
Servidores	Servidores	Alto
Almacenamientos	Almacenamientos	Alto
Portátiles	Portátiles	Medio

Tabla 10. (Continuación)

Nombre del Activo	Activo de información seleccionado para el Análisis de riesgos	Valor Cuantitativo
Switches	Switches	Medio
Tipo: [COM] Redes de comunicaciones		
Red LAN	Red LAN	Alto
Red Wifi	Red Wifi	Medio
Red LAN extendida (sedes)	Canales de comunicación contratados	Alto
Internet		Medio
Canal SIP Telefonía IP		Medio
Tipo: [Media] Soportes de información		
Discos Duros Externos	Discos Duros Externos	Medio
Tipo: [AUX] Elementos auxiliares		
UPS en Centros datos	UPS en Centros datos	Medio
Cableado estructurado	Cableado estructurado	Medio
Tipo: [L] Instalaciones físicas		
Centros de Datos	Centros de Datos	Alto
Tipo: [P] Personal		
Director TI	Talento Humano	Medio
Profesional de Tecnología		Medio
Profesional Junior de Redes y seguridad		Medio
Profesional Junior de Tecnología		Medio
Asistente de Tecnología		Medio
Ingeniera de Desarrollo		Medio
Auxiliar de Tecnología		Medio
Auxiliar Operativo		Medio
Programador		Medio
Coordinador de la Mesa de Ayuda		Medio
Técnicos de sistemas		Medio

Fuente: Elaboración propia

Actividad 2. Identificar las amenazas a las que están expuestos los activos.

Las amenazas es todo aquello que puede causar daño a un activo. Magerit en su Catálogo de elementos publicado en el libro 2 relaciona un listado de amenazas clasificándolas de acuerdo a su origen. Las categorías son:

- De origen natural o desastres naturales. Corresponde a todas aquellas amenazas que provienen de la naturaleza, tales como terremotos, incendios, inundaciones, huracanes.
- De origen industrial o del entorno. Corresponde a todas aquellas amenazas que son de tipo accidental o deliberada, que se originan de la actividad humana de tipo industrial, como incendios provocados, fugas de agua, explosiones, sobrecargas eléctricas, etc.
- Errores y fallos no intencionados. Corresponde a todas aquellas amenazas que son originadas por el mal uso de los activos ya sea por desconocimiento o por un error involuntario.
- Ataques intencionados. Corresponde a todas aquellas amenazas que son originadas por personas con la intención de dañar o deteriorar los activos de información.

Tabla 11. Listado de amenazas

Ítem	Amenaza
[N] Desastres naturales	
1	[N.1] Fuego
2	[N.2] Daños por agua
3	[N.*] Desastres naturales
[I] De origen industrial	
5	[I.1] Fuego
6	[I.2] Daños por agua
7	[I.*] Desastres industriales
8	[I.3] Contaminación mecánica
9	[I.4] Contaminación electromagnética
10	[I.5] Avería de origen físico o lógico
11	[I.6] Corte del suministro eléctrico
12	[I.7] Condiciones inadecuadas de temperatura o humedad
13	[I.8] Fallo de servicios de comunicaciones
14	[I.9] Interrupción de otros servicios y suministros esenciales

Tabla 11. (Continuación)

Ítem	Amenaza
15	[I.10] Degradación de los soportes de almacenamiento de la información
16	[I.11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados	
17	[E.1] Errores de los usuarios
18	[E.2] Errores del administrador
19	[E.3] Errores de monitorización (log)
20	[E.4] Errores de configuración
21	[E.7] Deficiencias en la organización
22	[E.8] Difusión de software dañino
23	[E.9] Errores de [re-]encaminamiento
24	[E.10] Errores de secuencia
25	[E.14] Escapes de información
26	[E.15] Alteración accidental de la información
27	[E.18] Destrucción de información
28	[E.19] Fugas de información
29	[E.20] Vulnerabilidades de los programas (software)
30	[E.21] Errores de mantenimiento / actualización de programas (software)
31	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
32	[E.24] Caída del sistema por agotamiento de recursos
33	[E.25] Pérdida de equipos
34	[E.28] Indisponibilidad del personal
[A] Ataques intencionados	
35	[A.3] Manipulación de los registros de actividad (log)
36	[A.4] Manipulación de la configuración
37	[A.5] Suplantación de la identidad del usuario
38	[A.6] Abuso de privilegios de acceso
39	[A.7] Uso no previsto
40	[A.8] Difusión de software dañino
41	[A.9] [Re-]encaminamiento de mensajes
42	[A.10] Alteración de secuencia
43	[A.11] Acceso no autorizado
44	[A.12] Análisis de tráfico
45	[A.13] Repudio
46	[A.14] Interceptación de información (escucha)
47	[A.15] Modificación deliberada de la información

Tabla 11. (Continuación)

Ítem	Amenaza
48	[A.18] Destrucción de información
49	[A.19] Divulgación de información
50	[A.22] Manipulación de programas
51	[A.23] Manipulación de los equipos
52	[A.24] Denegación de servicio
53	[A.25] Robo
54	[A.26] Ataque destructivo
55	[A.27] Ocupación enemiga
56	[A.28] Indisponibilidad del personal
57	[A.29] Extorsión
58	[A.30] Ingeniería social (picaresca)

Fuente: GOBIERNO DE ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Catálogo de Elementos. Madrid: El Ministerio. 2012. 127 p.

Actividad 3. Valoración de las amenazas.

No todas las amenazas afectan a todos los activos de información, ni tampoco lo hacen en igual medida para todas las dimensiones de seguridad. Es por esto que se determina para cada activo cuales amenazas pueden perjudicarlo, y valorar el nivel de afectación del activo.

Para esta valoración se tienen en cuenta dos dimensiones: El impacto y la probabilidad.

Probabilidad: Se analiza que tan probable es que la amenaza se pueda materializar, de acuerdo a la siguiente tabla. En este caso se puede analizar de acuerdo a la categoría o la frecuencia.

Tabla 12. Nivel de probabilidad de ocurrencia de la amenaza

	Nomenclatura	Categoría	Frecuencia	Valoración
Probabilidad	MA	Prácticamente seguro	A diario	5
	A	Probable	Mensualmente	4
	M	Posible	Una vez al año	3
	B	Poco probable	Cada varios años	2
	MB	Muy raro	Siglos	1

Fuente: Elaboración propia

Impacto: Se analiza cuál sería el impacto o degradación del activo ante la amenaza, de acuerdo a la siguiente tabla:

Tabla 13. Nivel de impacto de la amenaza sobre el activo

	Nomenclatura	Categoría	Valoración
Impacto	MA	Muy Alto	5
	A	Alto	4
	M	Medio	3
	B	Bajo	2
	MB	Muy Bajo	1

Fuente: Elaboración propia

Actividad 4. Valoración del riesgo.

Magerit define riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, podremos conocer el riesgo teniendo en cuenta la probabilidad de ocurrencia.

Un riesgo es mayor en la medida que su impacto y su probabilidad sean altas, y el riesgo será menos cuando el impacto y su probabilidad sean bajas.

En otras palabras podemos definir que el riesgo se calcula de la siguiente manera:

Riesgo = Impacto x Probabilidad

Para la valoración de los riesgos se utiliza la siguiente tabla donde:

- Nivel Crítico: Son riesgos que pueden ocurrir con mucha frecuencia y la afectación de los activos es alta.
- Nivel Alto: Son riesgos que pueden ocurrir con frecuencia y la afectación de los activos es moderada.
- Nivel Medio: Son riesgos que pueden ocurrir esporádicamente y la afectación de los activos es media.
- Nivel Bajo: Son riesgos que no ocurren con mucha frecuencia y la afectación en los activos es baja.
- Nivel Despreciable: Son riesgos cuya frecuencia y afectación son lo suficientemente bajos como para no tomarlos en cuenta para un tratamiento de riesgos.

Tabla 14. Niveles de valoración del riesgo

	Nomenclatura	Categoría	Valoración
Valoración del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Medio	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: Elaboración propia

A continuación se presenta la matriz de valoración de riesgos para los activos de información de la Dirección de Tecnología de la Cámara de Comercio de Cúcuta:

Tabla 15. Matriz de Valoración de riesgos

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
		D	I	C			
Bases de datos	[I.9] Interrupción de otros servicios y suministros esenciales	5	2	2	M	B	BAJO
	[I.10] Degradación de los soportes de almacenamiento de la información	5	1	1	B	M	BAJO
	[E.2] Errores del administrador	3	4	4	A	B	BAJO
	[E.3] Errores de monitorización (log)	3	2	4	M	B	BAJO
	[E.4] Errores de configuración	4	2	5	A	M	MEDIO
	[E.14] Escapes de información	2	2	5	M	M	BAJO
	[E.15] Alteración accidental de la información	2	5	5	A	B	BAJO
	[E.18] Destrucción de información	5	5	5	MA	B	MEDIO
	[E.19] Fugas de información	2	3	5	M	M	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	2	2	M	M	BAJO
	[E.24] Caída del sistema por agotamiento de recursos	4	2	2	M	M	BAJO
	[A.3] Manipulación de los registros de actividad (log)	2	5	4	A	B	BAJO
	[A.4] Manipulación de la configuración	4	5	5	MA	B	MEDIO
	[A.5] Suplantación de la identidad del usuario	2	5	5	A	B	BAJO
	[A.11] Acceso no autorizado	2	3	5	M	M	BAJO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Backups	[A.15] Modificación deliberada de la información	2	5	3	M	M	BAJO
	[A.18] Destrucción de información	5	5	5	MA	B	MEDIO
	[A.19] Divulgación de información	2	5	5	A	B	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	A	M	MEDIO
	[I.10] Degradación de los soportes de almacenamiento de la información	5	5	2	A	B	BAJO
	[E.2] Errores del administrador	4	4	3	A	M	MEDIO
	[E.7] Deficiencias en la organización	4	2	4	M	M	BAJO
	[E.14] Escapes de información	2	2	5	M	M	BAJO
	[E.15] Alteración accidental de la información	5	5	3	A	B	BAJO
	[E.18] Destrucción de información	5	2	2	M	B	BAJO
	[E.19] Fugas de información	2	2	5	M	A	MEDIO
	[E.28] Indisponibilidad del personal	5	2	2	M	M	BAJO
	[A.18] Destrucción de información	5	3	3	A	M	MEDIO
	[A.19] Divulgación de información	3	2	5	M	M	BAJO
	[A.28] Indisponibilidad del personal	5	2	2	M	B	BAJO
	[I.8] Fallo de servicios de comunicaciones	5	1	2	M	B	BAJO
Documentación de los sistemas	[E.2] Errores del administrador	5	4	4	A	MA	IMPORTANTE
	[E.7] Deficiencias en la organización	5	4	4	A	MA	IMPORTANTE
	[E.14] Escapes de información	3	2	5	M	M	BAJO
	[E.18] Destrucción de información	5	2	3	M	M	BAJO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
	[E.19] Fugas de información	3	2	5	M	M	BAJO
	[A.15] Modificación deliberada de la información	4	4	5	A	B	BAJO
	[A.18] Destrucción de información	4	-	-	A	B	BAJO
	[A.19] Divulgación de información	3	2	5	M	M	BAJO
	[A.28] Indisponibilidad del personal	4	3	3	M	M	BAJO
	[E.2] Errores del administrador	4	-	4	A	A	IMPORTANTE
	[E.3] Errores de monitorización (log)	4	-	-	A	A	IMPORTANTE
	[E.4] Errores de configuración	4	4	-	A	A	IMPORTANTE
	[E.7] Deficiencias en la organización	4	4	4	A	MA	IMPORTANTE
	[E.15] Alteración accidental de la información	-	4	-	A	M	MEDIO
Logs de los sistemas	[E.18] Destrucción de información	3	3	-	M	M	BAJO
	[E.19] Fugas de información	-	-	3	M	M	BAJO
	[A.3] Manipulación de los registros de actividad (log)	-	4	-	A	B	BAJO
	[A.4] Manipulación de la configuración	4	4	-	A	M	MEDIO
	[A.15] Modificación deliberada de la información	-	4	-	A	M	MEDIO
	[A.18] Destrucción de información	5	-	-	MA	M	MEDIO
	[E.1] Errores de los usuarios	-	-	2	B	A	BAJO
	[E.2] Errores del administrador	4	4	3	A	A	IMPORTANTE
Claves criptográficas	[E.14] Escapes de información	-	-	4	A	M	MEDIO
	[E.15] Alteración accidental de la información	-	2	-	B	M	BAJO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Directorio Activo - Autenticación	[E.18] Destrucción de información	3	-	-	M	M	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	A	A	IMPORTANTE
	[A.5] Suplantación de la identidad del usuario	5	5	5	MA	A	IMPORTANTE
	[A.18] Destrucción de información	5	-	-	MA	M	MEDIO
	[E.2] Errores del administrador	3	3	3	M	M	BAJO
	[E.4] Errores de configuración	3	2	-	M	M	BAJO
	[E.15] Alteración accidental de la información	3	3	-	M	M	BAJO
	[E.20] Vulnerabilidades de los programas (software)	3	3	-	M	M	BAJO
	[E.28] Indisponibilidad del personal	3	-	-	M	M	BAJO
	[A.4] Manipulación de la configuración	-	5	-	MA	M	MEDIO
	[A.6] Abuso de privilegios de acceso	-	5	5	MA	M	MEDIO
	[A.11] Acceso no autorizado	-	4	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	5	5	-	MA	B	MEDIO
	[A.18] Destrucción de información	5	5	-	MA	B	MEDIO
	[A.19] Divulgación de información	-	-	4	A	B	BAJO
Telefonía IP	[I.5] Avería de origen físico o lógico	5	-	-	MA	MA	CRITICO
	[I.6] Corte del suministro eléctrico	4	-	-	A	M	MEDIO
	[I.7] Condiciones inadecuadas de temperatura o humedad	4	-	-	A	B	BAJO
	[I.8] Fallo de servicios de comunicaciones	5	-	-	MA	B	MEDIO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
	[E.2] Errores del administrador	4	3	-	A	B	BAJO
	[E.4] Errores de configuración	4	3	-	A	B	BAJO
	[E.9] Errores de [re-]encaminamiento	4	-	-	A	B	BAJO
	[E.15] Alteración accidental de la información	2	3		M	B	BAJO
	[E.18] Destrucción de información	3	5	-	A	B	BAJO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	-	-	A	M	MEDIO
	[E.25] Pérdida de equipos	5	-	-	MA	B	MEDIO
	[E.28] Indisponibilidad del personal	2	-	-	B	A	BAJO
	[A.4] Manipulación de la configuración	5	5	5	MA	B	MEDIO
	[A.6] Abuso de privilegios de acceso	-	-	4	A	B	BAJO
	[A.11] Acceso no autorizado	4	4	5	A	B	BAJO
	[A.14] Interceptación de información (escucha)	-	-	5	MA	B	MEDIO
	[A.18] Destrucción de información	4	4	-	A	B	BAJO
	[A.19] Divulgación de información	-	-	4	A	B	BAJO
	[A.23] Manipulación de los equipos	4	-	-	A	B	BAJO
	[A.25] Robo	5	-	-	MA	B	MEDIO
Página web	[E.2] Errores del administrador	3	3	-	M	M	BAJO
	[E.4] Errores de configuración	3	3	-	M	M	BAJO
	[E.15] Alteración accidental de la información	3	5	-	A	B	BAJO
	[E.18] Destrucción de información	5	3	-	A	B	BAJO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
	[E.19] Fugas de información	-	-	4	A	B	BAJO
	[E.20] Vulnerabilidades de los programas (software)	5	-	-	MA	A	IMPORTANTE
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	-	-	MA	A	IMPORTANTE
	[E.28] Indisponibilidad del personal	5	-	-	MA	M	MEDIO
	[A.4] Manipulación de la configuración	-	5	-	MA	B	MEDIO
	[A.6] Abuso de privilegios de acceso	-	-	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	3	3	3	M	B	BAJO
	[A18] Destrucción de información	4	4	-	A	B	BAJO
	[A19] Divulgación de información	-	-	4	A	B	BAJO
	[A.24] Denegación de servicio	5	-	-	MA	B	MEDIO
	[E.2] Errores del administrador	3	3	-	M	M	BAJO
	[E.4] Errores de configuración	3	3	-	M	M	BAJO
	[E.15] Alteración accidental de la información	3	5	-	A	B	BAJO
	[E.18] Destrucción de información	5	3	-	A	B	BAJO
Mesa de ayuda	[E.19] Fugas de información	-	-	4	A	B	BAJO
	[E.20] Vulnerabilidades de los programas (software)	5	-	-	MA	MA	CRITICO
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	-	-	MA	MA	CRITICO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Intranet	[E.28] Indisponibilidad del personal	3	-	-	M	M	BAJO
	[A.4] Manipulación de la configuración	-	5	-	MA	B	MEDIO
	[A.6] Abuso de privilegios de acceso	-	-	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	3	3	3	M	B	BAJO
	[A18] Destrucción de información	4	4	-	A	B	BAJO
	[A19] Divulgación de información	-	-	4	A	B	BAJO
	[E.2] Errores del administrador	3	3	-	M	M	BAJO
	[E.4] Errores de configuración	3	3	-	M	M	BAJO
	[E.15] Alteración accidental de la información	3	5	-	A	B	BAJO
	[E.18] Destrucción de información	5	3	-	A	B	BAJO
	[E.19] Fugas de información	-	-	4	A	B	BAJO
	[E.20] Vulnerabilidades de los programas (software)	4	-	-	A	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	A	B	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	A	M	MEDIO
	[A.4] Manipulación de la configuración	-	4	-	A	B	BAJO
	[A.15] Modificación deliberada de la información	3	5	5	A	B	BAJO
	[A18] Destrucción de información	4	4	-	A	B	BAJO
	[A19] Divulgación de información	-	-	4	A	B	BAJO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Correo electrónico	[E.8] Difusión de software dañino	3	3	3	M	M	BAJO
	[E.19] Fugas de información	-	-	5	MA	A	IMPORTANTE
	[E.28] Indisponibilidad del personal	4	-	-	A	M	MEDIO
	[A.7] Uso no previsto	3	3	5	A	MA	IMPORTANTE
	[A.8] Difusión de software dañino	4	4	4	A	M	MEDIO
	[A30] Ingeniería social (picaresca)	-	-	4	A	MA	IMPORTANTE
DNS	[E.2] Errores del administrador	3	3	3	M	M	BAJO
	[E.3] Errores de monitorización (log)	3	-	-	M	M	BAJO
	[E.4] Errores de configuración	4	-	-	A	B	BAJO
	[E.15] Alteración accidental de la información	4	4	-	A	B	BAJO
	[E.20] Vulnerabilidades de los programas (software)	4	-	-	A	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	A	M	MEDIO
	[E.24] Caída del sistema por agotamiento de recursos	5	-	-	MA	M	MEDIO
	[E.28] Indisponibilidad del personal	3	-	-	M	M	BAJO
	[A.6] Abuso de privilegios de acceso	-	-	4	A	B	BAJO
	[A24] Denegación de servicio	5	-	-	MA	B	MEDIO
DHCP	[E.2] Errores del administrador	3	3	3	M	M	BAJO
	[E.3] Errores de monitorización (log)	3	-	-	M	M	BAJO
	[E.4] Errores de configuración	4	-	-	A	B	BAJO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Sistema de Gestión Documental	[E.15] Alteración accidental de la información	4	4	-	A	B	BAJO
	[E.20] Vulnerabilidades de los programas (software)	4	-	-	A	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	3	-	-	M	M	BAJO
	[E.24] Caída del sistema por agotamiento de recursos	3	-	-	M	M	BAJO
	[E.28] Indisponibilidad del personal	3	-	-	M	M	BAJO
	[A.6] Abuso de privilegios de acceso	-	-	4	A	B	BAJO
	[A24] Denegación de servicio	5	-	-	MA	B	MEDIO
	[E.1] Errores de los usuarios	-	3	-	M	MA	MEDIO
	[E.2] Errores del administrador	3	3	-	M	M	BAJO
	[E.4] Errores de configuración	3	3	3	M	A	MEDIO
	[E.14] Escapes de información	-	-	4	A	A	IMPORTANTE
	[E.15] Alteración accidental de la información	-	4	-	A	B	BAJO
	[E.18] Destrucción de información	5	-	-	MA	B	MEDIO
	[E.19] Fugas de información	-	-	5	MA	B	MEDIO
	[E.20] Vulnerabilidades de los programas (software)	-	4	4	A	A	IMPORTANTE
	[E.21] Errores de mantenimiento / actualización de programas (software)	-	4	-	A	A	IMPORTANTE

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Sistema de Gestión Documental registros públicos	[E.28] Indisponibilidad del personal	3	-	-	M	M	BAJO
	[A.4] Manipulación de la configuración	5	3	-	A	M	MEDIO
	[A.6] Abuso de privilegios de acceso	4	4	4	A	B	BAJO
	[A.11] Acceso no autorizado	4	4	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	4	4	4	A	B	BAJO
	[A18] Destrucción de información	4	4	4	A	B	BAJO
	[A19] Divulgación de información	4	4	4	A	B	BAJO
	[A22] Manipulación de programas	4	4	4	A	B	BAJO
	[E.1] Errores de los usuarios	-	3	-	M	MA	MEDIO
	[E.2] Errores del administrador	3	3	-	M	M	BAJO
	[E.4] Errores de configuración	3	3	3	M	A	MEDIO
	[E.14] Escapes de información	-	-	4	A	A	IMPORTANTE
	[E.15] Alteración accidental de la información	-	4	-	A	M	MEDIO
	[E.18] Destrucción de información	5	-	-	MA	M	MEDIO
	[E.19] Fugas de información	-	-	5	MA	M	MEDIO
	[E.20] Vulnerabilidades de los programas (software)	-	4	4	A	A	IMPORTANTE
	[E.21] Errores de mantenimiento / actualización de programas (software)	-	4	-	A	A	IMPORTANTE
	[E.28] Indisponibilidad del personal	3	-	-	M	M	BAJO
	[A.4] Manipulación de la configuración	5	3	-	A	M	MEDIO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Sistema de Registros Públicos	[A.6] Abuso de privilegios de acceso	4	4	4	A	B	BAJO
	[A.11] Acceso no autorizado	4	4	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	4	4	4	A	B	BAJO
	[A18] Destrucción de información	4	4	4	A	B	BAJO
	[A19] Divulgación de información	4	4	4	A	B	BAJO
	[A22] Manipulación de programas	4	4	4	A	B	BAJO
	[E.1] Errores de los usuarios	-	3	-	M	MA	MEDIO
	[E.2] Errores del administrador	3	3	-	M	M	BAJO
	[E.4] Errores de configuración	3	3	3	M	A	MEDIO
	[E.14] Escapes de información	-	-	4	A	A	IMPORTANTE
	[E.15] Alteración accidental de la información	-	4	-	A	M	MEDIO
	[E.18] Destrucción de información	5	-	-	MA	B	MEDIO
	[E.19] Fugas de información	-	-	5	MA	M	MEDIO
	[E.20] Vulnerabilidades de los programas (software)	-	4	4	A	B	BAJO
	[E.28] Indisponibilidad del personal	3	-	-	M	M	BAJO
	[A.4] Manipulación de la configuración	5	3	-	A	B	BAJO
	[A.6] Abuso de privilegios de acceso	4	4	4	A	B	BAJO
	[A.11] Acceso no autorizado	4	4	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	4	4	4	A	B	BAJO
	[A18] Destrucción de información	4	4	4	A	B	BAJO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Sistema de Gestión Administrativa y Financiera	[A19] Divulgación de información	4	4	4	A	B	BAJO
	[A22] Manipulación de programas	4	4	4	A	B	BAJO
	[E.1] Errores de los usuarios	-	3	-	M	M	BAJO
	[E.2] Errores del administrador	3	3	-	M	M	BAJO
	[E.4] Errores de configuración	3	3	3	M	A	MEDIO
	[E.14] Escapes de información	-	-	4	A	A	IMPORTANTE
	[E.15] Alteración accidental de la información	-	4	-	A	M	MEDIO
	[E.18] Destrucción de información	5	-	-	MA	M	MEDIO
	[E.19] Fugas de información	-	-	5	MA	M	MEDIO
	[E.21] Errores de mantenimiento / actualización de programas (software)	-	4	-	A	A	IMPORTANTE
	[E.28] Indisponibilidad del personal	3	-	-	M	M	BAJO
	[A.4] Manipulación de la configuración	5	3	-	A	B	BAJO
	[A.6] Abuso de privilegios de acceso	4	4	4	A	B	BAJO
	[A.11] Acceso no autorizado	4	4	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	4	4	4	A	B	BAJO
	[A18] Destrucción de información	4	4	4	A	B	BAJO
	[A19] Divulgación de información	4	4	4	A	B	BAJO
	[A22] Manipulación de programas	4	4	4	A	B	BAJO
Almacenamientos en la nube	[I.8] Fallo de servicios de comunicaciones	5	-	-	MA	A	IMPORTANTE
	[E.1] Errores de los usuarios	3	-	-	M	M	BAJO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
	[E.2] Errores del administrador	4	-	-	A	B	BAJO
	[E.14] Escapes de información	-	-	4	A	B	BAJO
	[E.15] Alteración accidental de la información	-	4	-	A	B	BAJO
	[E.18] Destrucción de información	2	3	-	M	B	BAJO
	[E.19] Fugas de información	-	-	5	MA	B	MEDIO
	[A.11] Acceso no autorizado	-	-	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	-	4	-	A	B	BAJO
	[A18] Destrucción de información	4	4	-	A	B	BAJO
	[A19] Divulgación de información	-	-	4	A	B	BAJO
	[A24] Denegación de servicio	4	-	-	A	M	MEDIO
	[E.4] Errores de configuración	4	4	-	A	B	BAJO
	[E.8] Difusión de software dañino	4	4	-	A	B	BAJO
Sistemas operativos	[E.20] Vulnerabilidades de los programas (software)	5	5	-	MA	B	MEDIO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	A	B	BAJO
	[E.2] Errores del administrador	4	4	-	A	B	BAJO
Software de gestión y administración	[E.4] Errores de configuración	4	4	-	A	B	BAJO
Bases de datos	[E.20] Vulnerabilidades de los programas (software)	4	-	-	A	M	MEDIO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Antivirus	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	A	M	MEDIO
	[E.28] Indisponibilidad del personal	3	-	-	M	M	BAJO
	[A.4] Manipulación de la configuración	-	5	-	MA	B	MEDIO
	[A.6] Abuso de privilegios de acceso	4	-	-	A	B	BAJO
	[E.2] Errores del administrador	3	-	-	M	M	BAJO
	[E.4] Errores de configuración	3	-	-	M	M	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	3	-	-	M	M	BAJO
	[E.2] Errores del administrador	3	3	-	M	M	BAJO
	[E.4] Errores de configuración	3	3	-	M	M	BAJO
Software de gestión y administración de backups	[E.15] Alteración accidental de la información	5	5	-	MA	B	MEDIO
	[E.18] Destrucción de información	5	3	-	A	B	BAJO
	[E.20] Vulnerabilidades de los programas (software)	4	-	-	A	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	A	B	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	A	M	MEDIO
	[A.4] Manipulación de la configuración	5	5	-	MA	B	MEDIO
	[A.6] Abuso de privilegios de acceso	-	-	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	3	3	3	M	B	BAJO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Software de administración Plataforma Tecnológica	[A18] Destrucción de información	4	4	-	A	B	BAJO
	[A19] Divulgación de información	-	-	4	A	B	BAJO
	[E.2] Errores del administrador	3	3	-	M	M	BAJO
	[E.4] Errores de configuración	3	3	-	M	M	BAJO
	[E.15] Alteración accidental de la información	5	5	-	MA	B	MEDIO
	[E.18] Destrucción de información	5	3	-	A	B	BAJO
	[E.20] Vulnerabilidades de los programas (software)	4	-	-	A	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	A	B	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	A	M	MEDIO
	[A.4] Manipulación de la configuración	5	5	-	MA	B	MEDIO
	[A.6] Abuso de privilegios de acceso	-	-	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	3	3	3	M	B	BAJO
Software de virtualización	[A18] Destrucción de información	4	4	-	A	B	BAJO
	[A19] Divulgación de información	-	-	4	A	B	BAJO
	[E.2] Errores del administrador	3	3	-	M	M	BAJO
	[E.4] Errores de configuración	3	3	-	M	M	BAJO
	[E.15] Alteración accidental de la información	5	5	-	MA	B	MEDIO
	[E.18] Destrucción de información	5	3	-	A	B	BAJO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Plataforma OFFICE 365	[E.20] Vulnerabilidades de los programas (software)	4	-	-	A	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	A	B	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	A	M	MEDIO
	[A.4] Manipulación de la configuración	5	5	-	MA	B	MEDIO
	[A.6] Abuso de privilegios de acceso	-	-	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	3	3	3	M	B	BAJO
	[A18] Destrucción de información	4	4	-	A	B	BAJO
	[A19] Divulgación de información	-	-	4	A	B	BAJO
	[I.8] Fallo de servicios de comunicaciones	5	-	-	MA	A	IMPORTANTE
	[E.1] Errores de los usuarios	3	-	-	M	M	BAJO
	[E.2] Errores del administrador	4	-	-	A	B	BAJO
	[E.24] Caída del sistema por agotamiento de recursos	4	-	-	A	B	BAJO
	[A.11] Acceso no autorizado	-	-	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	-	4	-	A	B	BAJO
Software de sincronización usuarios office 365	[E.2] Errores del administrador	3	3	-	M	M	BAJO
	[E.4] Errores de configuración	3	3	-	M	M	BAJO
	[I.8] Fallo de servicios de comunicaciones	5	-	-	MA	A	IMPORTANTE

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Firewall Seguridad perimetral	[E.20] Vulnerabilidades de los programas (software)	4	-	-	A	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	A	B	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	A	M	MEDIO
	[A.4] Manipulación de la configuración	5	5	-	MA	B	MEDIO
	[A.6] Abuso de privilegios de acceso	-	-	4	A	B	BAJO
	[E.2] Errores del administrador	4	-	-	A	B	BAJO
	[E.4] Errores de configuración	-	4	-	A	B	BAJO
	[E.9] Errores de [re-]encaminamiento	-	4	-	A	B	BAJO
Servidores	[E.20] Vulnerabilidades de los programas (software)	3	3	-	M	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	3	3	-	M	B	BAJO
	[A.4] Manipulación de la configuración	-	3	-	M	B	BAJO
	[A.6] Abuso de privilegios de acceso	3	3	-	M	B	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	A	M	MEDIO
	[N.1] Fuego	5	-	-	MA	A	IMPORTANTE
	[N.2] Daños por agua	5	-	-	MA	MB	BAJO
	[N.*] Desastres naturales	5	-	-	MA	B	MEDIO
	[I.5] Avería de origen físico o lógico	4	-	-	A	B	BAJO
	[I.6] Corte del suministro eléctrico	5	-	-	MA	M	MEDIO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión	Impacto	Probabilidad	Nivel de Riesgo
Almacenamientos	[I.7] Condiciones inadecuadas de temperatura o humedad	5 - -	MA	M	MEDIO
	[A25] Robo	5 - -	MA	B	MEDIO
	[A26] Ataque destructivo	5 - -	MA	B	MEDIO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5 - -	MA	B	MEDIO
	[N.1] Fuego	5 - -	MA	A	IMPORTANTE
	[N.2] Daños por agua	5 - -	MA	MB	BAJO
	[N.*] Desastres naturales	5 - -	MA	B	MEDIO
	[I.5] Avería de origen físico o lógico	4 - -	A	B	BAJO
	[I.6] Corte del suministro eléctrico	5 - -	MA	M	MEDIO
	[I.7] Condiciones inadecuadas de temperatura o humedad	5 - -	MA	M	MEDIO
	[A25] Robo	5 - -	MA	B	MEDIO
	[A26] Ataque destructivo	5 - -	MA	B	MEDIO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5 - -	MA	B	MEDIO
	[N.1] Fuego	5 - -	MA	B	MEDIO
	[N.2] Daños por agua	5 - -	MA	MB	BAJO
	[N.*] Desastres naturales	5 - -	MA	B	MEDIO
	[I.5] Avería de origen físico o lógico	4 - -	A	B	BAJO
Portátiles	[I.6] Corte del suministro eléctrico	5 - -	MA	M	MEDIO
	[I.7] Condiciones inadecuadas de temperatura o humedad	5 - -	MA	M	MEDIO
	[A25] Robo	5 - 5	MA	A	IMPORTANTE

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Switches	[A26] Ataque destructivo	5	-	-	MA	B	MEDIO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	MA	B	MEDIO
	[E.19] Fugas de información			5	MA	A	IMPORTANTE
	[E.25] Pérdida de equipos			5	MA	A	IMPORTANTE
	[N.1] Fuego	5	-	-	MA	B	MEDIO
	[N.2] Daños por agua	5	-	-	MA	B	MEDIO
	[N.*] Desastres naturales	5	-	-	MA	MB	BAJO
	[I.5] Avería de origen físico o lógico	5	-	-	MA	M	MEDIO
	[I.6] Corte del suministro eléctrico	5			MA	M	MEDIO
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	-	-	MA	B	MEDIO
	[E.2] Errores del administrador	4	3	-	A	B	BAJO
	[E.4] Errores de configuración	4	3	-	A	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	A	MA	IMPORTANTE
	[E.25] Pérdida de equipos	5	-	5	MA	MB	BAJO
	[A.4] Manipulación de la configuración	4	3	-	A	B	BAJO
	[A.6] Abuso de privilegios de acceso	4	3	-	A	B	BAJO
	[A.11] Acceso no autorizado	4	3	-	A	B	BAJO
	[A.14] Interceptación de información (escucha)	2	2	4	M	M	BAJO
	[A.23] Manipulación de los equipos	5	5	-	MA	M	MEDIO
	[A.25] Robo	5	-	-	MA	B	MEDIO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión	Impacto	Probabilidad	Nivel de Riesgo
Red LAN	[E.2] Errores del administrador	4 - -	A	B	BAJO
	[E.3] Errores de monitorización (log)	4 - -	A	B	BAJO
	[E.9] Errores de [re-]encaminamiento	4 - -	A	B	BAJO
	[E.24] Caída del sistema por agotamiento de recursos	5 - -	MA	B	MEDIO
	[E.28] Indisponibilidad del personal	5 - -	MA	M	MEDIO
	[A.12] Análisis de tráfico	- - 5	MA	M	MEDIO
	[A.14] Interceptación de información (escucha)	- - 5	MA	B	MEDIO
Red Wifi	[E.2] Errores del administrador	4 - -	A	B	BAJO
	[E.3] Errores de monitorización (log)	4 - -	A	B	BAJO
	[E.9] Errores de [re-]encaminamiento	4 - -	A	B	BAJO
	[E.24] Caída del sistema por agotamiento de recursos	5 - -	MA	A	IMPORTANTE
	[E.28] Indisponibilidad del personal	5 - -	MA	M	MEDIO
	[A.12] Análisis de tráfico	- - 3	M	M	BAJO
	[A.14] Interceptación de información (escucha)	- - 5	MA	B	MEDIO
Canales de comunicación contratados	[E.2] Errores del administrador	4 - -	A	B	BAJO
	[E.3] Errores de monitorización (log)	4 - -	A	B	BAJO
	[E.9] Errores de [re-]encaminamiento	4 - -	A	B	BAJO
	[E.24] Caída del sistema por agotamiento de recursos	5 - -	MA	A	IMPORTANTE

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de Riesgo
Discos Duros Externos	[E.28] Indisponibilidad del personal	5	-	-	MA	M	MEDIO
	[A.12] Análisis de tráfico	-	-	5	MA	M	MEDIO
	[A.14] Interceptación de información (escucha)	-	-	5	MA	B	MEDIO
	[N.1] Fuego	5	-	-	MA	A	IMPORTANTE
	[N.2] Daños por agua	5	-	-	MA	MB	BAJO
	[I.5] Avería de origen físico o lógico	4	-	-	A	B	BAJO
	[I.7] Condiciones inadecuadas de temperatura o humedad	4	-	-	A	B	BAJO
	[A25] Robo	5	-	-	MA	A	IMPORTANTE
	[A26] Ataque destructivo	5	-	-	MA	M	MEDIO
UPS en Centros datos	[N.1] Fuego	5	-	-	MA	A	IMPORTANTE
	[N.2] Daños por agua	5	-	-	MA	MB	BAJO
	[I.5] Avería de origen físico o lógico	4	-	-	A	B	BAJO
	[I.7] Condiciones inadecuadas de temperatura o humedad	4	-	-	A	B	BAJO
	[A25] Robo	5	-	-	MA	A	IMPORTANTE
	[A26] Ataque destructivo	5	-	-	MA	B	MEDIO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	MA	M	MEDIO
Cableado estructurado	[N.2] Daños por agua	3	-	-	M	B	BAJO
	[I.11] Emanaciones electromagnéticas	4	-	-	A	B	BAJO
	[A26] Ataque destructivo	5	-	-	MA	B	MEDIO

Tabla 15. (Continuación)

Activo	Amenazas	Impacto en cada dimensión	Impacto	Probabilidad	Nivel de Riesgo
Centros de Datos	[N.1] Fuego	5 - -	MA	B	MEDIO
	[N.2] Daños por agua	4 - -	A	B	BAJO
	[N.*] Desastres naturales	5 - -	MA	MB	BAJO
	[I.1] Fuego	5 - -	MA	A	IMPORTANTE
	[A.11] Acceso no autorizado	5 - 5	MA	MA	CRITICO
Talento Humano	[E.28] Indisponibilidad del personal	5 - -	MA	A	IMPORTANTE
	[E.7] Deficiencias en la organización	4 - -	A	B	BAJO

Fuente: Elaboración propia

Actividad 5. Análisis de resultados de la matriz de riesgos.

Teniendo en cuenta los resultados obtenidos, se procede a realizar un análisis para determinar la manera como serán tratados.

La siguiente tabla define los niveles de tratamiento de riesgos:

Tabla 16. Tratamiento de riesgos

Nivel de Riesgo	Tratamiento del riesgo
Crítico	Se reduce o se mitiga el riesgo por medio de controles.
Importante	Se reduce o mitiga el riesgo por medio de controles preventivos.
Medio	Se transfiere el riesgo por ejemplo tomando un seguro.
Bajo	Finaliza el proceso.

Fuente: Elaboración propia

En la siguiente tabla se observa la cantidad de riesgos que quedaron en cada uno de los niveles explicados anteriormente:

Tabla 17. Distribución de amenazas según la valoración de su riesgo

		PROBABILIDAD				
RIESGO		**MB**	**B**	**M**	**A**	**MA**
IMPACTO	**MA**	8	51	27	20	4
	A	0	144	27	14	6
	M	0	17	64	5	3
	B	0	0	2	2	0
	MB	0	0	0	0	0

Fuente: Elaboración propia

A continuación se presenta el análisis realizado con respecto a aquellos riesgos de tipo crítico, importante y medio:

Nivel crítico:

Se evidencia que el Sistema de Telefonía IP actualmente no es una solución virtualizada sobre la plataforma *Vmware* que tiene la Cámara de Comercio de Cúcuta para todos sus servidores. Esto a raíz de unas fallas existentes de compatibilidad entre el software que existía anteriormente y el proveedor del canal de comunicación de la telefonía IP. El proveedor suministró una PBX que durante el tiempo que ha estado instalada ha presentado fallas, incluso ha sido cambiada varias veces por parte del proveedor, pues los recursos de la máquina no son suficientes para el número de extensiones y llamadas recurrentes. Al ser un dispositivo físico la probabilidad de una suspensión del servicio debido a una

avería o daño es mayor, y el impacto es alto al dejar a la Entidad sin el servicio de telefonía IP interna y externa hasta que sea reparada la máquina o reemplazada. No se cuenta con una contingencia para estos casos.

El software de registro de incidentes Glpi de la Mesa de Ayuda actualmente no se encuentra actualizado con la última versión disponible, debido a que no existe un contrato de soporte para la realización de esta actividad, ocasionando que se encuentre en operación con una versión del sistema que muy probablemente tenga vulnerabilidades que han sido resueltas con las actualizaciones. El Glpi presenta bloqueos constantes, sobre todo cuando se intenta consultar o generar algún tipo de reporte que conlleve muchos registros. Cuando estos bloqueos se presentan la aplicación deja de funcionar y queda indisponible hasta que es reiniciado por el administrador.

Los Centros de Datos y de Telecomunicaciones de la Cámara de Comercio de Cúcuta son las áreas donde se encuentran ubicados todos los dispositivos de la plataforma tecnológica de la Entidad, tanto del componente de servidores como de la red de datos, ambos cruciales para la disponibilidad de todos los sistemas que soportan la operación de la Entidad. No se lleva un registro de acceso a estos cuartos, y el seguro de las puertas es una cerradura común, sin contar con un dispositivo biométrico que permita controlar y llevar registro de los accesos a los cuartos. Las llaves de las puertas de los centros de datos y de telecomunicaciones se guardan en la oficina de la Dirección de Tecnología dentro de una gaveta cuya llave tiene copia la Directora de Tecnología y la Profesional Junior de Redes y Seguridad. Existe una muy alta probabilidad de que se presenten accesos no autorizados a estos cuartos de datos, pues las llaves son usadas por las personas que pertenecen a la Dirección de Tecnología, especialmente el personal de la mesa de ayuda, y por consiguiente la posibilidad de que se pueda crear una copia de las llaves es alta. El impacto si esto llegara a ocurrir es muy alto, pues como se explica, son sitios donde se concentran todos los dispositivos que forman la base tecnológica de la Entidad, y sólo debe ingresar personal autorizado y que se lleve un registro de los accesos permitirá hacer una trazabilidad en el caso de que exista algún suceso de seguridad en estos cuartos.

Nivel Importante:

Dentro del nivel importante se encuentran aquellos riesgos que pueden ser mitigados aplicando algún control, y que la materialización de los mismos puede ocasionar interrupciones de la operación de la Entidad. Dentro de esta categoría se encuentran que los Centros de Datos y de Telecomunicaciones no cuentan con un sistema preventivo que garantice que ante un incendio se pueda minimizar el impacto del daño al apagar la fuente del mismo. En el pasado ya la Entidad tuvo

un evento similar y esto hace que se catalogue este riesgo como posible. Los activos de información que se verían afectados son los servidores, almacenamientos, discos duros y UPS.

Se evidencia que la disponibilidad de los servicios de la nube de Microsoft y del Software SII puede verse afectada por fallos en los servicios de comunicaciones, pues su acceso se realiza a través de Internet. La probabilidad de que este riesgo se materialice es alta y el impacto es muy alto, pues son servicios que se necesitan para la operación diaria de la Entidad. La probabilidad que los canales de Internet contratados presenten una indisponibilidad es alta, teniendo en cuenta que en el caso del Sistema SII es netamente transaccional, cualquier mínima interrupción del servicio puede ocasionar que la conexión establecida se pierda y la operación se caiga.

Los activos que son más vulnerables a robos son los portátiles y discos duros externos de las copias de seguridad. La Cámara de Comercio tiene asegurados los portátiles en caso de robo, pero la información contenida dentro de ellos no se encuentra cifrada. Es importante mantener las pólizas de aseguramiento del hardware pero también es importante que se implemente un sistema de cifrado de la información para asegurar que en caso robo la información no pueda ser leída. En el caso de los discos duros externos que son usados para extraer las copias de seguridad tampoco se están cifrando su contenido, y en el caso de pérdida o robo la información puede ser de fácil acceso y lectura.

Actualmente el personal que labora para la Cámara de Comercio de Cúcuta, tanto empleados como contratistas no han recibido formación para la toma de conciencia apropiadas sobre el buen uso de los recursos informáticos y de los activos a su cargo. Esto lleva a que el riesgo de que exista escapes o fugas de información, o un mal uso de los recursos a su cargo sea probable y el impacto sea alto para la Entidad, incurriendo en incumplimientos legales y afectando la imagen de la organización. En este punto tampoco existe un proceso formal y comunicado a todos los miembros de la Cámara de Comercio de Cúcuta sobre las consecuencias y acciones que se tomarán contra empleados que hayan cometidos violaciones a la seguridad de la información.

Con respecto a la documentación que maneja la Dirección de Tecnología como manuales de contingencia, manuales de los sistemas y documentos estandarizados TI se evidencia que algunos no se encuentran actualizados de acuerdo a las últimas versiones o configuraciones de los sistemas, esto debido a que el personal de la Dirección de Tecnología no cuenta con el tiempo necesario y requerido para mantener esta documentación al día. Es muy probable que en el momento de requerirse algún manual de contingencia no se encuentre

actualizado, y el impacto de esto sería muy alto, pues supondría que en caso de requerir levantar algún servicio el tiempo que se tome sea mucho más alto que si la documentación se encontrara actualizada.

Enlazado con el punto anterior, el talento humano de la Dirección de Tecnología, aunque son profesionales con experiencia y conocimientos sobre las áreas que tienen asignadas a su cargo, es posible que ante la ausencia de uno de los profesionales no exista una persona totalmente capacitada para realizar las actividades de quien no se encuentra disponible. En los períodos de vacaciones programados previamente es posible que se entrene una persona que asuma estas funciones, adicionalmente a las que ya posee, pero en casos de incapacidades a veces se torna difícil estos reemplazos, pudiendo ocasionar demoras en la resolución de fallas o respuesta a requerimientos de otras gerencias.

Se evidencia que no existe una política de retención logs de los sistemas, y no se tiene configurado un servicio que permita centralizar los eventos y hacer una correlación de los mismos. Actualmente la Dirección de Tecnología maneja para cada sistema individualmente un registro de logs que cada administrador accede y consulta en el caso requerirse. Al no existir un tiempo durante el cual se deben mantener estos logs, los mismos a veces podrían no estar disponibles para su consulta, y no habría una política que respaldara el tiempo mínimo de retención. Esto podría ocasionar un impacto alto en la imagen de la Dirección de Tecnología y de la Cámara de Comercio de Cúcuta misma frente a entes externos que llegaran a solicitar este tipo de información. También se debe considerar la posibilidad de que los administradores comentan errores y se eliminen logs que posteriormente se pudiesen llegar a necesitar.

Algunos sistemas como la página web, el Sistema de Gestión Documental y el Sistema de Gestión Documental de Registros Públicos se encuentran desactualizados, y al no estar en las últimas versiones disponibles son vulnerables a amenazas de tipo software que afecten la disponibilidad del sistema para los usuarios.

Se evidencia que la red inalámbrica Wifi de la Cámara de Comercio de Cúcuta, administrada por la Dirección de Tecnología se encuentra en estado de obsolescencia, pues los equipos como *Access point y routers* inalámbricos sobre la cual se basa esta red son equipos de más de 5 años de operación y no cuentan con un contrato de soporte en caso de falla. Se presentan casos constantemente de indisponibilidad del servicio por agotamiento de recursos, siendo un riesgo probable de que ocurra con un impacto muy alto, pues algunas de las personas

que laboran como contratistas de la Entidad necesitan este recurso para acceder a los sistemas como correo electrónico e Internet.

Así mismo algunos equipos activos de la red de datos se encuentran en estado de obsolescencia y sin contrato de soporte técnico, sin acceso a actualizaciones, lo que implica una muy alta probabilidad de indisponibilidad de la red a causa de la falla de estos equipos, pues no habría forma de reponerlos rápidamente.

Nivel Medio:

En el caso de la administración del Directorio Activo, hay delegación de funciones en relación a los servicios configurados en ese servidor, tales como la administración de usuarios, políticas, DHCP y DNS Interno. Esto implica una administración compartida que puede conllevar al riesgo de abusos de privilegio de acceso o de manipulación accidental de la configuración, que podría tener un impacto muy alto en la integridad del activo y la confidencialidad de la información contenida en este sistema.

Se evidencia que para las UPS de los Centros de Datos y Telecomunicaciones no existe un plan de mantenimiento preventivo periódico que garantice su óptimo desempeño. De esta manera es posible que estos dispositivos dejen de operar y causen daños a los equipos que dependen de ella para su funcionamiento como Servidores, almacenamientos, *switches*, etc. Los activos como Servidores, almacenamientos, *switches*, etc. que dependen para su disponibilidad del suministro eléctrico tienen un riesgo posible con impacto muy alto de no estar disponibles a causa de estas interrupciones eléctricas.

También se constituye en un riesgo las Condiciones inadecuadas de temperatura o humedad, que, aunque en los centros de datos y telecomunicaciones existen aires acondicionados, no existen dispositivos para el control de humedad que puede afectar la integridad de servidores, almacenamientos, *switches*, etc.

Con respecto a los discos duros externos de las copias de seguridad, son dispositivos propensos a ser robados o destruidos en el trasporte al sitio externo donde son almacenados. No se evidencia que exista una cadena de custodia establecida claramente con responsabilidades definidas que garanticen que estos dispositivos se conserven adecuadamente.

Se evidencia que existe un riesgo de indisponibilidad de personal, sobre todo en caso de incapacidades porque no existe una persona en el área que cubra durante el tiempo de la ausencia y la carga laboral recae en algún compañero que asuma las funciones temporalmente. Esto se agrava por el hecho de no contar con la documentación de procedimientos y manuales para poder resolver fallas rápidamente.

Actividad 6. Documento de aplicabilidad.

El documento de declaración de aplicabilidad es un documento importante donde se define como se implementará gran parte de la seguridad de la información en una organización. En este documento se identifican los controles que se debieran implementar que fueron identificados en el análisis de riesgos y también aquellos controles que corresponden a obligaciones legales o contractuales de las organizaciones.

La presente declaración contiene los controles que son relevantes para la Cámara de Comercio de Cúcuta. Adicionalmente en ella se encuentran justificada la exclusión de algunos de los controles y se muestra el motivo de selección de los controles aplicables, entre los motivos de selección se pueden encontrar: resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo, requisitos legales o reglamentos, obligaciones contractuales y necesidades empresariales de la organización en materia de seguridad de la información.

Tabla 18. Declaración de aplicabilidad

CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)	Versión: 01

La presente declaración los controles que son relevantes para la Cámara de Comercio de Cúcuta. Adicionalmente en ella se encuentran justificada la exclusión de algunos de los controles y se muestra el motivo de selección de los controles aplicables, entre los motivos de selección se pueden encontrar: resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo, requisitos legales o reglamentos, obligaciones contractuales y necesidades empresariales de la organización en materia de seguridad de la información. LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas, RRA: resultado de la valoración de riesgos.									Elaboró: Ing. Carolina Duarte Martínez
Sección	Objetivo de control	Descripción del control ISO 27001:2013	Control implementado	Justificación de exclusión	Control Seleccionado	Razones de selección				Control planeado
						LR	CO	BR/ BP	RRA	
5 Políticas de Seguridad										
5,1	Dirección de la alta gerencia para la seguridad de la información									
5.1.1	Políticas de seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Políticas de seguridad de la información AF-GIT-06 v.2		SI	X		X		Definición de las Políticas de Seguridad de la Información en base al diagnóstico del estado actual y del análisis de riesgos.
5.1.2	Revisión de las políticas de seguridad de la información	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	No		SI	X		X		Realizar a intervalos planificados la revisión de la Política de Seguridad de la Información
6 Organización de la Seguridad de la Información										
6,1	Organización interna									
6.1.1	Roles y responsabilidad de seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	No		SI			X		Se deben definir los roles, responsabilidades y funciones relacionadas con la Seguridad de la Información, y asignar formalmente a los respectivos responsables.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)							Versión: 01
6.1.2	Segregación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	No	SI			X		Establecer y formalizar la estructura en la entidad teniendo en cuenta las actividades críticas que deben ser manejadas por diferentes niveles jerárquicos sobre Seguridad de la Información.
6.1.3	Contacto con autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	No	SI	X		X		Definir directriz apropiada para hacer contacto con autoridades relacionadas con la Seguridad de la Información en Colombia.
6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	No	SI			X		Definir una directriz apropiada para mantener contacto con entidades, empresas, universidades y demás para que el personal que está en Tecnología esté al tanto de nuevas amenazas, incidentes y posibles soluciones.
6.1.5	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	No	SI	X	X	X	X	Definir un procedimiento para la Gestión de proyectos que incluya que durante el ciclo de vida de un proyecto se debe velar por el cumplimiento de la Política de Seguridad de la Información, e identificar los riesgos de Seguridad de la Información para los activos de información involucrados en cada proyecto.
6,2	Dispositivos móviles y teletrabajo								

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)								Versión: 01
6.2.1	Política de dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	No		SI	X	X	X	X	Definir una política de manejo adecuado de dispositivos móviles, especificando los controles necesarios para su operación segura.
6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	NO	En la empresa no se tiene la modalidad de contratación de personal a través del teletrabajo.	No					
7 Seguridad en los Recursos Humanos										
7,1	Previo al empleo									
7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	SI		SI	X	X	X		Manual de procedimiento AF-TH-03 Vinculación de Personal
7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	No		SI	X	X	X		Establecer un Acuerdo de Confidencialidad, dentro del proceso de Gestión de Talento Humano y actualizar el reglamento interno de trabajo, con el que se rija el comportamiento de los empleados con respecto a la Información a la que tienen acceso y las consecuencias de cometer actos en contra de la seguridad de la misma.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)						Versión: 01
7,2	Durante el empleo							
7.2.1	Responsabilidades de la Dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	No	SI	X	X	X	Definir los procedimientos para exigir a los empleados y contratistas el cumplimiento de todas las políticas de Seguridad de la Información definidas.
7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	No	SI	X	X	X	Definir un Plan de Capacitación y Sensibilización sobre temas relacionados con la Seguridad de la Información, con el compromiso de la Alta Dirección para la asignación del presupuesto requerido.
7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	No	SI	X	X		Definir un proceso formal con el cual se establezcan claramente las acciones que tomará la Entidad en contra un empleado que haya cometico una violación a la Seguridad de la Información.
7,3	Terminación y cambio de empleo							
7.3.1	Termino de responsabilidades o cambio de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	No	SI	X	X		Definir un proceso formal de paz y salvo a la terminación de los contratos laborales donde se deje constancia del recibido a satisfacción de los archivos físicos, y/o digitales y donde se establezcan los compromisos a guardar estricta reserva sobre la información a la que se tuvo acceso.

Tabla 18. (Continuación)

CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)						Versión: 01
8 Gestión de Activos							
8,1	Responsabilidad de los activos						
8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	No	SI		X	X	Definir un procedimiento formal con lineamientos para la correcta identificación y clasificación de los activos de información de la Cámara de Comercio de Cúcuta.
8.1.2	Propiedad de activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	No	SI		X	X	Mantener actualizada la matriz de valoración de Activos y Análisis de riesgos de Seguridad de la Información, que debe tener el registro de los propietarios de cada activo de información.
8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	No	SI		X	X	Definir un procedimiento formal donde se establezcan los lineamientos para el buen uso de los activos de información.
8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	No	SI	X	X	X	Definir un proceso formal de paz y salvo a la terminación de los contratos laborales donde se deje constancia del recibido a satisfacción de los archivos físicos, y/o digitales.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)							Versión: 01
8,2	Clasificación de la información								
8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	No	SI	X	X	X	X	Definir un procedimiento formal con lineamientos para la correcta identificación y clasificación de los activos de información de la Cámara de Comercio de Cúcuta.
8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	No	SI	X	X	X		Definir un procedimiento formal para el correcto etiquetado de los activos de información, de acuerdo a la clasificación de la información como clasificada, reservada o pública. Ley 1712 de 2014.
8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	No	SI			X		Definir un procedimiento formal que defina la manera en que se debe manejar la información de acuerdo a su clasificación en clasificada, reservada o pública. Ley 1712 de 2017.
8,3	Manejo de medios								
8.3.1	Gestión de medios removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	No	SI	X	X	X		Definir procedimiento para la solicitud, revisión y activación de utilización de medios removibles. Desactivación de puertos USB y unidades de CD/DVD.

Tabla 18. (Continuación)

	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)								Versión: 01
8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	No	SI	X	X	X		Definir un procedimiento formal que establezca la manera correcta en que se deben destruir los medios de almacenamiento de información, dependiendo de su naturaleza. También que se defina los responsables de este procedimiento en cada uno de sus pasos.
8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	No	SI	X	X	X	X	Definir procedimientos formales que establezcan los medios de transferencia seguros para la Entidad cuando se requiera proteger la integridad y confidencialidad de la información contenida en medios físicos.
9 Control de Acceso									
9,1	Requerimientos de negocio para el control de acceso								
9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	No	SI	X	X	X		Definir una política de control de acceso a la red de datos de la Cámara de Comercio de Cúcuta.
9.1.2	Acceso a redes y servicios de red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	No	SI		X	X	X	Definir el procedimiento formal para la activación de accesos a la red de datos, a través de los mecanismos que tenga establecidos la Entidad.
9,2	Gestión de accesos de usuario								

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)							Versión: 01
9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	No	SI	X	X	X	X	Definir un procedimiento de Gestión de usuarios para la solicitud de acceso de los usuarios a los sistemas, y de la cancelación del acceso otorgado.
9.2.2	Suministro de acceso a usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	No	SI	X	X	X		Definir un procedimiento de Gestión de usuarios para la solicitud de acceso de los usuarios a los sistemas, y de la cancelación del acceso otorgado.
9.2.3	Gestión de derechos de acceso privilegiados	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	No	SI	X	X	X		En el procedimiento de Gestión de usuarios se debe establecer los mecanismos para otorgar accesos privilegiados y quienes pueden solicitar este tipo de acceso.
9.2.4	Gestión de información secreta para la autenticación de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	No	SI	X	X	X		En el procedimiento de Gestión de Usuarios se debe establecer la manera en que se entrega la clave secreta de autenticación de los usuarios para garantizar su confidencialidad.
9.2.5	Revisión de derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	No	SI		X	X		En el procedimiento de Gestión de usuarios debe incluir la periodicidad con que los administradores de cada Sistema de Información depurarán los usuarios de los sistemas de información.

Tabla 18. (Continuación)

9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	No	SI		X	X		En el procedimiento de Gestión de usuarios debe incluir lo correspondiente al retiro de privilegio de acceso de los usuarios que ya no labore en la Entidad o ya no tengan un contrato suscrito vigente.
9,3	Responsabilidades del usuario								
9.3.1	Uso de información secreta para la autenticación	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.		SI	X	X	X		Definir una política sobre el buen uso de contraseñas
9,4	Control de acceso de sistemas y aplicaciones								
9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	No	SI	X	X	X		Definir una política de control de acceso a las aplicaciones.
9.4.2	Procedimientos de ingreso (Log-On) seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	No	SI	X	X	X	X	Definir una política de control de acceso a las aplicaciones que defina los procedimientos de ingreso seguro a las aplicaciones.
9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	No	SI			X	X	Definir una política de control de acceso a las aplicaciones que incluye los procedimientos en relación a la administración de claves y el restablecimiento de llaves dañadas u olvidadas, para garantizar la confidencialidad de la clave.
9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	No	SI	X	X	X	X	Definir una política de control de acceso a las aplicaciones y el uso de programas que de tipo privilegiado.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)							Versión: 01
9.4.5	Control de acceso al código fuente del programa	Control: Se debe restringir el acceso a los códigos fuente de los programas.	No	SI	X	X	X		Definir una política de control de acceso a las aplicaciones y al código fuente de los programas, a través de niveles y privilegios de acceso.
10 Criptografía									
10,1	Controles criptográficos								
10.1.1	Política en el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	No	SI	X	X	X	X	Definir una política sobre el uso de controles criptográficos para la protección de la información.
10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	No	SI					Definir e implementar una política de gestión de llaves criptográficas.
11 Seguridad Física y del Entorno									
11,1	Áreas seguras								
11.1.1	Perímetro de seguridad físico	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	No	SI	X	X	X	X	Definir una política de seguridad en el acceso a las áreas restringidas como Centros de Datos y de Telecomunicaciones.
11.1.2	Controles físicos de entrada	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	No	SI	X	X	X	X	Definir una política de seguridad en el acceso a las áreas restringidas tales como los Centros de Datos y Telecomunicaciones, áreas de Gestión Documental y archivo.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)							Versión: 01
11.1.3	Seguridad de oficinas, habitaciones y facilidades	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	No		SI		X	X	Definir una política de seguridad en el acceso a las áreas oficinas en general de la Entidad.
11.1.4	Protección contra amenazas externas y del ambiente	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	No		SI	X	X	X	X	Definir e implementar los sistemas que se requieran para proteger las instalaciones de la Cámara de Comercio de Cúcuta ante eventuales desastres naturales (sensores de humo, aspersores contra incendios, etc.)
11.1.5	Trabajo en áreas seguras	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	No		SI		X	X		Definir una política de seguridad en el acceso a las áreas seguras de la Entidad.
11.1.6	Áreas de entrega y carga	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	No	No hay zonas de carga por la naturaleza de la Entidad.	No					
11,2	Equipo									
11.2.1	Ubicación y protección de equipo	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	SI. Equipos dentro de áreas restringidas de acceso.		SI		X	X	X	Definir un procedimiento formal y guía sobre las ubicaciones autorizadas para los equipos para que queden protegidos de accesos no autorizados.

Tabla 18. (Continuación)

CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)							Versión: 01
11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Parcialmente. La mayoría de los equipos tienen UPS.	SI		X	X		Definir un procedimiento formal para la revisión del estado de todos los servicios de suministro que están relacionados con los equipos para evaluar si la capacidad está acorde a la cantidad de equipos.
11.2.3	Seguridad del cableado	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	SI. Cableado estructurado certificado	SI		X	X	X	Definir un procedimiento formal para el suministro de cableado estructurado, que incluya normas de seguridad y controles de acceso a cajas de inspección.
11.2.4	Mantenimiento de equipos	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI. Programa de mantenimiento preventivo a equipos.	SI		X	X	X	Definir una mayor periodicidad de los ciclos de mantenimiento preventivo, que sea superior a los dos ciclos al año.
11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	No	SI		X	X		Establecer procedimiento formal para el retiro de activos de la Entidad.
11.2.6	Seguridad del equipo y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	SI, parcialmente. Pólizas de seguros para equipos.	SI		X	X		Los equipos que se autorizan para ser trasladados o mantenerse fuera de la Entidad se deben proteger con pólizas de seguros y controles de seguridad informática.
11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobre-escrito en forma segura antes de su disposición o reúso.	No	SI	X	X			Definir un procedimiento formal que establezca la manera correcta en que se deben destruir los medios de almacenamiento de información, dependiendo de su naturaleza. También que se defina los responsables de este procedimiento en cada uno de sus pasos.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)						Versión: 01
11.2.8	Equipo de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	SI. Políticas del Directorio activo	SI		X	X	X	Establecer formalmente los procedimientos mediante el cual los sistemas desatendidos quedan protegidos a través de políticas del directorio activo.
11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	No	SI		X	X	X	Definir una política de escritorio limpio y pantalla limpia que incluya escritorios físicos, medios removibles y equipos.
12 Seguridad en las Operaciones									
12,1	Procedimientos Operacionales y Responsabilidades								
12.1.1	Documentación de procedimientos operacionales	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	No	SI	X	X	X		Crear manuales de procedimientos e instructivos de los sistemas de la Entidad.
12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	No	SI		X	X		Definir un proceso formal para tramitar y asegurar los cambios en los sistemas de información que administra la Dirección de Tecnología, con el fin de minimizar la probabilidad de interrupciones y cambios no autorizados.
12.1.3	Gestión de la capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	No	SI		X	X		Definir planes de Gestión de la capacidad con proyección mínimo a cinco años, para determinar los recursos que se necesitan a nivel de tecnología para que estén acorde a la demanda de la Entidad.

Tabla 18. (Continuación)

12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	SI, parcialmente. Ambientes de desarrollo, pruebas y operación para algunos sistemas.	SI		X	X		Definir ambientes de desarrollos, pruebas y producción para cada sistema de información de la Entidad, para la realización de pruebas de seguridad y operación antes de lanzar a producción.
12,2	Protección de Software Malicioso								
12.2.1	Controles contra software malicioso	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	SI. Software Antivirus	SI		X	X		Establecer dentro de los planes de formación lo referente a la toma de conciencia en temas de Seguridad de la Información.
12,3	Respaldo								
12.3.1	Respaldo de información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	SI. Consolidado Registro de Backups. Informe de restauración y verificación de Backups	SI	X	X	X	X	Mantener los controles actuales definidos por la Entidad.
12,4	Bitácoras y monitoreo								
12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	No	SI	X	X	X	X	Definir política de retención de logs en el tiempo, en cada uno de los sistemas a cargo de la Dirección de Tecnología.
12.4.2	Protección de la información de registro (log información)	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	No	SI	X		X	X	Definir política de retención de logs que indique la periodicidad con la cual se hará copia de seguridad de estos registros.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)							Versión: 01
12.4.3	Registros (logs) del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	No	SI	X		X	X	Definir política de retención de logs que incluya los registros de actividades de los administradores de los sistemas.
12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	SI. Servicio NTP en Directorio Activo.	SI			X		Mantener la sincronización de relojes a través del servicio NTP del Directorio Activo que se encuentra sincronizado con la hora legal colombiana. Incluir esta directriz dentro de la política de retención de logs.
12,5	Control de software operacional								
12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI. Proceso Instalación de aplicaciones. Proceso Instalación de software en Servidores Políticas de restricción de instalación de software del directorio activo.	SI		X	X		Aplicar los procesos ya definidos por la Entidad.
12,6	Gestión de vulnerabilidades técnicas								
12.6.1	Gestión de vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	No	SI		X	X	X	Definir un procedimiento formal para la detección de vulnerabilidades técnicas de los sistemas de información para tomar acciones de manera preventiva.

Tabla 18. (Continuación)

CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)								Versión: 01
12.6.2	Restricciones en la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	SI. Proceso Instalación de aplicaciones. Proceso Instalación de software en Servidores Políticas de restricción de instalación de software del directorio activo.	SI	X	X	X	X	Aplicar los procesos ya definidos por la Entidad.
12,7	Consideraciones de auditoria de sistemas de información								
12.7.1	Controles de auditoría de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	No	SI		X	X		Definir planes de auditoría a los sistemas de información.
13 Seguridad en las Comunicaciones									
13,1	Gestión de seguridad en red								
13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI, parcialmente. Monitoreo de la red	SI					Definir los procedimientos formales para el monitoreo y control de la información de los sistemas a cargo de la Dirección de Tecnología.
13.1.2	Seguridad en los servicios en red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red ya sea que los servicios se presten internamente o se contraten externamente.	No	SI		X	X	X	Definir los Acuerdos de Nivel de Servicio para todos los servicios que presta la Dirección de Tecnología.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)							Versión: 01
13.1.3	Separación en las redes	Control: Los grupos de servicios de información usuarios y sistemas de información se deben separar en las redes.	si, parcialmente. VLANs	SI			X	X	Definir procedimiento formal para la segmentación de la red a través de VLANs.
13,2	Transferencia de información								
13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	No	SI		X	X	X	Diseñar políticas, procedimientos y controles de transferencia de información para proteger la información que se envía a través de los diferentes medios de comunicación.
13.2.2	Acuerdos en la transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	No	SI	X	X	X	X	Definir acuerdos entre la Entidad y partes externas para la transferencia segura de la información.
13.2.3	Mensajería electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	No	SI		X	X	X	Definir dentro de la política de tratamiento de la información los lineamientos para el uso de mensajería electrónica autorizada por la Dirección de Tecnología, que es el correo electrónico corporativo.
13.2.4	Acuerdos de confidencialidad o no-revelación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	No	SI	X	X	X	X	Definir dentro de la política de tratamiento de la información los Acuerdos de confidencialidad de la información.

Tabla 18. (Continuación)

CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)							Versión: 01
14 Adquisición, Desarrollo y Mantenimiento de Sistemas								
14,1	Requerimientos de seguridad en sistemas de información							
14.1.1	Análisis y especificación de requerimientos de seguridad	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	No	SI	X	X	X	X	Establecer los requisitos de seguridad que deben cumplir todos los sistemas de información nuevos de la Entidad y cuando se les realicen mejoras en cada una de las fases del desarrollo, y definir un procedimiento para su aplicación.
14.1.2	Aseguramiento de servicios de aplicación en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	No	SI	X	X	X		Definir los procedimientos formales para la información que es transmitida por redes públicas.
14.1.3	Protección de transacciones en servicios de aplicación	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	No	SI	X	X	X	X	Definir los procedimientos formales para la información que es transmitida por redes públicas.
14,2	Seguridad en el proceso de desarrollo y soporte								
14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	No	SI		X	X		Establecer una política de desarrollo seguro que garantice que las aplicaciones cumplan con los requerimientos de seguridad en cada una de las fases de desarrollo.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)					Versión: 01
14.2.2	Procedimientos de control de cambios del sistema	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	No	SI	X	X	Definir un proceo formal para tramitar y asegurar los cambios en los sistemas de información que administra la Dirección de Tecnología, con el fin de minimizar la probabilidad de interrupciones y cambios no autorizados.
14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	No	SI	X	X	Definir procedimientos formales de pruebas a los sistemas de información luego de que se realicen cambios a las plataformas que los soportan (sistemas operativos, plataforma SAN, red, etc).
14.2.4	Restricción de cambios en paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	No	SI	X	X	Dentro de la política de desarrollo seguro se debe incluir los lineamientos para que a los paquetes de software no se les realice cambios a menos que sea estrictamente necesario y realizarlos bajo controles de seguridad.
14.2.5	Principios de seguridad en la ingeniería de sistemas	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	No	SI	X	X	Establecer una política de desarrollo seguro que garantice que las aplicaciones cumplan con los requerimientos de seguridad en cada una de las fases de desarrollo.
14.2.6	Entorno de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	No	SI	X	X	Establecer una política de desarrollo seguro que garantice que las aplicaciones tengan ambientes de desarrollo seguros.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)					Versión: 01
14.2.7	Desarrollo tercerizado	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	No	SI	X	X	Establecer una política de desarrollo seguro que garantice que los desarrollos contratados con terceros cumplan con lo requerido.
14.2.8	Pruebas de seguridad del sistema	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	No	SI	X	X	Establecer una política de desarrollo seguro que garantice que se realicen las pruebas necesarias de funcionalidad antes de la puesta en marcha del sistema.
14.2.9	Pruebas de aceptación del sistema	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	No	SI	X	X	Establecer una política de desarrollo seguro que garantice que se realicen las pruebas necesarias de funcionalidad antes de la puesta en marcha del sistema.
14,3	Datos de prueba						
14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	No	SI	X	X	Establecer una política de desarrollo seguro que garantice que los datos de prueba se seleccionan, se protegen y se controlan cuidadosamente.
15 Relaciones con Proveedores							
15,1	Seguridad de la información en relaciones con el proveedor						
15.1.1	Política de seguridad de la información en las relaciones con el proveedor	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	No	SI	X	X	La política de Seguridad de la Información debe incluir acuerdos de confidencialidad con proveedores.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)						Versión: 01
15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	No	SI		X	X	Definir los acuerdos de confidencialidad y reserva en el manejo de la información con proveedores.
15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	No	SI		X	X	Definir un listado maestro de los requisitos a exigir a cada proveedor dependiendo del tipo de servicio a suministrar, para mitigar riesgos de seguridad de la información.
15,2	Gestión de entrega de servicios de proveedor							
15.2.1	Monitoreo y revisión de servicios del proveedor	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	SI. Proceso de evaluación de proveedores del área de Compras	SI	X	X	X	Dentro del proceso de evaluación de proveedores se debe incluir lo correspondiente a la seguridad de la información.
15.2.2	Gestión de cambios a los servicios del proveedor	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	No	SI	X	X	X	Establecer una política de cambios a los servicios del proveedor.

Tabla 18. (Continuación)

CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)						Versión: 01
16 Gestión de Incidentes de Seguridad de la Información							
16,1	Gestión de incidentes de seguridad de la información y mejoras						
16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	No	SI	X	X	X	Definir un procedimiento formal para gestionar adecuadamente los incidentes de seguridad de la información.
16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	No	SI	X	X	X	Definir un procedimiento formal para gestionar adecuadamente los incidentes de seguridad de la información, que establezca los canales apropiados para el reporte de dichos eventos.
16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	No	SI	X	X	X	Establecer planes de concientización al personal sobre la seguridad de la información y la importancia de reportar cualquier debilidad que observen en los sistemas de información.
16.1.4	Evaluación de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	No	SI	X	X	X	Establecer el procedimiento formal de análisis y evaluación del impacto los incidentes de seguridad de la información.
16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	No	SI	X	X	X	Establecer el procedimiento formal para la respuesta ante un incidente de seguridad, recolección de evidencias, identificar fuentes de ataque, aplicar estrategias de recuperación y erradicación de la falla de seguridad.

Tabla 18. (Continuación)

CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)							Versión: 01
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	No	SI		X	X	X	Establecer una metodología para el manejo de lecciones aprendidas con respecto a incidentes de seguridad de la información, que incluya el mantener un listado de incidentes, bases de conocimiento, actualizar matriz de riesgos y capacitaciones a los usuarios.
16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	No	SI		X	X	X	Establecer el procedimiento formal para la respuesta ante un incidente de seguridad, recolección de evidencias, identificar fuentes de ataque, aplicar estrategias de recuperación y erradicación de la falla de seguridad.
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio									
17,1	Continuidad de la seguridad de la información								
17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	No	SI	X		X	X	Establecer un plan de continuidad que garantice la operatividad de la organización en caso de que los procesos críticos fallen.
17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	No	SI	X		X	X	Implementar un plan de continuidad que garantice la operatividad de la organización en caso de que los procesos críticos fallen.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)						Versión: 01
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	No	SI	X		X	X	Evaluar el plan de continuidad que garantice la operatividad de la organización en caso de que los procesos críticos fallen.
17,2	Redundancias								
17.2.1	Disponibilidad de facilidades de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI. Plataforma SAN redundante en un sitio alterno.	SI	X		X	X	Mantener los controles actuales implementados y extenderlos a los componentes de red.
18 Cumplimiento									
18,1	Cumplimiento con Requerimientos Legales y Contractuales								
18.1.1	Identificación de legislación aplicable y requerimientos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	No	SI	X	X	X		Definir el normograma que incluya lo relacionado a la Seguridad de la Información.
18.1.2	Derechos de propiedad intelectual (IPR)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	No	SI	X	X	X		Establecer procedimiento formal para asegurar el cumplimiento de los requisitos legales relacionados con derechos de propiedad intelectual.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)						Versión: 01
18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	No	SI	X	X	X	Establecer procedimiento formal para proteger los registros de la Entidad de acuerdo a los requisitos legales existentes aplicables a la Cámara de Comercio de Cúcuta.
18.1.4	Privacidad y protección de información personal identificable	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	SI. Manual de políticas y procedimientos de Protección de datos personales	SI	X	X	X	Mantener e implementar los manuales de políticas y procedimientos establecidos para la protección de datos personales.
18.1.5	Reglamentación de controles criptográficos	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	No	SI	X	X	X	Implementar controles criptográficos para garantizar la confidencialidad e integridad de la información.
18,2	Revisiones de seguridad de la información							
18.2.1	Revisión independiente de seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	No	SI	X	X	X	Plan anual de auditorías de seguridad de la información.

Tabla 18. (Continuación)

	CÁMARA DE COMERCIO DE CÚCUTA	CAMARA DE COMERCIO DE CUCUTA - Declaración de aplicabilidad (SOA)						Versión: 01
18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	No	SI	X	X	X	Por ser una entidad que maneja recursoso públicos, es recomendable acatar las indicaciones del Gobierno nacional sobre la inclusión de la seguridad de la información en todos sus procesos.
18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	No	SI	X	X	X	Plan anual de revisión de controles técnicos en los sistemas de información de la Entidad para el cumplimiento de las políticas y normas de seguridad de la información.

Fuente: Elaboración propia

Fase 3. Diseño de las políticas de seguridad de la información aplicables para la Unidad de Tecnología de la cámara de comercio de Cúcuta.

Actividad 1. Elaboración de la política de seguridad de información prioritarias de acuerdo al análisis realizado

A continuación se definen las Políticas de Seguridad de la Información para la Dirección de Tecnología de la Cámara de Comercio de Cúcuta.

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA DIRECCION DE TECNOLOGÍA DE LA CAMARA DE COMERCIO DE CUCUTA

Dirección de Tecnología de la Cámara de Comercio de Cúcuta, como unidad aliada estratégica de la Cámara de Comercio de Cúcuta en el logro de las metas institucionales implementando tecnologías, estándares y herramientas tecnológicas de última generación, busca la satisfacción de sus usuarios prestando servicios ágiles y oportunos, garantizando el cumplimiento de los requisitos establecidos por el Gobierno en cuanto a la seguridad de la información, se compromete a:

- Realizar una gestión de riesgos de seguridad de la información que permita la identificación de los activos de información, su valoración, identificación de riesgos e implementación de controles de seguridad.
- Garantizar la disponibilidad, confidencialidad e integridad de los activos de información de la Dirección de Tecnología.
- Divulgar esta política a todos los demás procesos de la Entidad y todos los empleados, proveedores y demás que interactúen con la Dirección de Tecnología.

La Dirección de Tecnología reconoce la importancia de la Seguridad de la Información y la protección de los activos para alcanzar los objetivos institucionales, así como también reconoce que el mal uso de los activos de información puede afectar el normal funcionamiento de la Entidad.

Alcance: Esta política es de cumplimiento por parte de todos los empleados, contratistas y terceros de la Entidad que de alguna u otra forma utilicen los servicio de la Dirección de Tecnología.

Cumplimiento: Todos los empleados, contratistas y terceros que en el desarrollo de sus funciones utilicen los servicios de la Dirección de Tecnología deben cumplir con la totalidad de la presente política. El incumplimiento de la misma puede tener consecuencias disciplinarias y/o legales.

Principios de seguridad: A continuación se establecen los principios de la Dirección de Tecnología con respecto a la seguridad de la Información:

- La Dirección de Tecnología protegerá la información contenida en los sistemas de información y medios de almacenamiento y a toda la infraestructura tecnológica sobre la que se soporta la operación de la Cámara de Comercio de Cúcuta.
- La Dirección de Tecnología protegerá las instalaciones donde se encuentra ubicada toda la infraestructura tecnológica que soporta la operación de la Entidad.
- La Dirección de Tecnología implementará controles de seguridad en el acceso a la información, a la red y a todos los recursos bajo su responsabilidad.
- La Dirección de Tecnología realizará una adecuada gestión de incidentes de seguridad y la mejora constante de los sistemas de información e infraestructura tecnológica para mejorar los niveles de seguridad de la información.

POLITICAS DE SEGUNDO NIVEL

Política de dispositivos móviles.

La Dirección de Tecnología define las siguientes políticas con respecto a los dispositivos móviles, tales como computadores y tabletas:

- Cada dispositivo móvil debe estar inventariado y registrados sus datos de conexión.
- La información deberá estar encriptada para salvaguardar la misma en el caso de pérdida o robo.
- La red inalámbrica a la que se conectan debe tener controles de seguridad y de segregación de redes.
- Todo dispositivo móvil estará configurado para ser usado con credenciales del dominio de la Cámara de Comercio de Cúcuta.
- La pérdida o robo de un dispositivo móvil deberá ser reportada a la Dirección a la mayor brevedad posible.

Política de seguridad de los recursos humanos

- Se debe dar cumplimiento a lo establecido en el procedimiento del área de Talento Humano AF-TH-03 Vinculación de Personal para el ingreso de personal a la Entidad.
- Todo usuario de los sistemas de información a cargo de la Dirección de Tecnología debe firmar el acuerdo de Confidencialidad, que estará a cargo del proceso de Gestión de Talento Humano, asociado también al reglamento interno de trabajo, con el que se rija el comportamiento de los empleados con respecto a la Información a la que tienen acceso y las consecuencias de cometer actos en contra de la seguridad de esta.
- Todos los empleados y contratistas deben dar cumplimiento a todas las políticas de Seguridad de la Información definidas.
- Se deben realizar capacitaciones y sensibilizaciones sobre temas relacionados con la Seguridad de la Información.
- En el caso de cometer actos en contra de la seguridad de la información se deberá seguir el procedimiento donde se establezcan las acciones que tomará la Entidad en contra un empleado que haya cometido una violación a la Seguridad de la Información.
- A la terminación de los contratos laborales se firmará un documento de paz y salvo a donde se deje constancia del recibido a satisfacción de los archivos físicos, y/o digitales y donde se establezcan los compromisos a guardar estricta reserva sobre la información a la que se tuvo acceso.

Política de Gestión de Activos

- La identificación y clasificación de los activos de información de la Dirección de Tecnología se llevará a cabo a través de un procedimiento formal con lineamientos para su ejecución, y se mantendrá actualizada la matriz de valoración de Activos y análisis de riesgos de Seguridad de la Información.
- Los activos de información deben estar etiquetados de acuerdo a la clasificación establecida en la Ley 1712 de 2014.

Política de manejo de medios removibles

- Se debe guardar bajo llave o con algún otro dispositivo de seguridad todos los documentos y dispositivos removibles como discos duros externos y memorias USB para evitar el acceso a ellos por personas no autorizadas.

- El uso de medios removibles debe autorizarse siguiendo el procedimiento establecido para esto, que indique los pasos de solicitud, revisión y activación de utilización.
- Los puertos USB de las estaciones de trabajo permanecerán desactivados, y solo se autorizará haciendo una solicitud formal que será evaluada, autorizada o denegada.
- Los medios removibles que son autorizados para su uso deberán mantenerse libres de cualquier software malicioso que pueda poner en riesgo la seguridad de la información. Para esto deberán ser analizados con el antivirus periódicamente.
- En el caso de requerir el traslado de medios removibles se utilizarán sólo los medios de transporte seguros para proteger la integridad y confidencialidad de la información contenida en estos medios físicos.
- La información contenida en medios removibles debe estar encriptada para poder ser trasportada con seguridad.
- Se debe disponer de manera segura de los medios removibles cuando cumplan su vida útil, siguiendo un procedimiento formal que establezca la manera correcta en que se deben destruir los medios de almacenamiento de información, dependiendo de su naturaleza. También que se defina los responsables de este procedimiento en cada uno de sus pasos.
- Todo medio removible de terceros utilizados por la Cámara de Comercio de Cúcuta, antes de su devolución se les realizará un proceso de borrado seguro de la información.

Política de control y administración de acceso

La Dirección de Tecnología debe controlar el acceso a la información y limitarla sólo a las personas autorizadas. Estos controles se harán tanto en los Sistemas de Información como a los recursos de red.

- El acceso de los usuarios a los sistemas se habilitará sólo cuando se haya solicitado formalmente este acceso a través del Sistema de Gestión Documental, con autorización firmada por el Gerente del área. No se aceptarán solicitudes de acceso a través de otro medio.
- La Dirección de Tecnología debe revisar las cuentas de los sistemas de información, una vez al año.
- La Dirección de Tecnología dispone de los mecanismos para realizar auditorías de creación, modificación y desactivación de usuarios en el caso de que se requiera este tipo de información.
- La Dirección de Tecnología realizará la desactivación de las cuentas de acceso a los sistemas de un usuario cuando se reciba la notificación del área de Talento Humano sobre su desvinculación temporal o definitiva a la Entidad.

Política de gestión de contraseñas

- Cada usuario tiene un único usuario de acceso a cada Sistemas de Información, y en el caso que aplique, será el mismo utilizado para autenticarse en el dominio de red de la Entidad.
- Las claves de acceso a los sistemas de información son personales e intransferibles. Es responsabilidad de cada usuario el buen uso de éstas, y velar porque no sea conocida por terceros no autorizados. De sospechar del conocimiento de la contraseña o de la pérdida de confidencialidad de esta, deberá ser cambiada de manera inmediata.
- Los Sistemas de Información forzarán el cambio de contraseñas de acceso a los sistemas de información deberán ser cambiadas periódicamente.
- Las contraseñas deberán tener una longitud mínima de ocho (8) caracteres, y deben incluir caracteres especiales, letras mayúsculas y minúsculas y números. Estas validaciones las debe realizar el sistema al momento de realizar el ingreso o cambio de una contraseña.
- No se podrá utilizar la misma contraseña en el cambio de ésta, y ni permitirse que se utilice una que sea igual ha alguna de los 5 cambios anteriores.
- El almacenamiento de las contraseñas en los sistemas de información deberá estar encriptada de forma tal que no puedan ser leídas.

Política de control de acceso a redes e internet

- El acceso de los usuarios a la red de datos se habilitará sólo cuando se haya solicitado formalmente este acceso a través del Sistema de Gestión Documental, con autorización firmada por el Gerente del área. No se aceptarán solicitudes de acceso a través de otro medio.
- El acceso a la red de la Cámara de Comercio de Cúcuta se hará únicamente a través de dispositivos autorizados por la Dirección de Tecnología.
- El acceso a la red inalámbrica Wifi de la Entidad se hará únicamente a través de dispositivos autorizados por la Dirección de Tecnología, y en los casos de dispositivos de usuarios invitados como en Salones y Eventos, el acceso se permitirá, pero a una red segregada distinta a la demás red inalámbrica.

Política de seguridad para el uso de Internet

- Cada usuario del directorio activo tendrá un acceso básico a páginas gubernamentales de Colombia. El acceso a otras páginas web se habilitará sólo cuando se haya solicitado formalmente este acceso a través del Sistema de Gestión Documental, con autorización firmada por el Gerente del área.

- Cada usuario tendrá un perfil de navegación en Internet que le brindará acceso solo a lo autorizado para ese nivel.
- La navegación a sitios de pornografía, terrorismo, juegos en línea y de azar o cualquier otro tipo de sitios catalogados como potencialmente peligrosos estarán bloqueado a través del sistema de filtrado de navegación.
- La salida directa a Internet no está permitida a menos que se requiera para una labor técnica, previamente autorizada por la Dirección de Tecnología.
- El acceso a Internet otorgado por la Dirección de Tecnología estará permanentemente monitoreado, y podrá ser suspendido en cualquier momento en que por razones de seguridad se requiera.
- El acceso a Internet se habilitará para fines exclusivamente laborales.

Política sobre accesos remotos

- Las conexiones remotas a la red de datos de la Entidad se habilitarán sólo cuando se haya solicitado formalmente este acceso a través del Sistema de Gestión Documental, con autorización firmada por el Gerente del área, en el caso de accesos de personal o contratistas de la Cámara de Comercio de Cúcuta.
- Las conexiones remotas a la red de datos de la Entidad se habilitarán sólo cuando se haya autorizado el acceso a través de un acuerdo de confidencialidad firmado por un tercero, como proveedores o asesores, en donde se establezca la responsabilidad, el tiempo de acceso y finalidad del mismo.
- Todas las conexiones remotas que habilite la Dirección de Tecnología se establecerán a través de conexiones seguras haciendo uso de mecanismos de encriptación.

Política sobre controles criptográficos

- La Dirección de Tecnología garantizará que en la plataforma tecnológica se tienen implementados mecanismos de encriptación de la información.
- Las claves de encriptación utilizadas serán protegidas para evitar que sean modificadas o copiadas sin autorización
- Las contraseñas se almacenarán de manera encriptadas en cada uno de los sistemas de información, y se garantizará que se mantiene la confidencialidad de estas en su almacenamiento y proceso de entrega al usuario final.
- Es responsabilidad del usuario al que se le ha entregado una firma digital o cualquier otro mecanismo criptográfico el buen uso de estos, y debe velar porque no sean conocidos por terceros no autorizados.

Política sobre seguridad física y del entorno

- Los equipos que forman parte de la plataforma tecnológica de la Cámara de Comercio de Cúcuta se encuentran dentro de en áreas delimitadas con acceso restringido. El acceso a estos sitios será controlado y permitido solo a personal autorizado.
- El control de acceso se realizará a través de mecanismos que permitan registrar quien ingresa y la hora de acceso y de retiro del área restringida.
- El ingreso al área restringida se realizará con acompañamiento de la persona de la Dirección de Tecnología designada, durante todo el tiempo que dure la visita.
- Las áreas restringidas donde se encuentran los equipos de la plataforma tecnológica tendrán siempre sistemas que permitan protegerlos de daños eléctricos, medio ambiental como humedad y temperatura y de desastres naturales o provocados tales como incendios.
- Cuando se requiera la creación de una nueva área restringida se tendrán en cuenta los riesgos de seguridad a evitar tales como incendios, explosiones, terremotos, etc., para su diseño y ubicación.

Política de seguridad de equipos de cómputo

- La Dirección de Tecnología revisará al menos una vez al año el estado de todos los servicios de suministro que están relacionados con los equipos para evaluar si la capacidad está acorde a la cantidad de equipos.
- Se realizarán al menos tres ciclos de mantenimiento preventivo a los equipos de cómputo.
- El traslado o movimiento de equipos de cómputo se realizará sólo cuando se haya solicitado formalmente este movimiento a través del Sistema de Gestión Documental, con autorización firmada por el Gerente del área y la respectiva actualización del inventario de activos.
- En el caso de reasignaciones de equipos por traslado de activos, se debe realizar una verificación previa para asegurar que cualquier dato confidencial o software licenciado no quede disponible para uso de un usuario que no está autorizado.

Política de escritorio limpio y pantalla limpia

- La información que sea de tipo clasificada o reservada que se encuentre en los escritorios de los usuarios debe mantenerse siempre bajo llave en, independientemente del medio físico en el que se encuentre almacenada, ya

sean documentos físicos o medios removibles, para evitar que personas no autorizadas tengo acceso.

- Es responsabilidad de los usuarios mantener bajo llave la información clasificada y reservada que se encuentre en medios físicos removibles o documentos físicos.
- En todo momento se debe mantener supervisión de los documentos físicos o en medios removibles, sin dejarlos desatendidos cuando se solicita que se les realice copia o escaneo.
- Todo documento escaneado debe ser eliminado del repositorio del equipo del escaneador para evitar que pueda existir fuga de información.
- En los Centros de Datos y de Telecomunicaciones (áreas restringidas) se mantendrá para los equipos las pantallas limpias.
- La Dirección de Tecnología a través del directorio activo programa el bloqueo de las sesiones de usuarios a los cinco minutos de actividad, pero es responsabilidad del usuario bloquear su sesión una vez se retire del equipo dejándolo desatendido, para evitar accesos no autorizados. El desbloqueo de la sesión sólo se podrá hacer con la contraseña de inicio de sesión en el dominio.

Política de seguridad en las operaciones

- La Dirección de Tecnología mantendrá actualizados los procedimientos de operación identificados en esta Política y los cambios serán autorizados por la Directora de Tecnología.
- La Dirección de Tecnología se asegurará que los cambios en los sistemas de información no afectarán la disponibilidad, confidencialidad e integridad de la información.
- Se mantendrán ambientes de desarrollo, pruebas y producción para cada sistema de información de la Entidad, para la realización de pruebas de seguridad y operación antes de lanzar a producción.

Política de protección de software malicioso

- La Dirección de Tecnología gestionará la implementación de un software de detección de malware para la detección de códigos maliciosos en equipos, servidores, dispositivos móviles, removibles o cualquier dispositivo conectado a la red de datos de la Entidad.
- Se realizará un proceso de análisis de código malicioso en los equipos y servidores periódicamente en un horario que no afecte el desempeño del dispositivo.

- Se concientizará a los usuarios de las vulnerabilidades asociadas a los virus informáticos.
- Los usuarios deben reportar inmediatamente cualquier evento sospechoso que detecten en los equipos a su cargo.
- No se permite la desactivación manual del software de antivirus. Esta actividad sólo la puede realizar personal de la Dirección de Tecnología autorizado, que tengan la clave para la desactivación.

Políticas de respaldo de Información

- Se realizan copias de seguridad a todas las bases de datos, sistemas de información y máquinas virtuales de la Cámara de Comercio de Cúcuta, con la periodicidad que se establezca en el procedimiento de backups de la Dirección de Tecnología.
- Las copias de seguridad son probadas periódicamente como lo establece el procedimiento de Backups, para garantizar su buen estado.
- Los empleados, contratistas y demás usuarios deben indexar en los expedientes los documentos que corresponden a su gestión en el Sistema de Gestión Documental para garantizar que son incluidos dentro de la programación de Backups de la Dirección de Tecnología.
- Los documentos de gestión diaria que los usuarios deseen respaldar, los deben subir al sistema de almacenamiento en la nube *OneDrive* que ha dispuesto la Dirección de Tecnología para tal fin.
- La Dirección de Tecnología garantiza la cadena de custodia en el transporte de medios removibles de almacenamiento de Backups.

Política de bitácoras y monitoreo

- La Dirección de Tecnología mantiene activados los logs de los sistemas críticos.
- Se realiza backup periódico de los logs de los sistemas críticos, y el tiempo de retención se define de acuerdo a lo establecido en el procedimiento de Backups.
- Los logs de actividad de los administradores están activados.
- El área de tecnología deberá revisar regularmente los logs de cada uno de los sistemas para tomar acción oportuna sobre los eventos relevantes de seguridad.
- Se mantiene la sincronización de relojes a través del servicio NTP del Directorio Activo que se encuentra sincronizado con la hora legal colombiana.

Política de control de software operacional

- La instalación de programas en los equipos de los usuarios es responsabilidad de la Dirección de Tecnología y se rige por el Proceso Instalación de aplicaciones.
- La Dirección de Tecnología mantiene la restricción de instalación de aplicaciones en los equipos de los usuarios a través de políticas del directorio activo.
- Los sistemas operativos de equipos y servidores estarán actualizados a la última versión disponible.

Política de seguridad en las comunicaciones

- La Dirección de Tecnología realiza monitoreo constante de las conexiones de red existentes para garantizar su operación.
- La Dirección de Tecnología segmenta la red de datos para separar la plataforma tecnológica de los equipos de usuarios, canales de Internet y demás servicios de conectividad ofrecidos por terceros.
- Para todos los servicios que se prestan en red se identificarán los mecanismos de seguridad y los acuerdos de nivel de servicio, ya sean estos servicios internos o que se contraten con terceros.
- En el caso de transferencia de información en medios físicos, esta se realizará de acuerdo a lo establecido por el Centro de Información Documental CINDOCCC y sus manuales respectivos.
- En el caso de transferencia de información digital con entidades externas, se realizarán previamente con la organización o entidad externa los estudios y análisis para que la comunicación se realice de manera segura, siempre en el marco de un contrato o convenio interinstitucional.
- Para la transferencia de información digital dentro de la Cámara de Comercio de Cúcuta, la Dirección de Tecnología implementará las herramientas que brinden seguridad para la comunicación.
- El correo electrónico corporativo es para ser utilizado con fines laborales. De igual manera, está prohibido el uso de los correos electrónicos personales para enviar o recibir información relacionada con la Cámara de Comercio de Cúcuta.

Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

- La Dirección de Tecnología velará por que los desarrollos de aplicaciones tanto internos como externos contratados cumplan con los requerimientos de seguridad para preservar la integridad, confidencialidad y disponibilidad de la información, durante todo el ciclo de vida del desarrollo del software
- Los proveedores contratados para desarrollo de aplicaciones deberán cumplir con las políticas acá descritas para garantizar la seguridad de la información.

- Las adquisiciones de software que realice la Cámara de Comercio de Cúcuta estarán apoyadas técnicamente por la Dirección de Tecnología, y se realizará con empresas que demuestren idoneidad y experiencia en el suministro requerido.
- Se debe mantener registro de control de cambios en el desarrollo de las aplicaciones, donde se especifiquen datos como fecha, hora y cambio realizado, motivo del cambio y quién lo realizó. Los cambios se realizarán siempre que sean necesarios y se justifique su necesidad.
- Deben existir ambientes de desarrollo, pruebas y producción.
- Cuando se realice un cambio en la aplicación, se deben hacer las pruebas necesarias para evitar que estos afecten la producción de otros sistemas o de la misma plataforma tecnológica de la Entidad.
- Todo desarrollo de una aplicación debe contar con los ambientes de desarrollo, pruebas y producción.
- Se deben realizar pruebas de seguridad a los sistemas en desarrollo durante todo el ciclo de vida para detectar vulnerabilidades y corregirlas.
- La Dirección de Tecnología velará por la realización de las pruebas necesarias de los sistemas antes de salir a producción.
- Los códigos fuentes de los programas estarán protegidos adecuadamente para preservar su integridad y confidencialidad.
- Se adoptarán los estándares y mejores prácticas para el desarrollo de códigos de aplicaciones para que estos operen de la manera más eficiente.

Política de Gestión de Incidentes de Seguridad de la Información

- Todos los empleados, contratistas y terceros de los sistemas de información deben reportar oportunamente cualquier debilidad o vulnerabilidad de seguridad detectada, siguiendo el procedimiento establecido para hacer el respectivo reporte.
- El oficial de Seguridad recibirá las notificaciones de incidentes de seguridad y les hará la respectiva gestión.
- Por cada incidente de seguridad se hará un registro y una evaluación para determinar el nivel de impacto, de acuerdo al procedimiento de evaluación de incidentes de seguridad.
- Se deben documentar las lecciones aprendidas con respecto a incidentes de seguridad de la información, para que el tratamiento aplicado sirva como solución para futuros incidentes similares.

4. CONCLUSIONES

Según los resultados obtenidos en el desarrollo del presente proyecto se concluye que la Dirección de Tecnología, como área de apoyo transversal de la Cámara de Comercio de Cúcuta puede disminuir el impacto sobre los activos de información al tener unas Políticas de Seguridad de la Información que permitan establecer el marco de operación de los Sistemas de Información y en general de todos los servicios prestados a los usuarios internos y externos. Al ser esta área la encargada de soportar toda la infraestructura tecnológica de la Entidad estas políticas servirán de base para que la Cámara de Comercio de Cúcuta, si así lo desea, las hagan extensivas a las demás áreas de la organización y asegurar los activos de información de toda la Entidad.

Dentro de proceso de análisis de riesgos se detectaron algunos riesgos que requieren que la Alta Dirección de la Cámara de Comercio de Cúcuta realice una inversión de recursos en la implementación de controles. Este análisis le permitirá a la Dirección de Tecnología presentar propuestas de implementación de sistemas que minimicen la materialización de estos riesgos de seguridad.

El diseño de las Políticas de Seguridad de la Información para la Dirección de Tecnología debe ser complementado con la definición de procedimientos, guías y manuales de seguridad de acuerdo a los controles de seguridad de la ISO 27001:2013. Estas permitirán llegar al detalle de cómo llevar a la práctica las políticas de seguridad. Se abre la puerta a un nuevo proyecto en este campo para la Dirección de Tecnología.

Las políticas de Seguridad de la Información deben ser revisadas periódicamente y ser socializadas con todo el personal para que se cree una cultura de seguridad al interior de la organización. También debe existir el apoyo de la Alta Dirección, tanto para la inversión de recursos para la implementación de los controles identificados que así lo requieren, como para el mantenimiento de los ya existentes que han demostrado efectividad.

BIBLIOGRAFIA

ARARAT MUÑOZ, Johanna Carolina. Diseño de un SGSI basado en la norma ISO 27001 para la empresa ma Peñalosa Cía. S.A.S. sede principal Cúcuta. Tesis de grado. Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería, Programa de Especialización de Seguridad Informática,2018. 153 p.

BUENAS TAREAS. Guía de estudios ETS seguridad informática. (En línea) (Citado el 16 de Mayo del 2019). Disponible en: http://www.buenastareas.com/ensayos/Horario-Voca-8-Segundo-Semestre/1513007.html

CAMARA DE COMERCIO DE CUCUTA. Información General Habeas Data, (En línea) (Citado el 16 de Octubre del 2013). Disponible en: http://www.cccucuta.org.co/secciones-128-s/informacion-general-habeas-data.htm

CARALLI Richard, et al. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. USA: Carnegie Mellon University, 2007. 154 p.

CARDONA, Jose Nayid y SALCEDO Willis Alberto. Análisis y evaluación de riesgos de seguridad informática Para la cámara de comercio de la dorada, puerto boyacá, puerto salgar y municipios de oriente de caldas. Tesis de grado. Universidad Nacional Abierta, Facultad de Ciencias Basicas, Departamento de Seguridad, 2017. 176 p.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley .1341 (30 de Julio 2009). por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de lastecnologías de la información y las comunicaciones. Bogota: El Congreso, 2009. 21 p.

-------. Ley 1273 de 2009.(enero 5). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado. Diario Oficial. Bogota: El Congreso, 2009. 2 p.

-------. Ley 527 de 1999 (agosto 18). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Diario Oficial. Bogota: El Congreso, 1999. 21 p.

-------. Ley estatutaria 1266 de 2008 (diciembre 31). por la cual se dictan las disposiciones generales del hábeas data. Bogota: El Congreso, 2008. 24 p.

COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. DECRETO NÚMERO 1317 DE 2013. "Por el cual se reglamenta parcialmente la Ley 1581 de 2012" Bogota: El Ministerio, 2013. 2 p.

ESTÁNDAR INTERNACIONAL ISO/IEC 17779. Tecnología de la información - Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información [en línea]. (citado s.n., 2011). Disponible en: https://mmujica.files.wordpress.com/2007/07/iso17799-2005-castellano.pdf

FAJARDO, Carmen Elizabeth. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano. Trabajo de grado. Bogota: Instituto Universitaria Politecnico Gran Colombiano, Facultad de Ingenierias, Departamento de Seguridad, 2017. 73 p.

GOBIERNO DE ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Catálogo de Elementos. Madrid: El Ministerio. 2012. 127 p.

ISO 27000.ES. El portal de ISO 27001 en Español. (En línea) (Citado el 16 de Mayo del 2018). Disponible en: http://www.iso27000.es/iso27000.html

ISO/IEC 27001. Information Technology - Security Techniques - Information Security Management Systems – Requirements. 2018 [En línea] Disponible en : https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

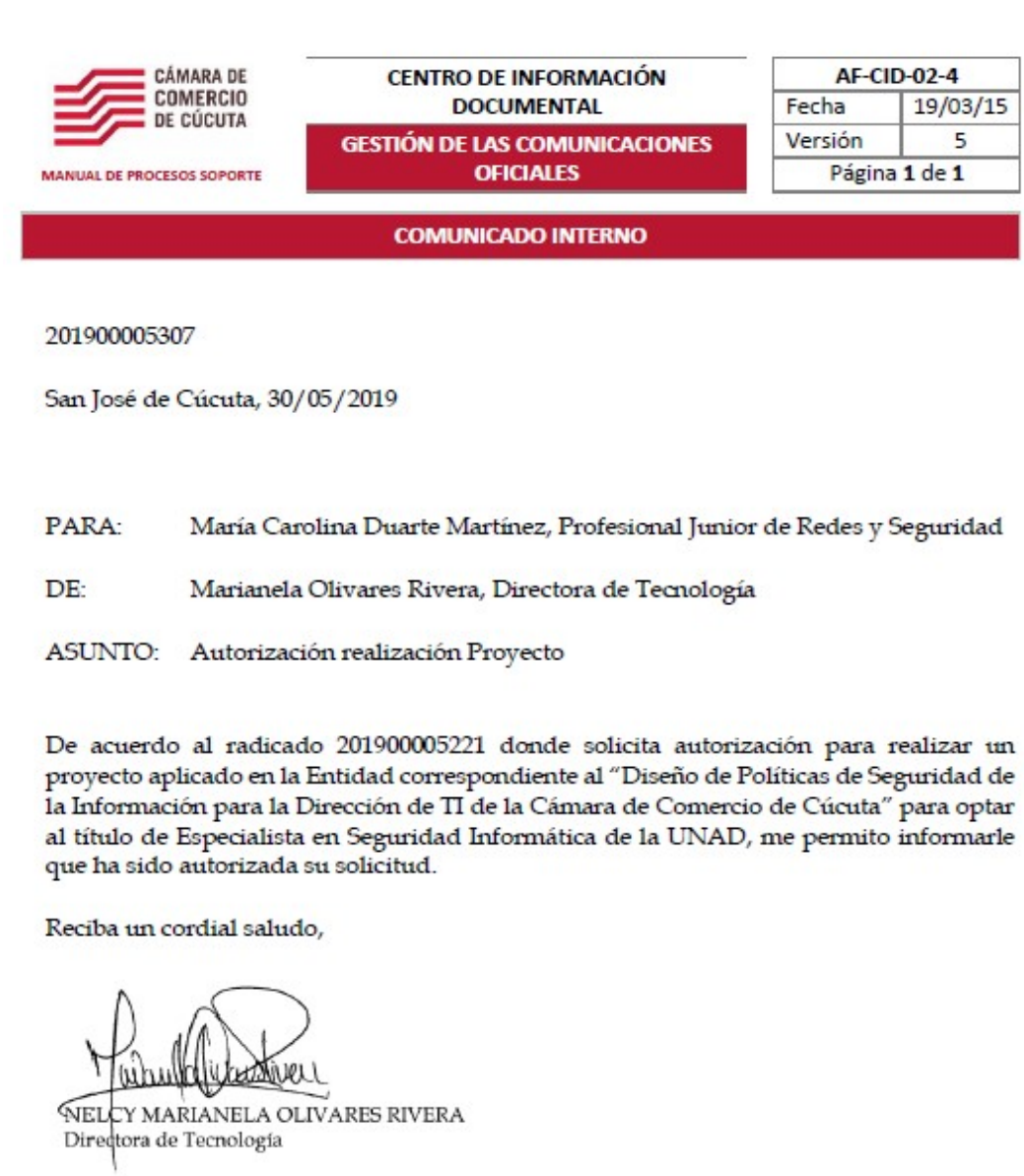
MARRUGO,RIVERA & ASOCIADOS. Manual de políticas y procedimientosde protección de datos personales. (En línea) (Citado el 16 de Octubre del 2016). Disponible en: http://www.cccucuta.org.co/media/habeas_data/manual_de_politicas_y_procedimientos_de_proteccion_de_datos_personales.pdf

ROUSE, Margaret. Information security management system (ISMS). (En línea) (Citado el 14 de Julio del 2018). Disponible en: https://whatis.techtarget.com/definition/information-security-management-system-ISMS

VANEGAS, Fair Hernando. Guía de auditoria basada en el análisis de riesgos a un centro de datos aplicando la metodología Magerit 3. Tesis de grado. Universidad Católica de Colombia, Facultad de Ingeniería, programa de especialista en sistemas, 2017. 168 p.

ANEXOS

Anexo A. Autorización



CÁMARA DE COMERCIO DE CÚCUTA

MANUAL DE PROCESOS SOPORTE

CENTRO DE INFORMACIÓN DOCUMENTAL	AF-CID-02-4	
GESTIÓN DE LAS COMUNICACIONES OFICIALES	Fecha	19/03/15
	Versión	5
	Página **1** de **1**	

COMUNICADO INTERNO

201900005307

San José de Cúcuta, 30/05/2019

PARA: María Carolina Duarte Martínez, Profesional Junior de Redes y Seguridad

DE: Marianela Olivares Rivera, Directora de Tecnología

ASUNTO: Autorización realización Proyecto

De acuerdo al radicado 201900005221 donde solicita autorización para realizar un proyecto aplicado en la Entidad correspondiente al "Diseño de Políticas de Seguridad de la Información para la Dirección de TI de la Cámara de Comercio de Cúcuta" para optar al título de Especialista en Seguridad Informática de la UNAD, me permito informarle que ha sido autorizada su solicitud.

Reciba un cordial saludo,

NELCY MARIANELA OLIVARES RIVERA
Directora de Tecnología

R	Responda para mi firma, por favor.		A	Aprobar (para su aprobación, por favor.)	
E	Encárguese del asunto, por favor		D	Divulgar (para conocimiento del personal)	
V	Verifique o revise, por favor.		O	Observaciones (devolver con observaciones)	
I	Infórmese, por favor.		C	Comentémoslo personalmente, por favor.	
S	Salir del trámite normal (Archivar)		Otro		

Anexo B. Procedimiento de instalación de servidores y/o software

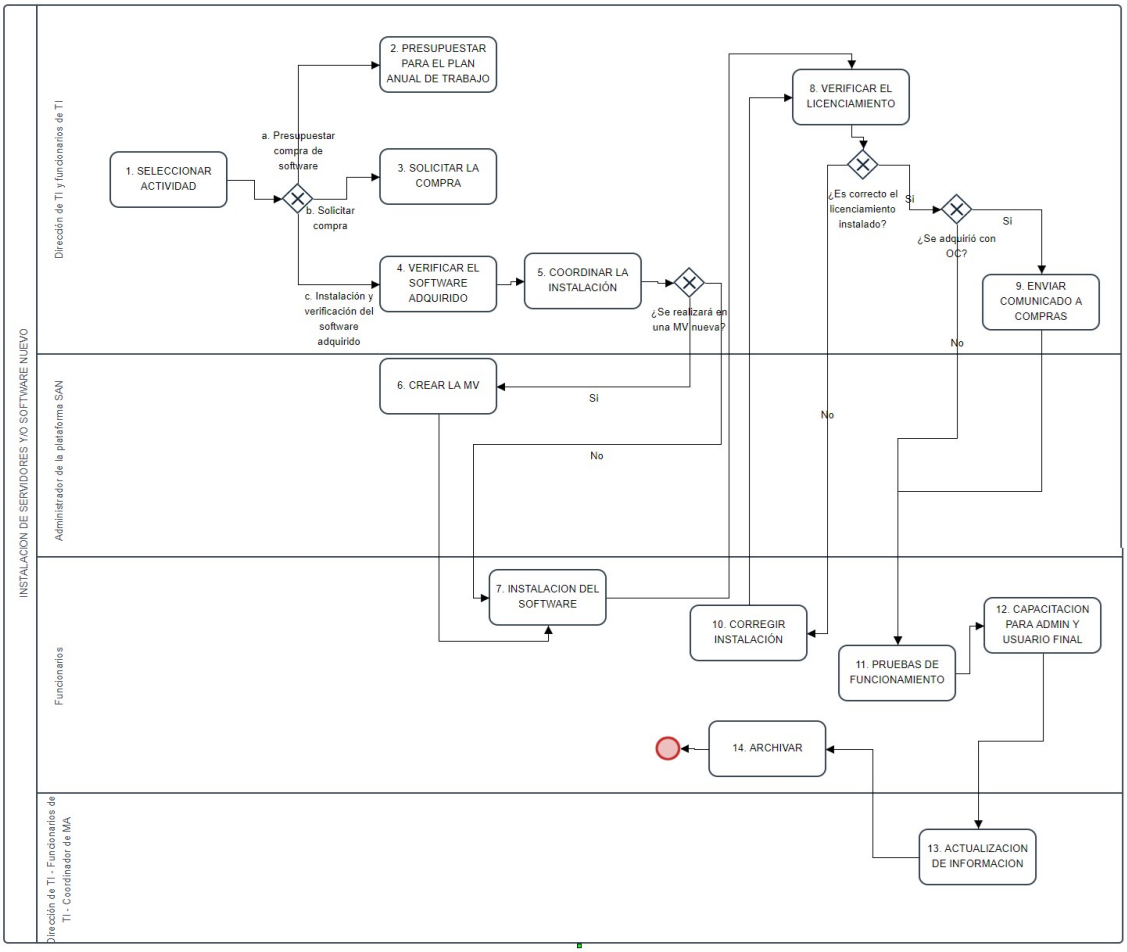
Objetivo.
Establecer el procedimiento a seguir para todas las instalaciones que se requieran dentro de la entidad, ya sea de servidores o de software nuevo para el funcionamiento de TI o de cualquiera de las gerencias y direcciones que componen la Cámara de Comercio de Cúcuta.

Alcance.
Aplicable a todas las máquinas virtuales (VM) y aplicativos para la entidad.

Definiciones.

- VM: Máquina virtual
- SO: Sistema Operativo
- MA: Mesa de Ayuda
- ADMIN: Usuario Administrador

Flujograma



ETAPA	DETALLE	RESPONSABLE	REGISTRO
1. SELECCIONAR ACTIVIDAD	• Se debe seleccionar que actividad se desea realizar: a. Presupuestar compra de software b. Solicitar compra c. Instalación y verificación del software adquirido	Dirección de TI Funcionarios de TI	
2. PRESUPUESTAR PARA EL PLAN ANUAL DE TRABAJO	• Se planifica en el presupuesto de la Dirección de T.I. y en el plan anual de trabajo el requerimiento de compra del aplicativo que se requiere para la plataforma de la entidad o por solicitud de un gerente de acuerdo con las necesidades de compra para la ejecución de las actividades de las gerencias. Alimentar los documentos registro.	Dirección de TI Funcionarios de TI	Presupuesto anual de TI Plan anual de trabajo de TI
3. SOLICITAR LA COMPRA	• Con las respectivas aprobaciones se realiza el proceso de compra en la fecha prevista en la planeación. Se inicia ruta de compras.	Dirección de TI Funcionarios de TI	Solicitudes de pedido
4. VERIFICAR EL SOFTWARE ADQUIRIDO	• Con el proveedor del software se hace la revisión correspondiente para	Dirección de TI Funcionarios de TI	Contrato, orden de compra y/o Actas de

ETAPA	DETALLE	RESPONSABLE	REGISTRO
	constatar que el software, aplicativo o licenciamiento adquirido es el que se está recibiendo y se solicitan los soportes a nombre de la Cámara de Comercio de Cúcuta. Si el software a instalar no requiere compra de licenciamiento porque es software libre, de igual manera se realiza las revisiones pertinentes validando el uso en la Entidad sin pago y descargar documento del fabricante que constate esta legalidad.		entrega o de inicio
5. COORDINAR LA INSTALACIÓN	• Se realiza la coordinación requerida ya sea con el proveedor del aplicativo para la instalación del software o con el ingeniero que corresponda en el área de TI de acuerdo con el perfil de lo adquirido. NOTA: La Dirección TI determina o asigna al ingeniero responsable de realizar la validación del proceso de instalación. El ingeniero de TI validará si se cuenta con los requerimientos para	Dirección de TI Funcionarios de TI	Informe de instalación

ETAPA	DETALLE	RESPONSABLE	REGISTRO
	la instalación correcta del aplicativo, con el licenciamiento del SO y los requisitos de memoria, disco duro y procesador. Ingeniero a cargo de la instalación: (listado de funcionarios de la Dirección de TI) La instalación del aplicativo se realizará en: a. Servidor nuevo b. Servidor existente Si la instalación es es un servidor nuevo diligenciar los siguientes campos: ✓ Nombre del servidor: ✓ Sistema Operativo: ✓ Memoria: ✓ Procesador: ✓ Disco Duro: ✓ Aplicaciones a instalar: Si la instalación es un servidor existente diligenciar los siguientes campos: ✓ Servidor: (lista de servidores existentes) ✓ Aplicación a instalar: Alimentar informe de		

ETAPA	DETALLE	RESPONSABLE	REGISTRO
	instalación.		
6. CREACION DE LA VM	Si la selección de la etapa 5 es la de "Servidor Nuevo" • De acuerdo con los requisitos se solicita al administrador de la SAN la creación de la respectiva VM asignando el nombre que se haya definido para la misma y que represente su función con el fin de que sea fácilmente identificable. Alimentar informe de instalación.	Funcionarios de TI	Informe de instalación
7. INSTALACION DEL SOFTWARE	• Se procede a instalar el aplicativo con el acompañamiento del proveedor si aplica. • Si la VM creada está con SO Windows Server se debe realizar la instalación del antivirus. Alimentar informe de instalación.	Funcionarios de TI	Informe de instalación
8. VERIFICAR EL LICENCIAMIENTO	• Se debe verificar que el licenciamiento sea el correcto y verificar si la licencia del SO está entre el stock de licencias de la CCC validando la versión y la clave con el listado de servidores y listado de licencias adquiridas que se lleva actualizado por	Dirección de TI Funcionarios de TI	Informe de instalación Listados de Servidores y de Licencias

ETAPA	DETALLE	RESPONSABLE	REGISTRO
	la Dirección de TI y actualizar los mismos en caso de nuevo licenciamiento. Seleccionar: ¿Es correcto el licenciamiento instalado? Si – No ¿Se adquirió con OC o contrato? Si- No Alimentar informe de instalación.		
9. ENVIAR COMUNICADO A COMPRAS	• Si el licenciamiento instalado es correcto y la adquisición fue por una compra, se envía comunicado interno al área de compras en el término de 45 días informando la instalación del software. •	Dirección de TI Funcionarios de TI	Comunicado en mercurio
10. CORREGIR LA INSTALACION	• Si el licenciamiento instalado no es correcto se procede a corregir la instalación con el proveedor Alimentar informe de instalación.	Funcionarios de TI	Informe de instalación
11. PRUEBAS DE FUNCIONAMIENTO	• Se realizan las pruebas de funcionamiento del aplicativo de acuerdo con los requerimientos planteados en el contrato o en la orden de compra.	Funcionarios de TI	Informe de instalación

ETAPA	DETALLE	RESPONSABLE	REGISTRO
	Alimentar informe de instalación.		
12. CAPACITACION PARA ADMIN Y USUARIO FINAL	• Se procede a recibir la capacitación por parte del proveedor a nivel de ADMIN y a nivel de Usuario Final. Alimentar informe de instalación.	Dirección de TI Funcionarios de TI	Informe de instalación
13. ACTUALIZACION DE INFORMACION	• Se debe crear la información tanto del software como del servidor creados con los respectivos soportes de licenciamiento y se debe actualizar el listado de servidores y listado de licencias para el control de intangibles de la CCC. Alimentar: Informe de instalación. Hoja de vida del servidor Listados de Servidores y de Licencias actualizados	Dirección de TI Funcionarios de TI Coordinador de MA	Informe de instalación Informe mensual de MA Listados de Servidores y de Licencias actualizados
14. ARCHIVAR	• Se procede a archivar los tipos documentales generados en el proceso	Funcionarios de TI	

DOCUMENTOS RELACIONADOS	
CÓDIGO	**NOMBRE**
XXXX	Informe de instalación
XXXX	Listados de Servidores y de Licencias actualizados
XXXX	Hoja de vida del servidor

REGISTROS RELACIONADOS	
CÓDIGO	**NOMBRE**

CONTROL DE CAMBIOS		
FECHA	**VERSIÓN**	**RAZÓN DEL CAMBIO**
DD/MM/AA/	1	Versión Original

ELABORÓ.	REVISÓ.	APROBÓ.
Andrea Emiliana Cárdenas Silva	**Marianela Olivares Rivera**	**Marianela Olivares Rivera**

Anexo C. Caracterización de los procesos

CÁMARA DE COMERCIO DE CÚCUTA

MANUAL DE GESTIÓN Y CONTROL

CARACTERIZACIÓN POR PROCESOS

TECNOLOGIA DE LA INFORMACIÓN

C.CR.08	
Fecha:	09/06/2018
Versión:	1
Página 1 de 5	

	Gerenciales
	Misionales
	De Apoyo

RESPONSABLE: Director de TI

OBJETIVO: Ser aliado estratégico en el logro de las metas institucionales implementando tecnologías, estándares y herramientas informáticas de última generación, siguiendo un plan estructurado que asegure servicios ágiles y oportunos con integridad, calidad y seguridad en la información con el fin de asegurar el mejoramiento continuo de los procesos y el uso adecuado de la infraestructura de la entidad.

Factores Claves de Éxito

- Eficiencia en soporte y atención de usuarios
- Disponibilidad de la infraestructura
- Integridad y seguridad de la información
- Transformación Digital Interna

CLIENTES / GRUPOS DE INTERÉS – REQUISITOS / NECESIDADES / EXPECTATIVAS

Alta Dirección

- Apoyo nuevo direccionamiento estratégico con la Transformación Digital interna

Procesos internos

Plataforma para la ejecución de los procesos a través de las aplicaciones que facilitan el desempeño de las funciones

Usuarios / clientes externos / grupos de interés

Atención oportuna y eficiente a las solicitudes de clientes internos y externos

PROVEEDORES	INSUMOS	PROCESO	PRODUCTOS	CLIENTES Y/O GRUPOS DE INTERÉS
Todos los procesos	Inventario de equipos	**Mantenimiento preventivo de equipos:** • Identificar y programar equipos para mantenimiento preventivo • Validar agendamiento o tarea • Ejecutar actividades programadas y verificación • Verificar funcionamiento del equipo • Informar el cumplimiento del mantenimiento, medir y archivar	Cronograma de mantenimientos Informe de ejecución de mantenimiento	Todos los procesos
Todos los procesos	Solicitud de incidencia por parte del usuario	**Solicitud de soporte técnico:** • Recibir la solicitud del usuario y asignar responsable de la solución, • Atender solicitud y describir la solución, • Calificar el servicio, • Revisar satisfacción del usuario y archivar	Incidencia asignada y cerrada Reporte de calificaciones	Todos los procesos
Todos los procesos	Solicitud de instalación	**Instalación de aplicativos:** • Validar aplicativo por Director de ti • Revisar solicitud, verificar su licenciamiento y Asignar responsable de la instalación • Atender solicitud y describir la solución, • Calificar el servicio, • Confirmar instalación y archivar en hoja de vida del aplicativo	Incidencia asignada y cerrada Reporte de calificaciones Listado de licenciamiento actualizado Hoja de vida de equipo actualizado	Todos los procesos
Todos los procesos	Solicitud de actualización	**Actualizaciones de aplicaciones en estaciones de trabajo:** • Revisar solicitud, verificar su licenciamiento y Asignar responsable de la actualización, • Atender solicitud y describir la solución, • Calificar el servicio, • Revisar satisfacción del usuario y archivar	Incidencia asignada y cerrada Reporte de calificaciones Listado de licenciamiento actualizado Hoja de vida de equipo actualizado	Todos los procesos

PROVEEDORES	INSUMOS	PROCESO	PRODUCTOS	CLIENTES Y/O GRUPOS DE INTERÉS
Todos los procesos	Inventario de servidores	**Registro de backups:** • Programación de backups automáticos a realizarse en cada servidor o cada aplicación • Verificación de la realización de backups automáticos, enviar backups magnéticos • Registrar monitoreos realizados e informar • Almacenar	Programación de backups y respaldos para cada servidor Registro de monitoreos	Todos los procesos

INTERRELACIONES	PROCESOS DE SOPORTE	PARÁMETROS/ MEDICIÓN/ SEGUIMIENTO				RECURSOS	REQUISITOS
		PERSPECTIVA	CÓD.	INDICADOR	ÍNDICE		
AUTORIDAD Presidente Ejecutivo **EJECUTA** Dirección de TI	Administrativo y Financiero	3. Perspectiva interna del negocio	3.7.A	Disponibilidad de los recursos Tecnológicos	(Disponibilidad de aplicativos + disponibilidad de Hardware + Disponibilidad de Servidores / 3)	Fungibles de oficina, Financieros Tecnológicos	**ISO 9001:2015** 7.1.3 Infraestructura
			3.8.A	Actualización tecnológica	Recursos tecnológicos ajustados a las necesidades de la Entidad / Total recursos tecnológicos		
				Cumplimiento Mantenimiento preventivo de equipos	(Mantenimientos ejecutados/Mantenimientos planeados) * 100		**Sistema Cameral de Control Interno SCCI** 3.6 Control sistemas de información 4.1 Sistemas de información

CÓDIGO	DOCUMENTO	CÓDIGO	REGISTRO
MPA-0401	Mantenimiento preventivo y correctivo de equipos de trabajo		
MPA-0402	Administrador del servidor		
MPA-0403	Registro de Backups		
MPA-0404	Manuales de contingencia		
MPA-0405	Solicitud de soporte técnico		
	Instalación de aplicativos		
	Actualización de aplicativos		
	Normograma		