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

JOSÉ NAYID CARDONA CASTAÑEDA
WILLIS ALBERTO SALCEDO RUIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LA DORADA, CALDAS
2017

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

JOSÉ NAYID CARDONA CASTAÑEDA
WILLIS ALBERTO SALCEDO RUIZ

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

MARTIN CAMILO CANCELADO RUIZ
DIRECTOR DE PROYECTO DE GRADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LA DORADA, CALDAS
2017

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

La Dorada, Caldas, 14 de junio de 2017

AGRADECIMIENTOS

A mi esposa Lucero quien siempre me ha brindado su apoyo incondicional y a mis hijos Diego Alejandro y Santiago que son el motor que me impulsa a seguir adelante, a ellos agradezco su paciencia ya que he tomado parte del tiempo destinado a ellos y así poder lograr esta meta.
.

José Nayid Cardona Castañeda

Al iniciar este proyecto de vida, sabía que necesitaría de mi esposa Luz Dary y de mi hijo Willis David, para ellos mis agradecimientos por los momentos de apoyo, desvelos y fuerza de voluntad que me brindaron, para que alcanzara esta meta.

Willis Alberto Salcedo Ruiz

A los tutores que gracias a sus conocimientos y estímulo permitieron que este proyecto sea una realidad.

CONTENIDO

LISTAS DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

Debido a su crecimiento y la normatividad contemplada en la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013, Decreto 2042 de 2014 y al Código de Comercio, la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas, debe implementar sus Políticas de Seguridad Informática, y actualmente se carece de estas, se tienen un documento con algunas políticas, pero estas se quedan cortas ya que solo consideran aspectos muy básicos relativos a la seguridad de la información, el único inventario con que se cuenta es el que manejan en el área contable, el cual nada tiene que ver un inventario de activos de información.

Ante este panorama se hace necesario realizar un análisis y evaluación de riesgos, para lo cual se realiza un inventario de activos de información, se determinan las amenazas y vulnerabilidades a que está expuesta la organización, aplicando Magerit V3, luego se realiza el análisis y evaluación de los riesgos, se verifica también la existencia de controles de acuerdo a las normas ISO 27001:2013 e ISO 27002:2013 y de acuerdo a los resultados obtenidos se realiza el documento entregable con los hallazgos y controles a implementar.

Palabras Claves:

- EAR/PILAR
- Inventario de Activos de Información
- ISO 27001
- ISO 27002
- Magerit
- Riesgos

INTRODUCCIÓN

Las Cámaras de Comercio son entidades de tipo gremial con carácter privado que manejan recursos públicos. La Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas cuenta con una jurisdicción que comprende nueve municipios en tres departamentos.

Dado el buen manejo de los recursos públicos el Gobierno Nacional ha ido delegando en ellas nuevas funciones. Esto ha hecho que la responsabilidad sea cada vez mayor, debiendo cubrir necesidades de los empresarios además de las contempladas en la ley.

Esto ha ocasionado preocupación en la Alta Gerencia ya que en la actualidad para nadie es un secreto los peligros a los cuales están expuestas las empresas en el manejo de la información, estos riesgos se pueden presentar por varias razones como el acceso no autorizado a la misma, o manejo inadecuado de la información, por eso se hace necesario realizar un análisis de vulnerabilidades y amenazas.

Por esta razón se plantea realizar un protocolo basado en la norma ISO 27001:2013 teniendo en cuenta la importancia de la seguridad la cual se debe aplicar en todos los ámbitos de la empresa.

1 PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Debido a su crecimiento y la normatividad contemplada en la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013, Decreto 2042 de 2014 y al Código de Comercio, la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas, debe implementar sus Políticas de Seguridad Informática, ya que actualmente carece de estas, lo cual hace que cada funcionario maneje los riesgos según su parecer personal, esto abre una gran brecha en materia de seguridad ya que existe disparidad de criterios y permite que se puedan presentar situaciones que podrían acarrear sanciones económicas por parte de los entes de control e incluso dependiendo la gravedad determinar el cierre.

La alta gerencia de la entidad, está comprometida con brindar a sus clientes la seguridad que demandan, para lo cual se han realizado inversiones en equipos, que se suman a los existentes y que se entienden por obsoletos, sin embargo, esto contrario a lo esperado no ha sido la solución, ya que de todas formas se siguen presentando amenazas, que comprometen la seguridad no sólo de la información si no de la red en general.

En la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas la red carece de la suficiente seguridad ya que adolece de mecanismos adecuados para blindarla y proteger la información institucional; los usuarios no tienen una política clara en lo referente al manejo de las contraseñas, la gran mayoría tiene un par y las va rotando cada vez que se le pide realizar el cambio de la misma, los accesos inalámbricos solo tienen un autenticación WPA/WPA2 y la clave está difundida incluso a personal externo, todo esto hace que esté expuesta a ataques o accesos no autorizados.

1.2 DESCRIPCIÓN DEL PROBLEMA

En la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas, se cuenta con personal idóneo en sus funciones, sin embargo, esta misma condición hace que los funcionarios intenten por su propia cuenta solucionar las incidencias que se presentan, sin reportarlas a los funcionarios que realmente son los indicados para realizar los procesos de solución, los cuales deberían ser documentados de forma correcta, para determinar a futuro cual es la razón por la cual se está presentando la incidencia y tomar los correctivos necesarios.

Dentro de los problemas presentados, se pueden destacar los siguientes:

- Intentos de accesos no autorizados a los servidores ya que el nivel de protección con que se cuenta, no brinda la suficiente protección.

- Continuos bloqueos de los enrutadores inalámbricos y ha sido necesario configurarlos nuevamente o al menos reiniciarlos.

- Falta de una política institucional para el manejo de contraseñas para redes inalámbricas, ya que estas permanecen sin cambio durante mucho tiempo o sea que cambian de acuerdo al parecer del personal encargado del área técnica.

- La gran mayoría de funcionarios tiene sus propias memorias USB y estas son conectadas sin ningún tipo de protección en los equipos de la institución.

- En general faltan políticas claras en cuanto al manejo de la infraestructura tecnológica de la Cámara de Comercio.

1.3 FORMULACIÓN DEL PROBLEMA

¿Cómo los resultados del análisis y evaluación de riesgos ayudarán a disminuir las vulnerabilidades y amenazas de seguridad informática a través de un sistema de control que incluya políticas y procedimientos para la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas?

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Disminuir las vulnerabilidades y amenazas de seguridad informática a través de un sistema de control que incluya políticas y procedimientos de acuerdo a los resultados del análisis y evaluación de riesgos en la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas.

2.2 OBJETIVO ESPECÍFICOS

- Recopilar información para conocer la situación actual de la Cámara de Comercio, para determinar los riesgos de seguridad.

- Determinar los activos informáticos con que cuenta la Cámara de Comercio y que son usados para el manejo de la información.

- Realizar el proceso de análisis y evaluación de los riesgos a que está expuesta la organización debido a las vulnerabilidades y amenazas existentes usando la metodología MAGERIT de gestión de riesgo informático.

- Presentar informe detallado de resultados obtenidos durante la aplicación de los instrumentos de análisis y determinar los controles para mitigar los riesgos a que está expuesta la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas.

3 JUSTIFICACIÓN

Dado que la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas es una entidad gremial, de carácter privado, y tiene dentro de sus objetivos prestar servicios registrales delegados por el Estado con eficiencia y efectividad, promoviendo programas y proyectos dirigidos al desarrollo y la competitividad regional, se hace necesario garantizar la disponibilidad, confidencialidad e integridad de los recursos informáticos que tienen a cargo los funcionarios.

Al conocer las vulnerabilidades y amenazas a la que está expuesta la Cámara de Comercio en seguridad de la información, se podrá ofrecer un mejor servicio a los ciudadanos que utilizan cotidianamente los trámites.

Los 25 funcionarios de la Cámara de Comercio, tendrán herramientas que les permitirán apropiarse de forma profesional de sus funciones.

Continuar con el esquema actual de trabajo, sólo llevará a que en el futuro sea necesario una reestructuración de procesos y procedimientos, que en su mayoría estarán enfocados a solucionar problemas causados por la falta de seguridad de la información.

4 ALCANCE Y DELIMITACIÓN

El análisis y evaluación de riesgos se realizará específicamente sobre los activos de información de la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas, para identifica los riesgos y amenazas, así como también medir su impacto hacia la organización.

El desarrollo del proyecto se llevará a cabo en la sede principal de la Cámara de Comercio, ubicada en La Dorada, Caldas, ya que allí es donde se encuentra la mayor parte de activos de información. El proyecto se realizará entre los meses de abril a noviembre del 2016.

5 MARCO DE REFERENCIA

5.1 ANTECEDENTES

El documento, “Guía de Seguridad ICC para los negocios” emanado de la organización empresarial mundial Cámara de Comercio Internacional, aborda de manera detallada y profesional gran cantidad de temas con respecto a la seguridad de la información, destacándose el capítulo “seis medidas esenciales de seguridad”.

El manual “Políticas de Seguridad de la Información”, de la Cámara de Comercio de Dos Quebradas”, es un documento que permite visualizar el resultado final de un análisis de riesgos y vulnerabilidades bien aplicado a una entidad.

El proyecto denominado “Implementación de Sistema de Gestión de Seguridad de la Información aplicada al área de recursos humanos de la empresa DECEVALE S.A.”, presentado por Diana Onofre, Martin Estrella y Manuel Flores en la Escuela de Diseño y Comunicación Visual (Ecuador). Este proyecto se utilizará como guía para la conocer las etapas en la implementación de un SGSI.

El proyecto “Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la Empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala”, presentado por Karina del Rocío Gaona Vásquez en la Universidad Politécnica Salesiana en la ciudad de Cuenca (Ecuador). Este proyecto se utilizará como guía para la aplicación de la Metodología Magerit para la en el análisis de riegos se seguridad en la información

5.2 MARCO CONTEXTUAL

5.2.1 Reseña histórica.

La Cámara de Comercio de La Dorada es una persona jurídica sin ánimo de lucro, de carácter corporativo y gremial, está sujeta en todas sus actuaciones administrativas, de gestión y contratación al derecho privado, tiene como finalidad defender y apoyar los intereses gremiales de los empresarios, también maneja el registro mercantil, de entidades sin ánimo de lucro y el registro único de proponentes delegados por el estado, sin ser una entidad de orden público.

La Cámara de Comercio de La Dorada fue creada mediante el decreto 75 del 13 de enero de 1961, la denominación que recibió desde ese entonces fue el de Cámara de Comercio de La Dorada, y su jurisdicción inicial fue La Dorada en el Departamento de Caldas y Puerto Salgar en Cundinamarca, luego le fueron agregados varios municipios del Oriente de Caldas y Puerto Boyacá en el departamento de Boyacá.

Con el Decreto 622 de 2000 su jurisdicción comprende los municipios de La Dorada, Manzanares, Marquetalia, Pensilvania, Samaná y Victoria, en el departamento de Caldas, Puerto Boyacá en el departamento de Boyacá y Puerto Salgar, en el departamento de Cundinamarca.

De conformidad con el Decreto Número 0018 de enero 10 de 2012, expedido por el Ministerio de Comercio, Industria y Turismo, se decretó el cambio de nombre de la Cámara de Comercio de La Dorada por el de CÁMARA DE COMERCIO DE LA DORADA, PUERTO BOYACA, PUERTO SALGAR Y ORIENTE DE CALDAS.

En la actualidad cuenta con varias sedes distribuidas así:

- Sede Principal en La Dorada, Caldas.
- Punto de Atención al Comerciante en Puerto Boyacá, Boyacá.
- Punto de Atención al Comerciante en Manzanares, Caldas.
- Punto de Atención al Comerciante en Pensilvania.
- Punto de Atención al Comerciante en Samaná, Caldas.
- Punto de Atención al Comerciante en Marquetalia, Caldas

5.2.2 Misión.

"Somos una entidad gremial, Privada, que presta los servicios registrales delegados por el Estado con eficiencia y efectividad, promoviendo programas y proyectos dirigidos al desarrollo y la competitividad regional"[1].

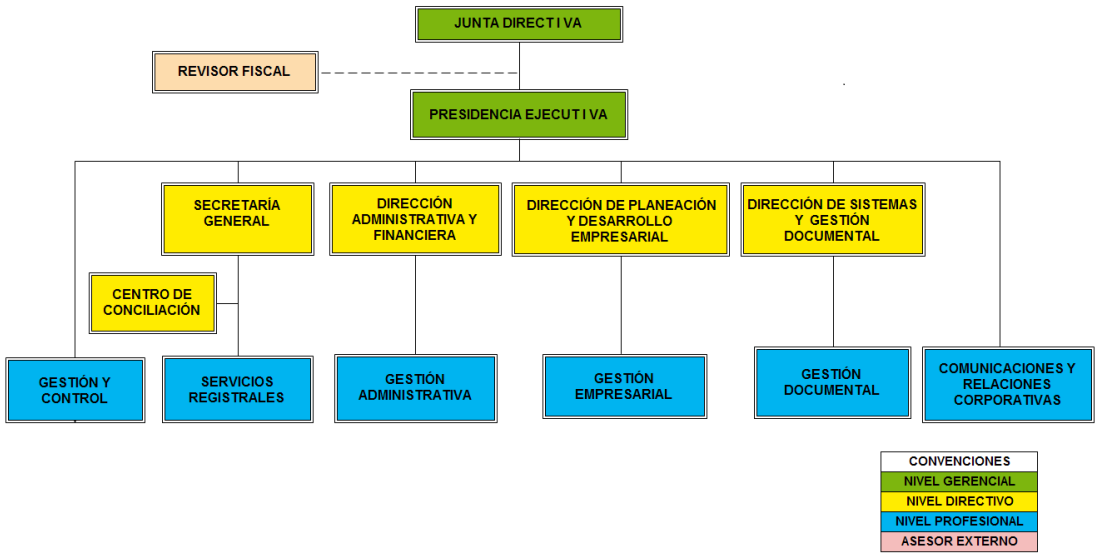
5.2.3 Visión.

"En el año 2017 seremos una entidad sostenible y líder en el ámbito empresarial y regional, que genera oportunidades para el desarrollo y la competitividad, posicionándose a nivel nacional con una infraestructura tecnológica y administrativa óptima y un talento humano capacitado y comprometido"[2].

5.2.4 Estructura organizacional.

[1] Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. (2016).
[2] Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. (2016).

Figura 1. Estructura Organizacional CCD



Fuente: http://www.camaradorada.org.co/version2/wp-content/uploads/2016/02/ORGANIGRAMA-sin-cod.png

5.3 DESCRIPCIÓN DE LA ACTIVIDAD DE LA CÁMARA DE COMERCIO

Como parte de las funciones delegadas por el Estado, ponemos enumerar:

1. Llevar los registros públicos encomendados a ellas por la ley y certificar sobre los actos y documentos allí inscritos.

2. Recopilar y certificar la costumbre mercantil mediante investigación realizada por cada Cámara de Comercio dentro de su propia jurisdicción. La investigación tendrá por objeto establecer las prácticas o reglas de conducta comercial observadas en forma pública, uniforme, reiterada y general, siempre que no se opongan a normas legales vigentes.

3. Crear centros de arbitraje, conciliación y amigable composición por medio de los cuales se ofrezcan los servicios propios de los métodos alternos de solución de conflictos, de acuerdo con las disposiciones legales.

4. Adelantar acciones y programas dirigidos a dotar a la región de las instalaciones necesarias para la organización y realización de ferias, exposiciones, eventos artísticos, culturales, científicos y académicos, entre otros, que sean de interés para la comunidad empresarial de la jurisdicción de la respectiva Cámara de Comercio.

5. Participar en la creación y operación de centros de eventos, convenciones y recintos feriales de acuerdo con lo dispuesto en la Ley 1558 de 2012 y las demás normas que las sustituyan, modifiquen o adicionen.

6. Promover la formalización, el fortalecimiento y la innovación empresarial, así como desarrollar actividades de capacitación en las áreas comercial e industrial y otras de interés regional, a través de cursos especializados, seminarios, conferencias y publicaciones.

7. Promover el desarrollo regional y empresarial, el mejoramiento de la competitividad y participar en programas nacionales de esta índole.

8. Promover la afiliación de los comerciantes inscritos que cumplan los requisitos señalados en la ley, con el fin de estimular la participación empresarial en la gestión de las cámaras de comercio y el acceso a los servicios y programas especiales.

9. Prestar servicios de información empresarial originada exclusivamente en los registros públicos, para lo cual podrán cobrar solo los costos de producción de la misma.

10. Prestar servicios remunerados de información de valor agregado que incorpore datos de otras fuentes.

11. Desempeñar y promover actividades de veeduría cívica en temas de interés general de su correspondiente jurisdicción.

12. Promover programas, y actividades en favor de los sectores productivos de las regiones en que les corresponde actuar, así como la promoción de la cultura, la educación, la recreación y el turismo.

13. Participar en actividades que tiendan al fortalecimiento del sector empresarial, siempre y cuando se pueda demostrar que el proyecto representa un avance tecnológico o suple necesidades o implica el desarrollo para la región.

14. Mantener disponibles programas y servicios especiales para sus afiliados.

15. Disponer de los servicios tecnológicos necesarios para el cumplimiento y debido desarrollo de sus funciones registrales y la prestación eficiente de sus servicios.

16. Publicar la noticia mercantil de que trata el numeral 4 del artículo 86 del Código de Comercio, que podrá hacerse en los boletines u órganos de publicidad de las cámaras de comercio, a través de Internet o por cualquier medio electrónico que lo permita.

17. Realizar aportes y contribuciones a toda clase de programas y proyectos de desarrollo económico, social y cultural en el que la nación o los entes territoriales,

así como sus entidades descentralizadas y entidades sin ánimo de lucro tengan interés o hayan comprometido sus recursos.

18. Participar en programas regionales, nacionales e internacionales cuyo fin sea el desarrollo económico, cultural o social en Colombia.

19. Gestionar la consecución de recursos de cooperación internacional para el desarrollo de sus actividades.

20. Prestar los servicios de entidades de certificación previsto en la Ley 527 de 1999, de manera directa o mediante la asociación con otras personas naturales o jurídicas.

21. Administrar individualmente o en su conjunto cualquier otro registro público de personas, bienes, o servicios que se deriven de funciones atribuidas a entidades públicas con el fin de conferir publicidad a actos o documentos, siempre que tales registros se desarrollen en virtud de autorización legal y de vínculos contractuales de tipo habilitante que celebren con dichas entidades.[3]

5.4 MARCO TEÓRICO

5.4.1 ISO2007/ISO 27001.

- ISO 27000: Contiene el vocabulario o definiciones que se utiliza en la implementación de SGSI (Sistema de Gestión de la Seguridad de la Información), es similar a la norma ISO 9000 que contiene el vocabulario para la implementación de un SGC (Sistema de Gestión de la Calidad).

- ISO 27001, en esta norma se recopilan los requerimientos para implementar un SGSI (Sistema de Gestión de la Seguridad de la Información), tiene en común con la norma ISO 9001 que esta muestra los requerimientos para crear un SGC (Sistema de Gestión de la Calidad).

5.4.2 Magerit.

Es una metodología para análisis y control de riesgos creada por el Consejo Superior de Administración Electrónica, aplicable a las Tecnologías de Información y dirigida a las Administraciones Públicas.

Para realizar el análisis de riesgo se deben seguir los siguientes pasos:

[3] Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. (2016). Funciones y Deberes. Cámara de Comercio de La Dorada.

- Realizar un inventario de activos de información.
- Identificar las amenazas a los que se encuentran expuestos los activos.
- Determinar las salvaguardas e identificar que tan eficaces son frente a los riesgos.
- Estimar el impacto en caso de materializarse alguna amenaza.
- Estimar el riesgo

5.4.3 Metodología de análisis de riesgos informáticos.

Objetivos de las metodologías

Existen varios enfoques para realizar el análisis de riesgos, en esencia, suelen dividirse en dos tipos fundamentales: Cuantitativos y Cualitativos.

- **Enfoque cuantitativo del análisis de riesgos.**

Este enfoque emplea dos elementos fundamentales, la probabilidad de que se produzca un evento y el impacto que ocasionaría la probable pérdida en caso de que ocurra el citado evento.

El enfoque cuantitativo de análisis de riesgos consiste en la obtención de un valor a partir del producto de estos elementos. La forma de calcularlo, para un evento dado, es realizando la multiplicación del valor de la pérdida potencial por el valor de la probabilidad de ocurrencia. De esta manera es prácticamente concreto y posible valorar los eventos y calcular el riesgo a fin de tomar las decisiones correspondientes.

- **Análisis de las metodologías Magerit, Octave y Mehari.**

Existen varias metodologías para el análisis de riesgos, las más conocidas son Magerit, Octave y Mehari.

- **Principales elementos de Magerit.**

    - Escalas de valores cualitativos, cuantitativos y de indisponibilidad del servicio.
    - Modelo de frecuencia de una amenaza como una tasa anual de ocurrencia.
    - Escala alternativa de estimación del riesgo.
    - Catálogos de amenazas
    - Catálogos de medidas de control

- **Principales elementos de Octave.**

- Medidas de probabilidad considerando un rango de frecuencias.
- Análisis del límite entre niveles de probabilidad.

- **Principales elementos de Mehari.**

  - Niveles de categorías de controles
  - Niveles de calidad de los servicios de seguridad
  - Evaluación de la calidad del servicio por medio de cuestionarios
  - Tabla modelo de impactos

5.4.4 EAR /PILAR. Entorno Análisis de Riesgos / Procedimiento Informático y Lógico de Análisis de Riesgos. Las herramientas EAR soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit.

En esencia son un conjunto de herramientas para realizar un análisis general, sobre las diversas dimensiones de seguridad (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) o un análisis de la continuidad, centrado en la disponibilidad del sistema, buscando reducir los tiempos de interrupción del servicio cuando sobrevienen desastres. EAR/PILAR ha sido parcialmente financiada por el Centro Criptológico Nacional.

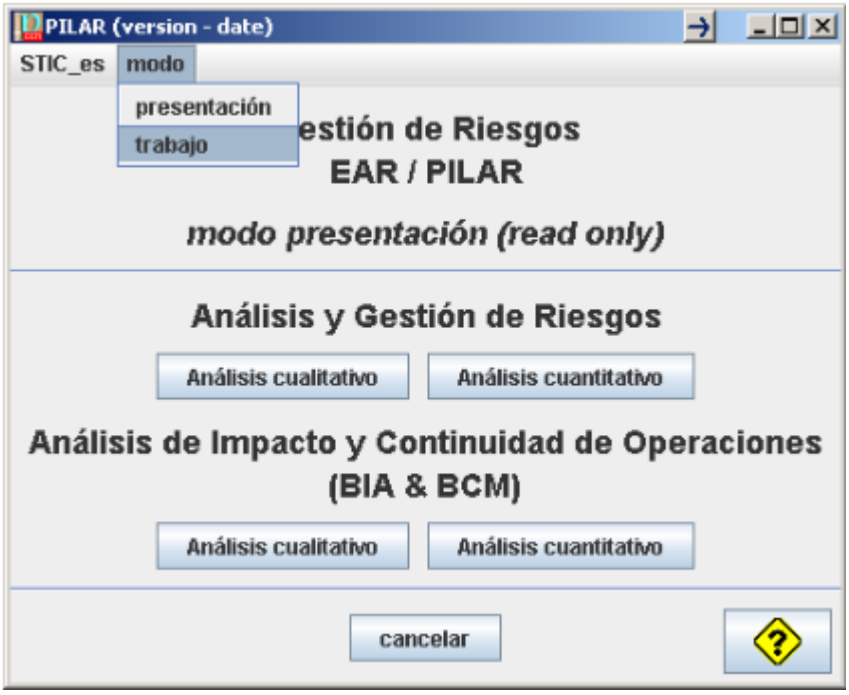
PILAR dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son:

- Esquema Nacional de Seguridad.
- ISO/IEC 27002:2005.

Para tratar el riesgo se proponen:

- Salvaguardas o contramedidas.
- Elementos de respaldo (backup).
- Planes de recuperación de desastres.

Figura 2. Interfaz de trabajo de PILAR



Fuente: http://www.ar-tools.com/es/tools/pilar/first_time/index.html

5.4.5 Seguridad de la información. Hace referencia a las técnicas que se utilicen para brindar protección al sistema informático, es decir configurar los sistemas con antivirus, controles de seguridad desde el mismo sistema operativo, que garanticen la integridad de los datos y además su privacidad.

Se plantea la necesidad de un marco de seguridad y privacidad de la información que esté orientado a preservar los pilares fundamentales de la seguridad de la información.

5.4.6 Seguridad Informática. Es la aplicación de instrumentos técnicos destinados a proteger la información como antivirus, firewall, detección de intrusiones, etc.

La seguridad informática se resume, por lo general, en cinco objetivos principales:

- **Integridad**: garantizar que los datos sean los que se supone que son.
- **Confidencialidad**: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.
- **Disponibilidad**: garantizar el correcto funcionamiento de los sistemas de información.
- **Evitar el rechazo**: garantizar de que no pueda negar una operación realizada.

- **Autenticación**: asegurar que sólo los individuos autorizados tengan acceso a los recursos.

5.5 MARCO CONCEPTUAL

- **Confidencialidad**. La confidencialidad consiste en hacer que la información sea ininteligible para aquellos individuos que no estén involucrados en la operación.

- **Integridad.** La verificación de la integridad de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente).

- **Disponibilidad.** El objetivo de la disponibilidad es garantizar el acceso a un servicio o a los recursos.

- **No repudio.** Evitar el repudio de información constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada.

- **Autenticación.** La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite garantizar el acceso a recursos únicamente a las personas autorizadas.

- **Necesidad de un enfoque global.** Frecuentemente, la seguridad de los sistemas de información es objeto de metáforas. A menudo, se la compara con una cadena, afirmándose que el nivel de seguridad de un sistema es efectivo únicamente si el nivel de seguridad del eslabón más débil también lo es. De la misma forma, una puerta blindada no sirve para proteger un edificio si se dejan las ventanas completamente abiertas.

- **Vulnerabilidad**: Debilidad de un sistema al permitir a un atacante violar la confidencialidad, disponibilidad, control de acceso y consistencia del sistema o de los datos.

- **Trazabilidad:** Propiedad que permite hace seguimiento a los datos, para poder determinar quién hace que, cuando y donde.[4]

[4] Cámara de Comercio de Dos Quebradas (2016). Política de Seguridad de la Información.

5.6 MARCO LEGAL

Las Cámaras de Comercio se rigen por el siguiente marco normativo:

- Ley 1727 de 2014 y Decreto 1074 de 2015: Por la cual se reforma el Código de Comercio, se fijan normas para el fortalecimiento de la Gobernabilidad y el Funcionamiento de las Cámaras de Comercio y se dictan otras disposiciones.

- Código de Comercio de Colombia del artículo 26 al 47 y del 78 al 97: Art 26 a 47. LIBRO PRIMERO, TITULO III, DEL REGISTRO MERCANTIL y Art. 78 a 97. LIBRO PRIMERO, TITULO VI, DE LAS CAMARAS DE COMERCIO.

- Circular Única de la Superintendencia de Industria y Comercio: Ley 1429 de 2010, Por el cual se expide la Ley de Formalización y Generación de Empleo.

- Decreto reglamentario 545 de 2011 y Decreto reglamentario 489 de 2013: Por el cual se reglamentan parcialmente los artículos 5, 7, 48 y 50 de la Ley 1429 de 2010, y Por el cual se reglamenta parcialmente la Ley 1429 de 2010, respectivamente.

- Decreto Ley 019 de 2012 - Reglamentado por el Decreto Nacional 734 de 2012, Reglamentado por el Decreto Nacional 1450 de 2012, Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

- Ley 1607 de 2012 art 182, “De la tasa contributiva a favor de las Cámaras de Comercio”.

- Decreto - Ley 2150 de 1995: Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.

- Ley 643 de 2001: Reglamentada parcialmente por los Decretos Nacionales 2975 de 2004; 855 de 2009 y 1289 de 2010, Modificada por el art. 36, Decreto Nacional 126 de 2010, en lo relativo a las multas, Reglamentada por el Decreto Nacional 3034 de 2013 por la cual se fija el régimen propio del monopolio rentístico de juegos de suerte y azar.

- Ley 850 de 2003: Por medio de la cual se reglamentan las veedurías ciudadanas.

- Ley 1101 de 2006: Por la cual se modifica la Ley 300 de 1996 – Ley General de Turismo y se dictan otras disposiciones.

- Decreto 2893 de 2011: Por el cual se modifican los objetivos, la estructura orgánica y funciones del Ministerio del Interior y se integra el sector administrativo del interior.

- Ley 454 de 1998: Por la cual se determina el marco conceptual que regula la economía solidaria, se transforma el Departamento Administrativo Nacional de Cooperativas en el Departamento Nacional de la Economía Solidaria, se crea la Superintendencia de la Economía Solidaria, se crea el Fondo de Garantías para las Cooperativas Financieras y de Ahorro y Crédito, se dictan normas sobre la actividad financiera de las entidades de naturaleza cooperativa y se expiden otras disposiciones.

- Ley 80 de 1993: Reglamentada por el Decreto Nacional 734 de 2012, Modificada por la Ley 1150 de 2007, Reglamentada parcialmente por los Decretos Nacionales 679 de 1994, 626de 2001, 2170 de 2002, 3629 y 3740 de 2004, 959, 2434 y 4375 de 2006; 2474 de 2008 y 2473 de 2010, por la cual se expide el Estatuto General de Contratación de la Administración Pública.

- Decreto 1510 de 2013: por el cual se reglamenta el sistema de compras y contratación pública.

- Ley 1581 de 2012: Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por la cual se dictan disposiciones generales para la protección de datos personales.

- Ley 1273 de 2009, el Congreso de la República de Colombia crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”.

6 MARCO METODOLÓGICO

6.1 METODOLOGÍA DE INVESTIGACIÓN

6.1.1 Tipo de Investigación. El tipo de investigación a realizar es cuantitativo, ya que mediante ella se pretende realizar un análisis de riesgos y así detectar las vulnerabilidades y amenazas a los cuales está expuesta la infraestructura tecnológica de la Cámara de Comercio.

La investigación es fáctica ya que para cumplir con los objetivos propuestos se basa en la experiencia propia para la recolección y análisis de información, así como los criterios adquiridos previamente en el desarrollo de la Especialización en Seguridad Informática.

6.2 DISEÑO DE LA INVESTIGACIÓN

6.2.1 Universo y muestra.

La población de estudio está conformada por los usuarios internos y externos que tienen acceso a la infraestructura tecnológica de la Cámara de Comercio. En tanto que el muestreo es aleatorio estratificado ya que existen varios tipos de usuarios y el número de cada uno de ellos es elevado.

6.3 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Dado que uno de los investigadores hace parte del grupo poblacional, este tiene acceso de primera a la información necesaria, por tal razón los instrumentos de recolección de información a utilizar son:

- Observación directa.
- Entrevistas
- Listas de Chequeo.

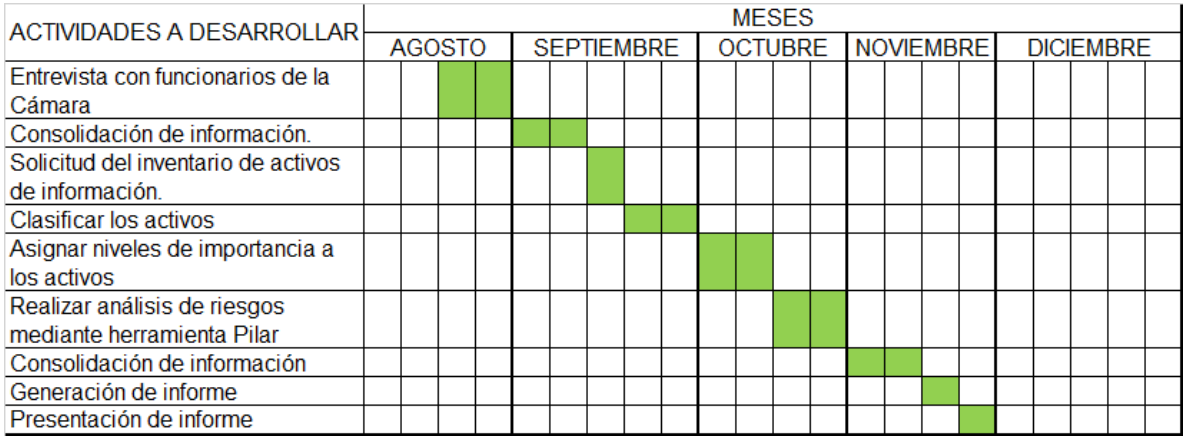
6.4 METODOLOGÍA DE DESARROLLO

En esta sección se desarrollan las actividades cuya finalidad es cumplir con los objetivos específicos para el análisis y evaluación de riesgos de seguridad informática para la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas.

De la misma forma, se relacionan elementos como insumos, datos recolectados, procesos de valoración realizados para el cumplimiento de cada una de las actividades definidas en la metodología de desarrollo.

7 CRONOGRAMA DE ACTIVIDADES

Figura 3. Cronograma de Actividades



Fuente: Los autores

8 DESARROLLO DEL PROYECTO

8.1 Recopilación de Información

Se realizó el levantamiento de información a través de entrevistas con los funcionarios de la Cámara; para esto se dividieron en grupos de acuerdo a su rol, distribuidos de la siguiente manera:

- Jefes de Área
- Asistentes
- Auxiliares

Como resultado de las entrevistas se obtuvieron los siguientes datos:

8.1.1 Políticas de seguridad.

La entidad tiene definidas unas Políticas de Seguridad, las cuales están normalizadas como parte del Sistema de Gestión de Calidad, y se identifican con el código ODIN-01 versión 3 vigencia 2012-11-06, pero estas no están definidas de acuerdo a los dominios de la norma ISO 27000/2013.

El documento suministrado aparece a continuación:

1. Para asegurar la integridad, confidencialidad y disponibilidad de los datos, información y los recursos asociados a ésta, cada funcionario únicamente tiene acceso a la información y recursos estrictamente necesarios para el desarrollo adecuado de su función.

2. Todos los funcionarios que deban tener acceso a las herramientas que apoyan el sistema de información, cuentan con clave de acceso y tiene definidos perfiles de usuarios que aseguren la autorización para grabar, modificar y consultar información.

3. Las claves asignadas para acceder a los sistemas de información son de uso personal e intransferible y está bajo la responsabilidad de cada usuario.

4. Los funcionarios deben cambiar la clave cuando lo consideren necesario debido a alguna vulnerabilidad en los criterios de seguridad; no obstante, los sistemas de información proveen mecanismos automáticos que exigen el cambio periódico de sus claves de acceso.

5. El uso de contraseñas adecuadas es de vital importancia en la seguridad de la información institucional, por lo tanto, deben cumplirse lineamientos básicos de seguridad que serán de acatamiento obligatorio por parte de todos los usuarios de la red y aplicaciones.

6. Las contraseñas deben ser una combinación de letras y números. No deben contener palabras comunes tales como nombres, apellidos o que sean de fácil deducción.

7. Los recursos o servicios suministrados por la Cámara de Comercio a los funcionarios, para facilitarle la realización de las labores, siendo estos recursos o servicios propiedad de la institución, deben recibir por parte de estos un trato adecuado, siempre resguardando que no se haga mal uso o abuso de los mismos.

8. Cuando el funcionario deja el puesto de trabajo, se deben cerrar las aplicaciones que se estén utilizando.

9. Con el fin de prevenir el acceso no autorizado a los datos de las estaciones de trabajo propiedad de la Cámara, la cuenta de administrador local de cada una de las estaciones de trabajo propiedad de la institución, debe estar protegida por contraseña.

10. No se deben descargar ni actualizar programas desde Internet en los equipos de la Cámara, salvo las actualizaciones configuradas automáticamente.

11. La instalación de software ajeno al suministrado por la Cámara de Comercio, no está permitida.

12. Los usuarios de cada uno de los sistemas de información son responsables de solicitar soporte informático en caso de encontrar situaciones sospechosas en el sistema.

13. La utilización de medios magnéticos propios (memorias USB, discos extraíbles, otros) se debe realizar previamente el proceso de vacunación.

14. El uso de Internet se concede a los funcionarios como una herramienta que colabora y apoya en la realización de las tareas, por lo tanto, cada usuario debe darle un uso apropiado a este servicio estrictamente relacionado con las labores que desempeña en la Cámara de Comercio de La Dorada, cualquier uso para otros propósitos no es permitido.

15. La navegación en sitios de contenido pornográfico, descargas, radio, televisión, drogas, además de no estar permitida está bloqueada.

16. La Cámara de Comercio, dependiendo del mal uso o abuso que le dé el usuario al servicio otorgado para la navegación en Internet, suspenderá o eliminará el servicio, en caso de comprobarse mal uso o abuso del mismo, según se define en esta política.

17. Cada usuario debe considerar las medidas de racionalidad y seguridad que garanticen que su trabajo se llevará a cabo de una manera eficiente y productiva.

18. En cada computador asignado a un funcionario, en apoyo al cumplimiento de sus labores, existe una carpeta compartida, esta es solamente para el almacenamiento temporal de archivos, la cual debe ser depurada para evitar la acumulación de material innecesario.

19. Para los asuntos relacionados con las labores institucionales cada funcionario cuenta con un correo identificado con el dominio de la Cámara de Comercio. Los correos de proveedores gratuitos tales como Hotmail, Yahoo!, Gmail, etc. no están permitido.

20. El correo electrónico se concede a los funcionarios como una herramienta que colabora y apoya en la realización de las tareas. Cada usuario debe darle un uso apropiado a este servicio estrictamente relacionado con las labores que desempeña en la Cámara de Comercio, los usos para otros propósitos no son aceptables.

21. El usuario deberá considerar las medidas de racionalidad y seguridad que garanticen que su trabajo se llevará a cabo de una manera eficiente y productiva.

22. Derivado del mal uso o abuso del correo electrónico, se podrá proceder a la suspensión o eliminación del servicio, dado que la Cámara como proveedora del servicio tiene la autoridad para controlar y negar el acceso a cualquiera que no cumpla con las políticas.

23. Las copias de seguridad de los aplicativos críticos, se deben realizar un respaldo diariamente en el equipo donde se tiene el aplicativo, la cual se debe almacenar en un servidor diferente al que tiene instalado el aplicativo.

24. Los dueños de los procesos deben velar porque los procesos de información que se realizan en sus áreas estén soportados por un proceso de respaldo de la información y por lo tanto deben solicitar al área de Sistemas y Gestión Documental para que se implemente el mecanismo de respaldo que asegure la información.

25. Se verificará por parte de Sistemas y Gestión Documental la realización de los respectivos respaldos en cada uno de los puestos de trabajo.

26. Los funcionarios que tengan asignado cualquier equipo tipo portátil, deben hacer correcto uso de los mismos y de la información que contienen.

27. Cualquier equipo que se encuentre dentro del inventario de la Cámara de Comercio que deba ser retirado de la institución, dicho traslado debe ser autorizado por la Presidencia Ejecutiva.

28. La información constituye uno de los principales activos de la Cámara de Comercio, por tanto, el manejo adecuado de la misma es responsabilidad de todos los funcionarios, así como la correcta utilización de los dispositivos utilizados para el almacenamiento y respaldo de información.

29. Los equipos en los cuales se almacenan y procesan datos críticos que colaboran con el cumplimiento de los servicios informáticos, deben estar ubicados en un espacio especial que cumpla con condiciones básicas de seguridad para la protección de los datos que contienen y del equipo en sí.

30. La información confidencial a la cual cada funcionario tiene acceso en cumplimiento de sus funciones, debe ser administrada de modo que no sea divulgada a personas que podrían utilizarla en beneficio propio, en contra de terceros o de la propia institución. Ningún funcionario podrá modificar, borrar, esconder o divulgar información en beneficio propio o de terceros.

31. Cualquier funcionario que debido a las necesidades institucionales detecte que debe aplicarse una excepción a algunas de las políticas anteriores, debe informarla por escrito a la Presidencia Ejecutiva, quien en conjunto con el área de Sistemas y Gestión Documental analizará el caso y determinarán la validez o no de la excepción. Si la excepción es válida, la comunicará por escrito indicando el período válido de la excepción. Una vez pasado el período de excepción Sistemas y Gestión Documental valorará si continúa siendo una excepción, caso en el cual deberá ser aprobada y evaluada nuevamente.[5]

8.1.2 Manual de funciones y perfiles.

La Cámara de Comercio tiene un Manual de Perfiles y Funciones, el cual hace parte del Sistema de Gestión de Calidad. El nombre del área encargada del manejo de TI en la Cámara de Comercio se denomina SISTEMAS Y GESTION DOCUMENTAL, está compuesta por tres funcionarios, de los cuales dos se dedican al manejo de la Gestión Documental y otra que es el Director de Sistemas y Gestión Documental, el cual es la única persona dedicada al manejo de TI en la organización. Con conocimiento técnico solo existe otro funcionario,

[5] Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. (2016). Política de Seguridad de la Información.

pero hace parte de otra área y se dedica a otras funciones diferentes al manejo de TI.

El Manual de Funciones y Perfiles adolece de información relacionada sobre el tratamiento de datos personales.

A continuación, aparece el Manual de Funciones y Perfiles del Director de Sistemas y Gestión Documental.

NOMBRE DEL ÁREA:	SISTEMAS Y GESTIÓN DOCUMENTAL
NOMBRE DEL CARGO:	DIRECTOR DE SISTEMAS YGESTION DOCUMENTAL
RELACIÓN DE DEPENDENCIA:	PRESIDENTE
NIVEL DEL CARGO:	COORDINADOR DE
RELACIÓN DE AUTORIDAD:	ASISTENTE DE GESTIONDOCUMENTAL

MISIÓN DEL CARGO

Garantizar el manejo ágil, preciso y objetivo de los sistemas de cómputo y la información de la entidad para emitir los informes asegurando la precisión en los datos reportados, como base para el desarrollo de los programas y proyectos de las Directivas de la Cámara de Comercio.

Buscar que el archivo de la Cámara de Comercio de La Dorada se adecue a las normas establecidas para tal fin y a las necesidades propias de la entidad.

Asegurar la generación oportuna de la información relacionada con el Centro de Atención Empresarial y la entrega de la misma a las entidades públicas que hacen parte del convenio CAE.

FUNCIONES

1. Instalar, manejar y atender los programas y equipos de cómputo, así como sus actualizaciones respondiendo por su buen funcionamiento y controlando su traslado.

2. Proponer, proyectar, diseñar y ejecutar los programas de capacitación en el área de sistemas, dirigidos a los empleados, de conformidad con las instrucciones impartidas por la Presidencia Ejecutiva.

3. Realizar y responder por las copias de seguridad de los archivos y su integridad, proponiendo y estableciendo las medidas que sean necesarias dentro de la posibilidad de recursos.

4. Elaborar y ejecutar el programa para el mantenimiento de equipos de cómputo, accesorios y periféricos y presentarlo a la Presidencia Ejecutiva para su aprobación.

5. Elaborar las hojas de vida de los equipos de cómputo y presentar las observaciones a la Presidencia Ejecutiva.

6. Dar solución eficaz a los eventos anormales que se presenten en la operación de los computadores y los programas.

7. Verificar el cumplimiento de los procedimientos establecidos en las diferentes operaciones de los sistemas y claves.

8. Procesar formatos, informes, bases de datos y demás trabajos especiales de manera oportuna y de acuerdo con las instrucciones impartidas por la Presidencia Ejecutiva.

9. Operar los servidores y en general toda la red de cómputo velando por su estricto cuidado y seguridad e informando de manera inmediata a la Presidencia Ejecutiva de cualquier anomalía.

10. Velar por el buen funcionamiento de los equipos de cómputo y programas de la entidad, con un gran sentido de confidencialidad.

11. Administrar de manera eficaz la página Web y el correo electrónico de la entidad.

12. Apoyar al área de Registros Públicos en todo lo relacionado con el funcionamiento del Registro Único Empresarial (RUE) y las actividades propias de la evolución tecnológica de la entidad, informando oportunamente a la Presidencia Ejecutiva de las necesidades y su ejecución.

13. Apoyar al área de Registros Públicos en la elaboración de informes para organismos de control.

14. Velar por el buen manejo de los expedientes de los comerciantes, Entidades Sin Ánimo de Lucro, Proponentes y todos los que estén sujetos a archivo por parte de la Cámara de Comercio.

15. Velar por el buen funcionamiento del Programa de Gestión Documental.

16. Generar la información sobre los nuevos matriculados para enviar a las Entidades públicas.

17. Hacer seguimiento a las Entidades públicas y a la DIAN sobre la oportuna y correcta generación, envío y recepción de información.

18. Garantizar que los procesos automáticos de generación, envío, recibo y actualización de información corran oportuna y correctamente sobre la Base de Datos.

19. Mantener comunicación permanente con el responsable del CAE y/o las Entidades públicas sobre cualquier inconveniente que pueda afectar la oportunidad y/o calidad de la información a los clientes de la Cámara de Comercio.

20. Actualizar la sección de preguntas frecuentes del CAE en la página web institucional.

21. Formar parte del Comité de Gestión y Control en el sostenimiento del Sistema de Gestión de la Calidad ISO 9001 y el Sistema de Control Interno.

22. Cumplir con las tareas que se le asignen en pro de sostener el Sistema de Gestión de la Calidad ISO 9001 y el Sistema de Control Interno de la Cámara de Comercio de La Dorada.

23. Guardar absoluta reserva por los asuntos que lleguen a su conocimiento por razón de su cargo.

24. Las demás funciones que le sean asignadas por su superior inmediato, de acuerdo a la naturaleza del cargo.

8.1.3 Procesos y procedimientos documentados y relacionados con el área.

En la Cámara de Comercio de La Dorada, también se tiene documentado como parte del Sistema de Gestión de Calidad, el procedimiento de Infraestructura, el cual contiene lo relacionado con algunos aspectos del manejo de TI, también un documento sobre el manejo de copias de seguridad y formatos de Hoja de Vida de Equipo de Cómputo y Programación de Mantenimientos.[6]

A continuación, aparece el documento sobre manejo de Copias de Seguridad.

MANEJO COPIAS DE SEGURIDAD	CODIGO: PRIN-02	Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas
	VERSIÓN: 2	
	VIGENCIA: 2012-06-01	
	PÁGINA: 39 de 4	

[6] Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. (2016). Manual de Funciones.

PROPÓSITO

Mantener un conjunto de copias de seguridad de la información generada en los sistemas, bases de datos, así como la información residente en los equipos de la Cámara, para brindar continuidad de los aplicativos críticos.

ALCANCE

Desde el momento en que realicen las copias hasta su eliminación.

DEFINICIONES

- **ARCHIVO:** Conjunto de documentos sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o institución pública o privada, en el transcurso de su gestión.

- **SEGURIDAD DE LA INFORMACIÓN**: preservación de la confidencialidad, integridad y disponibilidad de la información.

- **CONFIDENCIALIDAD**: aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.

- **INTEGRIDAD**: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.

- **DISPONIBILIDAD**: aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

- **COMUNICACIONES ELECTRÓNICAS**: Incluyen todo uso de los sistemas de información para comunicar o publicar material y contenido por medio de servicios como correo electrónico, foros de discusión, video conferencias, páginas HTML, o alguna herramienta similar.

- **SISTEMAS DE INFORMACIÓN**: Incluye cualquier sistema físico o aplicación de software que sea administrado por la Cámara y por los cuales ella sea responsable, como computadores, redes, servidores, enrutadores y aparatos similares junto con sus aplicaciones de red o aplicaciones de escritorio como sistemas operativos, aplicaciones ofimáticas, aplicaciones de Internet etc.

- **REDES:** Incluye varios sistemas electrónicos como redes de video, datos, voz, audio y dispositivos de almacenamiento, circuito cerrado de televisión, llamado de emergencias, sistema contra incendios.

- **USUARIOS**: Incluye toda aquella persona no necesariamente vincula con la entidad, a quien la misma le proporciona los medios y niveles de autorización y acceso necesarios para hacer uso de los servicios o sistemas de información de esta.

- **COPIA DE SEGURIDAD:** es una copia de la información con el fin de que esta puedan utilizarse para restaurar el original después de una eventual pérdida de datos.

- **SIREP:** Sistema Integrado de Registros Públicos

- **SEGA:** Sistema Estándar de Gestión Administrativa

- **SII:** Sistema integrado de información, que contiene módulos para el manejo de los Registros Públicos y Gestión Administrativa y Financiera.

- **DOCUWARE:** Sistema de gestión electrónica de documentos.

- **APLICATIVOS CRÍTICOS:** Se consideran aplicativos críticos los utilizados para el manejo de los registros públicos (SIREP, SII), financiero (SEGA) y gestión documental (DOCUWARE).

CONDICIONES GENERALES

- Para los aplicativos críticos, se debe realizar un respaldo diariamente en el equipo donde se tiene el aplicativo y uno semanal almacenado en un servidor diferente.

- Cada funcionario debe realizar copia de seguridad semanal o mensual, según el flujo de información, de las actividades o transacciones realizadas y enviarlas al área de Sistemas y Gestión Documental.

- Los CD o DVD de las copias de seguridad se nombran con el periodo de tiempo al que corresponde la información y al sistema o área que pertenecen.

- El área de Sistemas y Gestión Documental verifica la realización de los respectivos respaldos en cada uno de los puestos de trabajo.

- Se deben realizar pruebas continuas para asegurarse que los respaldos estén correctamente ejecutados y deben almacenarse en un lugar seguro y lejano de la fuente de información original.

DESCRIPCIÓN

APLICATIVOS CRÍTICOS

1. El Coordinador de Sistemas y Gestión Documental realiza diariamente a final del día las copias de seguridad del SIREP, SII y SEGA. En el caso del Sega y SII las copias quedan almacenadas en los servidores del Datacenter de Confecámaras.

2. Una vez realizadas las copias de seguridad del Sirep el Coordinador de Sistemas y Gestión Documental debe elaborar una copia de las mismas en otro servidor diferente al que tiene instalado el aplicativo.

3. Las copias se almacenan durante un mes en el servidor donde está instalado el sistema y en un equipo externo de la Cámara como contingencia.

4. Mensualmente el Coordinador de Sistemas y Gestión Documental graba en CD o DVD las copias de seguridad según sea el caso y se borran de los servidores.

5. Esta copia de seguridad se debe almacenar en una caja fuerte diferente a la sede principal.

EQUIPOS PORTATILES O DE ESCRITORIO

1. Cada funcionario debe realizar copia de seguridad en CD o DVD de forma semanal o mensual, según el flujo de información, de las actividades o transacciones realizadas, de los equipos de portátiles y de escritorio a su cargo y enviarlas al área de Sistemas y Gestión Documental relacionándolas en el formato FDGD-06 CONTROL DE DOCUMENTOS ENTREGADOS EN GENERAL.

2. Mensualmente el Coordinador de Sistemas y Gestión Documental consolida la información y se graban en CD o DVD, según sea el caso.

3. El Coordinador de Sistemas y Gestión Documental almacena esta copia de seguridad en una caja fuerte diferente a la sede principal.

VERIFICACIÓN COPIAS DE SEGURIDAD

Trimestralmente se deben seleccionar aleatoriamente dos copias de seguridad por cada sistema crítico, descomprimirlas y restaurarlas para verificar su integridad.[7]

EVIDENCIAS RELACIONADAS

[7] Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. (2016). Manejo de Copias de Seguridad.

CÓDIGO	NOMBRE DE LA EVIDENCIA
FDGD-06	CONTROL DE DOCUMENTOS ENTREGADOS EN GENERAL

HISTORIA DEL DOCUMENTO

FECHA DEL CAMBIO	VERSIÓN	DESCRIPCIÓN DEL CAMBIO GENERADO CON LA NUEVA VERSIÓN DEL DOCUMENTO
2012-05-25	2	Se amplía la definición de SII. Se ajustó ya que los aplicativos SII y Sega se tienen instalados en el Datacenter de Confecámaras. Se eliminó el punto de la copia semanal de las copias realizadas a un servidor externo. Se cambia el encabezado del documento.

ELABORADO: **COORDINACIÓN DE SISTEMAS Y GESTION DOCUMENTAL**	**REVISADO Y APROBADO:** **COMITÉ DE GESTIÓN Y CONTROL**
FECHA: 2012 – 05– 22	**FECHA: 2012 – 05 – 25**

8.1.4 Formato Hoja de vida equipos de cómputo

Figura 4. Formato Hoja de Vida Equipos de Cómputo

HOJA DE VIDA DE EQUIPOS DE COMPUTO	CODIGO: FDIN-01 VERSION: 3 VIGENCIA: 2012-06-01 PAGINA: 1 de 1	

DESCRIPCION:		
UBICACIÓN:	CODIGO MODULO DE ACTIVOS:	CODIGO DE BARRAS:
RESPONSABLE:		

FECHA	DETALLE	OBSERVACIONES	ACCIONES DE MEJORA

Fuente: Cámara de Comercio

8.2 ACTIVOS DE INFORMACIÓN

8.2.1 Inventario de activos de información

Con el fin de identificar los activos informáticos con que cuenta la Cámara de Comercio y que son usados para el manejo de la información, se realizó solicitud del inventario de activos de información al Director de Sistemas y Gestión Documental, como resultado se obtuvo la siguiente información:.

Tabla 1. Software y Aplicaciones

Descripción SO	No. Equipos	No. Usuarios
Windows Server 2008	1	
Windows 7 Professional x36/x64	20	
Linux Ubuntu Server 14.04 LTS	1	
Linux Suse SLES 11 SP4	1	
Linux Ubuntu Server 12.04 LTS	1	
MS Office Estándar 2007	12	
MS Office Estándar 2010	8	
MS Office Estándar 2013	5	
Windows 8.1 Professional x64	4	
Kaspersky Antivirus	30	
Sistema Integrado de Información Sii	1	50
Sistema de Registros Públicos Sirep	1	50
Sistema Administrativo y Contable JSP7	1	5
MySQL Enterprise	1	
Adabas Software AG	1	
Natural Software AG	1	
Entire Connection 4.5	30	

Fuente: Los autores

Tabla 2. Hardware

EQUIPO	RESPONSABLE
Dell Inspiron Desktop: Core i3, RAM 4Gb, DD 1Tb, DVD/RW, Tarjeta Red Inalámbrica y Cableada.	Asesor Especializado
Dell Inspiron Desktop: Core i3, RAM 4Gb, DD 1Tb, DVD/RW, Tarjeta Red Inalámbrica y Cableada.	Asesor Especializado y Jurídico
HP Compaq 6200 Pro A2W45UT Desktop PC - 2nd generation Intel Core i5-2400 3.10GHz, 4GB DDR3, 500GB HDD, DVDRW	Asistente de Gestión y Control
Acer Aspire X1700: Intel Core i3, RAM 4GB, tarjeta gráfica NVIDIA, disco duro SATA de 720GB a 7200rpm, unidad óptica grabadora de DVD, lector de tarjetas de memoria:	Asistente Gestión Documental
Todo en Uno Compaq: Intel Celeron, 2GB RAM, Disco duro 500GB, Tarjetas de red inalámbrica y cableada, DVD/RW.	Asesor Especializado y Jurídico
Todo en Uno Compaq: Intel Celeron, 2GB RAM, Disco duro 500GB, Tarjetas de red inalámbrica y cableada, DVD/RW.	Asesor Especializado y Jurídico
Acer Aspire X1700: Intel Core i3, RAM 4GB, tarjeta gráfica NVIDIA, disco duro SATA de 720GB a 7200rpm, unidad óptica grabadora de DVD, lector de tarjetas de memoria:	Auxiliar Contable
Acer Aspire X1700: Intel Core i3, RAM 4GB, tarjeta gráfica NVIDIA, disco duro SATA de 720GB a 7200rpm, unidad óptica grabadora de DVD, lector de tarjetas de memoria:	Auxiliar de Registro 1
Acer Aspire X1700: Intel Core i3, RAM 4GB, tarjeta gráfica NVIDIA, disco duro SATA de 720GB a 7200rpm, unidad óptica grabadora de DVD, lector de tarjetas de memoria:	Auxiliar de Registro 2
Acer Aspire X1700: Intel Core i3, RAM 4GB, tarjeta gráfica NVIDIA, disco duro SATA de 720GB a 7200rpm, unidad óptica grabadora de DVD, lector de tarjetas de memoria:	Auxiliar de Registro 3
Acer Aspire X1700: Intel Core i3, RAM 4GB, tarjeta gráfica NVIDIA, disco duro SATA de 720GB a 7200rpm, unidad óptica grabadora de DVD, lector de tarjetas de memoria:	Auxiliar Gestión Documental

EQUIPO	RESPONSABLE
Dell Inspiron Desktop: Core i3, RAM 4Gb, DD 1Tb, DVD/RW, Tarjeta Red Inalámbrica y Cableada.	Digiturno
Todo en Uno Lenovo C50-30: Procesador: Intel Core i5 5200U Velocidad del procesador: 2.7 GHz Disco duro: 1 Tera DDR3 RAM 4 Gb Pantalla Táctil Pantalla 23" Unidad CD DVD RW	Director Administrativo
Acer Aspire X1700: Intel Core i3, RAM 4GB, tarjeta gráfica NVIDIA, disco duro SATA de 720GB a 7200rpm, unidad óptica grabadora de DVD, lector de tarjetas de memoria:	Director de Proyectos
HP All-in-One 200-5030la: Procesador Intel Pentium E5300, RAM 4GB, Disco Duro 750, Tarjeta de Red Inalámbrica y cableada, DVD/RW	Director de Sistemas
Acer Aspire X1700: Intel Core i3, RAM 4GB, tarjeta gráfica NVIDIA, disco duro SATA de 720GB a 7200rpm, unidad óptica grabadora de DVD, lector de tarjetas de memoria:	Director Jurídico
Acer Aspire X1700: Intel Core i3, RAM 4GB, tarjeta gráfica NVIDIA, disco duro SATA de 720GB a 7200rpm, unidad óptica grabadora de DVD, lector de tarjetas de memoria:	Gestor Empresarial
Dell Inspiron Desktop: Core i3, RAM 4Gb, DD 1Tb, DVD/RW, Tarjeta Red Inalámbrica y Cableada.	Informador
HP Compaq 6200 Pro A2W45UT Desktop PC - 2nd generación Intel Core i5-2400 3.10GHz, 4GB DDR3, 500GB HDD, DVDRW	Secretaria
Servidor HP ML 350 GEN 8!!! SERIE P HP ProLiant ML350p Gen8 Base, Procesador: (1) Intel® Xeon® E5-2620 (2.00GHz/6-core/15MB/7.2GT-s QPI/95W, DDR3-1333, HT, Discos Duro 1 TB 6G SATA 7.2K rpm SFF, Memoria: 8GB (2 x 4GB) DDR3 RDIMM	Sistemas
Servidor SAS de rendimiento HP ProLiant DL360 Gen9 E5-2650v3 2P de 32 GB-R P440ar, fuente de alimentación redundante de 800 W, Disco duro 1 TB SATA 7200 Raid 1	Sistemas

EQUIPO	RESPONSABLE
Servidor HP ProLiant ML 310 Gen8 Base, Procesador: (1) Intel® Xeon®, Discos Duro 500 GB SATA 7.2K rpm SFF Raid 1, Memoria: 8GB (2 x 4GB) DDR3 RDIMM	Sistemas
Servidor HP TC2120: (1) Intel® Pentium 4, Disco Duro 300 GB 7.2K rpm, Memoria: 4GB	Sistemas
Portátil Lenovo 10": Intel Atom, RAM 2GB, Disco duro 500Gb	Director de Proyectos
Portátil Asus UX303LA-RO301H - Core I7 - DD 256 GB SSD - RAM 8Gb	Director de Proyectos
Tablet Samsung Tab S 10.5": CPU: Octa-Core, 1.9GHz, 1.3GHz Pantalla: Super AMOLED, 2560 x 1600 (WQXGA) Resolución: CMOS 8.0 MP	Director de Proyectos

Fuente: Los autores

Tabla 3. Red

DESCRIPCIÓN	CANTIDAD
Switch Hp 24 Puertos Administrable 10/100/1000 Capa 2, bandeja para Fibra Óptica	2
Router D-Link DIR-655	2
Router Huawei EchoLife HG8425H	2

Fuente: Los autores

Tabla 4. Equipamiento Auxiliar

DESCRIPCIÓN	CANTIDAD
UPS APC SUA 3000	2

Fuente: Los autores

Tabla 5. Instalación

DESCRIPCIÓN
Cableado estructurado 20 puntos dobles, 80% con UTP categoría 5E, 20% con UTP categoría 6.
Instalaciones eléctricas reguladas y doble polo a tierra

Fuente: Los autores

Tabla 6. Servicios

DESCRIPCIÓN
Conexión a Internet: Dos canales ADSL, el principal 20MB con UNE y otro como contingencia de 10 con Movistar
Mantenimiento Preventivo: Dos veces al año por el mismo personal de la Cámara y Correctivo por personal técnico externo en caso de ser necesario.
Troncal SIP de 5 líneas con UNE

Fuente: Los autores

Tabla 7. Personal

DESCRIPCIÓN	CANT.
Director de Sistemas: Cumple las funciones de Administrador de los sistemas de información, encargado del mantenimiento y soporte a usuarios internos.	1
Usuarios Finales Internos	30
Usuarios Externos: Entidades de Control y Estatales	20

Fuente: Los autores

8.2.2 Clasificación de los activos.

Del inventario suministrado se evaluaron la criticidad de los mismos y se extrae la siguiente información de los activos más importantes.

Tabla 8. Clasificación de Activos

Tipo de activo de información (De acuerdo con los criterios descritos en la norma ISO 27005**)**	**No.**	**Descripción del Activo de Información**	**Nombre del activo asociado a información**	**Responsable del activo**	**Confidencialidad**	**Disponibilidad**	**Integridad**	**Promedio**	**Importancia**
Hardware	1	Servidor de aplicaciones	Servidor de aplicaciones	Director de Sistemas	2	3	3	2,7	Alto
Hardware	2	Central telefonía IP	Central telefonía IP	Director de Sistemas	1	2	2	1,7	Medio
Redes	3	Línea ADSL	Línea ADSL	Director de Sistemas	2	3	3	2,7	Alto
Redes	4	Ups Servidores	Ups Servidores	Director de Sistemas	2	3	2	2,3	Alto
Redes	5	Switch	Switch	Director de Sistemas	2	3	3	2,7	Alto
Redes	6	Enrutadores	Enrutadores	Director de Sistemas	2	3	3	2,7	Alto
Software	7	Suse Linux 11 SLES	Suse Linux 11 SLES	Director de Sistemas	1	3	3	2,3	Alto

Tabla 8. (Continuación)

Software	8	Windows Server 2012	Windows Server 2012	Director de Sistemas	1	3	2	2,0	Medio
Software	9	Sistema Integrado de Información	Sistema Integrado de Información	Director de Sistemas	2	3	3	2,7	Alto
Software	10	Sistema de Gestión Administrativa	Sistema de Gestión Administrativa	Director de Sistemas	2	1	1	1,3	Medio

Fuente: Los autores

Para la tabla anterior se aplican los siguientes criterios:

Tabla 9. Criterios de Valoración de Activos

CONFIDENCIALIDAD	
1	Información pública
2	Información clasificada
3	Información reservada
INTEGRIDAD	
1	Si se modifican los datos no es relevante para la entidad
2	Si se modifican los datos tiene un impacto medio para la entidad
3	Si se modifican los datos es crítico para la entidad
DISPONIBILIDAD	
1	No importa si un día no está disponible el activo
2	Si esta indisponible por 8 horas genera retrasos en el cumplimiento de objetivos
3	Si esta indisponible una hora seria crítico para la entidad
IMPORTANCIA (Se aproxima a la unidad entera más cercana)	
1	Bajo: En caso de suceder algo a este activo la entidad no se afectaría.
2	Medio: En caso de suceder algo a este activo su impacto es poco crítico.
3	Alto: Se implementar los controles que le mitiguen los riesgos, porque en caso que le pase algo a este activo afectaría a la entidad.

Fuente: Los autores

8.3 Análisis y evaluación de los riesgos a que está expuesta la organización debido a las vulnerabilidades y amenazas existentes.

8.3.1 Identificación de Amenazas

Puede considerarse amenaza todo lo que pueda causar daño o genera peligro a los activos de información de una organización. Las amenazas se pueden clasificar en:

- Amenazas naturales

- Amenazas a instalaciones
- Amenazas humanas
- Amenazas Tecnológicas

Para la identificación de amenazas trabajadas se establecieron las siguientes categorías según la anterior clasificación.

Tabla 10. Categorías para la identificación de Amenazas

Hardware/Software
• Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros).
• Ataque malicioso (explosivos, químicos, vandalismo, hurto, radiación electromagnética, entre otros).
• Ataques contra el sistema (negación del servicio, manipulación de software, manipulación de equipo informático entre otros).
• Código malicioso (troyanos, gusanos, bomba lógica, entre otros).
• Daño físico (fuego, agua, humedad, contaminación química, construcción, entre otros). ▪ Destrucción de equipos o medios. ▪ Errores de transmisión o almacenamiento. ▪ Falla / degradación o mal funcionamiento del software o hardware. ▪ Falla de la red interna. ▪ Falla de suministro de servicios esenciales (agua, gas, aire acondicionado).
• Falla en el suministro de energía (perdida suministro de energía, planta eléctrica, UPS, banco de baterías). ▪ Fuego, agua, humedad, variaciones de temperatura/voltaje, radioactividad, polvo, gases, oxidación, campos electromagnéticos, entre otros.
• Hurto o robo (información, documentos, medios o equipos). ▪ Incumplimiento en el mantenimiento. ▪ Saturación del sistema de información.
• Abuso de derechos (de usuario, administrador). ▪ Uso de software no licenciado o no autorizado.
• Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores).
• Insuficiencia recursos tecnológicos (Poca disponibilidad de recursos tecnológicos, Medios, computadores, Sistemas de información).

Tabla 10. (Continuación)

Información
• Abuso de derechos (de usuario, administrador).
• Acceso no autorizado (sistema de información, documentación, información).
• Actos fraudulentos (suplantación, fraude, venta de información, soborno, extorsión, falsificación de derechos, entre otros).
• Ataque malicioso (explosivos, químicos, vandalismo, hurto, radiación electromagnética, entre otros).
• Código malicioso (troyanos, gusanos, bomba lógica, entre otros).
• Daño físico (fuego, agua, humedad, contaminación química, construcción, entre otros). • Deterioro del sistema o medio de almacenaje. • Divulgación no autorizada.
• Error en el uso (de equipos, medios, información, sistemas o servicios de información).
• Hurto o robo (información, documentos, medios o equipos). • Incumplimiento de leyes o regulaciones (propiedad intelectual, entre otros). • Incumplimiento de políticas o procedimientos internos.
• Pérdida de información (contenida en documentación física o digital). • Recuperación de medios reciclados o desechados. • Saturación del sistema de información.
• Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores).
Personal
• Abuso de derechos (de usuario, administrador).
• Acceso no autorizado (sistema de información, documentación, información, entre otros).
• Actos fraudulentos (suplantación, fraude, venta de información, soborno, extorsión, falsificación de derechos, entre otros). • Contaminación, Pandemias, virus. • Déficit de personal. • Destrucción de equipos o medios. • Divulgación no autorizada.
• Empleados (Acciones involuntarias y/o deliberadas).
• Error en el uso (de equipos, medios, información, sistemas o servicios de información).
• Espionaje (interceptación, ingeniería social).
• Hurto o robo (información, documentos, medios o equipos). • Incumplimiento de políticas o procedimientos internos.
• Intrusión o acceso forzado (instalaciones, sistemas de información, información).

• Intruso externo (Ej.: Exempleados, delincuente informático, competidores). • Piratería. • Proveedor o contratista.
• Ataque malicioso (explosivos, químicos, vandalismo, hurto, radiación electromagnética, entre otros).
• Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores). • Negligencia en el uso adecuado de recursos de información.
Infraestructura
• Ataque malicioso (explosivos, químicos, vandalismo, hurto, radiación electromagnética, entre otros).
• Daño físico (fuego, agua, humedad, contaminación química, construcción, entre otros).
• Desastre natural (temblor, terremoto, inundación, incendio, rayos, contaminación química entre otros). • Destrucción de equipos o medios. • Fuego, agua, humedad, variaciones de temperatura/voltaje, radioactividad, polvo, gases, oxidación, campos electromagnéticos, entre otros. • Incumplimiento en el mantenimiento.
Servicios
• Cierre de operación de un proveedor o contratista crítico para la Entidad.
• Falla de suministro de servicios esenciales (agua, gas, aire acondicionado).
• Falla en el suministro de energía (perdida suministro de energía planta eléctrica, UPS, banco de baterías).
• Falla sistema de comunicaciones (Internet, canales, Radio, entre otros).
• Incumplimiento de leyes o regulaciones (propiedad intelectual, entre otros).
• Incumplimiento en el mantenimiento.
• Incumplimiento en el servicio de mantenimiento.
Intangibles
• Hurto o robo (información, documentos, medios o equipos).
• Incumplimiento de leyes o regulaciones (propiedad intelectual, entre otros).
• Incumplimiento de políticas o procedimientos internos.
• Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores).
• Ausencia de políticas o procedimientos internos.
• Intrusión o acceso forzado (instalaciones, sistemas de información, información).

Fuente: Los autores

8.3.2 Identificación de Vulnerabilidades

Vulnerabilidades son puntos débiles de algún activo de información.

Al igual que las amenazas se desarrolló un catálogo de vulnerabilidades clasificadas en:

- Hardware
- Software
- Información
- Personas
- Infraestructura física
- Servicios
- Intangible

Tabla 11. Categorías para la identificación de Vulnerabilidades

HARDWARE
• Acceso o uso no controlado.
• Almacenamiento de equipos sin protección.
• Arquitectura insegura de la red.
• Ausencia de esquemas de respaldo.
• Ausencia de segmentación de la red.
• Ausencia de sistemas y/o procedimientos de monitoreo de los recursos de procesamiento de información.
• Ausencia o insuficiencia de control de cambios en la configuración.
• Ausencia de un plan de mantenimiento anual.
• Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad.
• Ausencia o insuficiencia en el control de los activos que se encuentran fuera de las instalaciones.
• Canales de comunicación sin encriptación.
• Capacidad inadecuada.
• Conexión deficiente y/o desorganización del cableado estructurado / eléctrico.
SOFTWARE
• Acceso o uso no controlado del sistema de información (software, aplicativo).
• Ausencia de logs o registros de auditoría.
• Ausencia o insuficiencia de procedimientos de control de cambios.
• Ausencia o insuficiencia de actualizaciones.

Tabla 11. (Continuación)

• Ausencia o insuficiencia de Políticas eficientes de copias de respaldo.

• Ausencia o insuficiencia de documentación de uso y/o administración.
• Ausencia o insuficiencia de mecanismos de identificación y autenticación.
• Ausencia o insuficiencia de perfiles de acceso o falta de gestión de privilegios de acceso.
• Ausencia o insuficiencia de pruebas.
• Ausencia o insuficiencia en la gestión de usuarios y contraseñas.
• Configuración incorrecta de parámetros o configuraciones por defecto.
• Descarga y uso no controlado de software.
• Documentación insuficiente o desactualizada.
• Eliminación de información sin borrado seguro.
• Especificaciones o requerimientos incompletos, inadecuados o no claros.
• Fallas conocidas o defectos del software.
• Puertos o servicios activos no requeridos.
• Relojes no sincronizados.
• Transferencia y/o almacenamiento de información en texto claro.
• Uso de Software ilegal / No autorizado / Software Malicioso.
• Disposición/reutilización de medios de almacenamiento sin borrado seguro.
• Ausencia de "terminación/bloqueo de la sesión" cuando se abandona la estación de trabajo.
• Ausencia de sistemas y/o procedimientos de monitoreo de los recursos de procesamiento de información.
• Insuficiente entrenamiento, capacitación o sensibilización.
• Ausencia de procedimientos aprobados.
• Ausencia de conocimientos en el manejo de las aplicaciones.
INFORMACIÓN
• Acceso no controlado a información sensible / confidencial.
• Ausencia de control de los activos de información que se encuentran en las instalaciones.
• Ausencia o insuficiencia de contratos, acuerdos de nivel de servicio y/o confidencialidad con empleados o terceros.
• Ausencia o insuficiencia de copias de respaldo.
• Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad. (Desconocimiento de políticas de tratamiento de la información en soportes físicos).
• Ausencia o insuficiencia de procedimientos de monitoreo de los recursos de procesamiento de información.
• Ausencia o insuficiencia de procedimientos para el manejo información clasificada.

Tabla 11. (Continuación)

• Ausencia o insuficiencia de un proceso de análisis y tratamiento de riesgos.
• Ausencia o insuficiencia de un proceso para clasificar y etiquetar la información.
• Descarga y/o uso no controlado de software.
• Documentación insuficiente o desactualizada.
• Eliminación de información sin borrado seguro.
• Falta de segregación de funciones o incorrecta aplicación de las mismas.
• Uso de Software ilegal / No autorizado / Software malicioso.
• Transferencia y/o almacenamiento de información en texto claro.
• Almacenamiento de información sin protección.
• Canales de comunicación sin encriptación.
• Ausencia o insuficiencia en el control de los activos que se encuentran fuera de las instalaciones.
• Ausencia de procedimiento de control de cambios.
• Ausencia de procedimiento formal para la autorización de la información disponible al público.
• Insuficiente entrenamiento, capacitación o sensibilización.
PERSONAL (ROL)
• Acceso no controlado a información sensible / confidencial.
• Falta de capacitación al personal, respecto al manejo de la información, software y hardware.
• Ausencia de controles y verificaciones en los procesos de selección y contratación de personal.
• Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros.
• Ausencia o insuficiencia de cláusulas contractuales y/o acuerdos de confidencialidad.
• Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los empleados y/o terceras partes.
• Ausencia o insuficiencia de políticas, procedimientos y/o directrices de seguridad.
• Ausencia o insuficiencia en la definición y formalización de roles, funciones y responsabilidades en la seguridad de la información.
• Dependencia de personal clave, ausentismo y/o personal insuficiente.
• Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables.
• Falta de segregación de funciones o incorrecta aplicación de las mismas.
• Incumplimiento de políticas o procedimientos internos.
• Insuficiente entrenamiento, capacitación o sensibilización.

Tabla 11. (Continuación)

• Personal inconforme o molesto.
• Ausencia o insuficiencia de procesos disciplinarios definidos en el caso de incidente de seguridad de la información.
INFRAESTRUCTURA FÍSICA
• Ausencia o insuficiencia de controles de acceso a las instalaciones.
• Ausencia o insuficiencia de controles de monitoreo de las instalaciones (por ej. detección o extinción de incendios, líquidos inflamables, entre otros).
• Ausencia o insuficiencia de mantenimiento preventivo / correctivo.
• Ausencia o insuficiencia de planes de emergencia y simulacros de evacuación.
• Falla en los servicios esenciales (internet, teléfonos, aire acondicionado, energía, agua, etc.).
• Ubicación geográfica de las instalaciones en una zona de alto impacto por eventos externos (desastres naturales, orden público, entre otros).
• Ausencia de planes de continuidad.
• Ausencia o insuficiencia de un proceso de análisis y tratamiento de riesgos.
• Falta o deficiencia de los ductos de ventilación.
SERVICIOS
• Ausencia o insuficiencia de contratos, acuerdos de niveles de servicio y/o confidencialidad.
• Dependencia de proveedores.
• Proveedor o contratista único en el mercado.
• Proveedor, contratista y/o cliente sin el suficiente respaldo técnico.
• Ausencia de planes de continuidad.
• Ausencia o insuficiencia de un proceso de análisis y tratamiento de riesgos.
• Ausencia de procedimiento formal para la autorización de la información disponible al público.
INTANGIBLES
• Ausencia de planes de continuidad.
• Ausencia de responsables sobre la gestión en seguridad de la información y/o continuidad de negocio.
• Ausencia o insuficiencia de un procedimiento para el manejo de comunicaciones externas.
• Ausencia o insuficiencia de un proceso de gestión de incidentes de seguridad.
• Ausencia o insuficiencia de un proceso de análisis y tratamiento de riesgos.
• Ausencia de procedimiento formal para la autorización de la información disponible al público.
• Ausencia de políticas o procedimientos internos documentados.

Fuente: Los autores

8.3.3 Análisis de Vulnerabilidades

Una vez identificados y valorados los activos, se procede a la identificación de amenazas para cada uno de los activos, así como a la degradación y el impacto de éstas sobre los activos de acuerdo a su valoración. También se realiza deducción de la probabilidad o frecuencia con las que se presentan las amenazas y/o vulnerabilidades identificadas en la empresa.

Tabla 12. Escala de frecuencia de amenazas

Escala de rango de frecuencia de amenazas		
Valor	**Rango**	**Probabilidad**
5	1 vez cada semana	Alta
4	1 vez cada mes	Media
3	1 vez cada 6 meses	Baja
2	1 vez al año	Muy baja
1	1 vez cada 2 años	Raro

Fuente: Manual MAGERIT

Tabla 13. Rango porcentual de impactos en activos para dimensiones de seguridad

Rango porcentual de impactos en activos para cada dimensión de seguridad	
Impacto	**Valor Cualitativo**
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Fuente: Manual MAGERIT

Tabla 14. Rango de impactos en activos

Rango de impactos en activos	
Impacto	**Valor Cualitativo**
Desastroso	8
Mayor	5
Moderado	3
Menor	2
Insignificante	1

Fuente: Manual MAGERIT

La estimación del impacto se realiza para determinar el alcance del daño producido sobre un activo informática cuando se materializa una amenaza. A partir de los datos obtenidos en las fases anteriores, se procede a estimar el impacto. El primer dato requerido es el “Nivel del activo” valorado cuantitativa y/o cualitativamente:

Tabla 15. Amenazas en Software y/o Aplicaciones detectadas

RELACION DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO																
Código Grupo de Activo	Activo	Valor Activo	Amenazas	Frecuencia					Impacto para cada dimensión					Degradación	Impacto
				[app]	[dbms]	[office]	[av]	[os]	[A]	[C]	[I]	[D]	[T]		
[app] Servidor de aplicaciones	[Server_App]	8	[I.5] Avería de origen físico o lógico	2	2	1	3	3	50%	100%	75%	100%		100%	Mayor
	[SII]	8	[E.2] Errores del administrador	1	2	1	2	2		50%	50%	75%		100%	Mayor
	[SRP]	8	[E.8] Difusión de software dañino	1	1	1	1	4		20%	20%	75%		100%	Mayor
	[SAC]	7	[E.9] Errores de [re-]encaminamiento	2	2	1	2	3		50%	50%	50%		50%	Moderado
[dbms] Sistema de gestión de bases de datos	[S_BaseDeDatos]	7	[E.18] Destrucción de información	1	1	3	3	2		75%		100%		100%	Mayor
	[AS_AG]	7	[E.19] Fugas de información	3	2	3	2	1		50%	50%	50%		50%	Moderado
	[NS_AG]	7	[E.20] Vulnerabilidades de los programas (software)	3	2	4	2	4		50%	50%	50%		50%	Moderado
	[EC]	7	[E.21] Errores de mantenimiento / actualización de programas (software)	4	2	3	3	4		75%	75%	75%		1%	Menor
[Office] Ofimática	[Office_2007]	3	[A.5] Suplantación de la identidad del usuario	1	1	2	2	3		30%	30%	30%		1%	Menor
	[Office_2010]	4	[A.6] Abuso de privilegios de acceso	3	1	2	2	3		75%	50%	100%		1%	Menor
	[Office_2013]	5	[A.7] Uso no previsto	2	2	3	1	3		50%	75%	50%		1%	Menor
[av] Antivirus	[Antivirus]	6	[A.8] Difusión de software dañino	1	1	2	1	3			50%			50%	Moderado
[os] Sistema operativo	[OS_Win7_Win8]	5	[A.11] Acceso no autorizado	2	2	4	1	2						50%	Menor
	[OS_WinSer2008]	8	[A.15] Modificación deliberada de la información	1	1	4	3	1						100%	Mayor
	[OS_LinUS_14]	8	[A.18] Destrucción de información	1	1	4	2	2						100%	Mayor
	[OS_LinUS_12]	8	[A.22] Manipulación de programas											100%	Mayor
	[OS_SuseLin_11]	9												100%	Desastroso

Fuente: Los autores

Tabla 16. Amenazas en Hardware detectadas

RELACION DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO																		
Código Grupo de Activo	Activo	Valor Activo	Amenazas	Frecuencia							Impacto para cada dimensión					Degradación	Impacto
				[host]	[mid]	[pc]	[print]	[switch]	[router]	[pabx]	[A]	[C]	[I]	[D]	[T]		
[host] Grandes equipos	[Servidor]	8	[N.1] Fuego	1	1	1	1	1	1	1				100%		100%	Mayor
			[N.2] Daños por agua	1	1	2	1	1	1	1		75%	75%	100%			
[mid] Equipos medios	[PC_escritorio]	7	[N.7] Desastres Naturales. Fenómeno sísmico	1	1	1	1	1	1	1		75%	75%	100%		50%	Moderado
			[I.1] Fuego	1	1	1	1	1	1	1		75%	75%	100%			
	[PC_todoenuno]	7	[I.2] Daños por agua	1	1	1	1	1	1	1				100%		50%	Moderado
			[I.3] Contaminación mecánica	2	2	2	2	2	2	2		75%		75%			
[pc] Equipos que son fácilmente transportados	[PC_portatiles]	7	[I.4] Contaminación electromagnética	1	1	1	1	1	1	1				100%		1%	Menor
			[I.5] Avería de origen físico o lógico	3	3	3	3	3	3	3		75%		100%			
	[Tablet]	6	[I.6] Corte del suministro eléctrico	3	3	2	3	3	3	3				100%		1%	Menor
			[I.7] Condiciones inadecuadas de temperatura o humedad	2	2	2	2	2	2	2				100%			
[print] Equipos de impresión	[Impresoras]	5	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	2	2	2	2	2	2				75%		1%	Insignificante
				2	2	2	2	2	2	2				100%			
[switch] Conmutadores	[Switch]	8	[E.24] Caída del sistema por agotamiento de recursos	1	1	1	1	1	1	1				100%		100%	Mayor
			[E.25] Pérdida de equipos	1	1	1	1	1	1	1				75%			
[router] Enrutadores	[Routers]	8	[A.6] Abuso de privilegios de acceso	1	1	1	1	1	1	1				75%		100%	Mayor
			[A.7] Uso no previsto	1	1	1	1	1	1	1				20%			
			[A.11] Acceso no autorizado	2	2	2	2	2	2	2				100%			
[pabx] Centralita telefónica	[Troncal_SIP]	5	[A.23] Manipulación de los equipos	1	1	1	1	1	1	1				75%		50%	Menor
			[A.24] Denegación de servicio	1	1	1	1	1	1	1				100%			
			[A.25] Robo	1	1	1	1	1	1	1				100%			
			[A.26] Ataque destructivo														

Fuente: Los autores

Tabla 17. Amenazas en Equipos Auxiliares detectadas

RELACION DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO														
Código Grupo de Activo	Activo	Valor	Amenazas	Frecuencia			Impacto para cada dimensión					Degradación	Impacto
				[ups]	[wire]	[supply]	[A]	[C]	[I]	[D]	[T]		
[ups] Sistemas de alimentación ininterrumpida UPS	[UPS_Servidores]	8	[N.1] Fuego	1	1	1				50%		100%	Mayor
			[N.2] Daños por agua	2	2	2		75%	40%	50%			
			[N.7] Desastres Naturales. Fenómeno sísmico	1	1	1		40% 10%	10%	50%			
			[I.1] Fuego	1	1	1		10%		50%			
			[I.2] Daños por agua	2	2	2				50%			
			[I.3] Contaminación mecánica	2	2	2		75%		20%			
			[I.4] Contaminación electromagnética	1	1	1				20%			
[wire] Cableado eléctrico	[Cab_electrico]	8	[I.5] Avería de origen físico o lógico	2	2	2				20%		50%	Moderado
			[I.6] Corte del suministro eléctrico	3	3	3				5%			
			[I.7] Condiciones inadecuadas de temperatura o humedad	2	3	3				5%			
			[I.9] Interrupción de otros servicios y suministros esenciales	2	2	2				5%			
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	2	2				75%			
[supply] Suministros Esenciales	[Consumibles]	5	[E.25] Pérdida de equipos	1	1	4				100%		1%	Menor
			[A.7] Uso no previsto	1	2	3				40%			
			[A.11] Acceso no autorizado	1	1	1							
			[A.23] Manipulación de los equipos	2	2	2				10%			
			[A.25] Robo	1	1	1				20%			
			[A.26] Ataque destructivo	1	1	1				50%			

Fuente: Los autores

Tabla 18. Amenazas en Servicios contratados detectados

RELACION DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO													
Código Grupo de Activo	Activo	Valor	Amenazas	Frecuencia		Impacto para cada dimensión					Degradación	Impacto
				[internet]	[ADSL]	[A]	[C]	[I]	[D]	[T]		
[internet] Internet	[Internet]	5	[I.8] Fallo de servicios de comunicaciones	3	3	100%	100%	75%	100%		50%	Menor
			[E.2] Errores del administrador	2	2		20%		75%			
			[E.9] Errores de [re-]encaminamiento	1	1			100%				
			[E.24] Caída del sistema por agotamiento de recursos	1	1		100%	50%	100%			
			[A.5] Suplantación de la identidad del usuario	1	1		75%	75%	75%			
[ADSL] ADSL	[Linea_ADSL]	5	[A.6] Abuso de privilegios de acceso	2	2		75%	20%	75%		50%	Menor
			[A.7] Uso no previsto	2	2		75%		50%			
			[A.11] Acceso no autorizado	2	1		75%					
			[A.12] Análisis de tráfico	1	1				50%			
			[A.14] Interceptación de información (escucha)	1	1				75%			
			[A.15] Modificación deliberada de la información	1	1							
			[A.19] Divulgación de información	1	1							
			[A.24] Denegación de servicio	1	1							

Fuente: Los autores

Tabla 19. Amenazas en Personal detectadas

RELACION DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO													
Código Grupo de Activo	Activo	Valor	Amenazas	Frecuencia			Impacto para cada dimensión					Degradación	Impacto
				[ue]	[ui]	[adm]	[A]	[C]	[I]	[D]	[T]		
[ue] Usuarios externos	[UE]	8	[E.7] Deficiencias en la organización	1	1	1		75%	75%	75%		1%	Menor
			[E.19] Fugas de información	2	2	2			75%	75%			
[ui] Usuarios internos	[UFI]	7	[E.28] Indisponibilidad del personal	3	3	3		75%		75%		50%	Moderado
			[A.28] Indisponibilidad del personal	3	3	3		75%		75%			
[adm] Administrador de sistemas	[DS]	6	[A.29] Extorsión	1	1	1				75%		50%	Moderado
			[A.30] Ingeniería social (picaresca)	2	2	2							

Fuente: Los autores

8.3.4 Selección de dominios, objetivos de control y controles que aplican para la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas.

Una vez realizada la lectura de la norma ISO/IEC 27001:2013, se determina aplicar los controles:

- A5. Política de la seguridad de la información.
- A6. Organización de la seguridad de la información.
- A7. Seguridad de los recursos humanos.
- A8. Gestión de activos.
- A9. Control de acceso.
- A10. Criptografía
- A11. Seguridad física y ambiental.
- A12. Seguridad de las operaciones.
- A13. Seguridad de las comunicaciones.
- A14. Adquisición, desarrollo y mantenimiento de sistemas.
- A15. Relaciones con los proveedores.
- A16. Gestión de incidentes de seguridad de la información.
- A17. Aspectos de seguridad de la información de la gestión de la continuidad de negocio.
- A18. Cumplimiento.

Tabla 20. Dominios seleccionados para aplicar en la CCD

ISO27001:2013 - ANEXO A			
OBJETIVOS DE CONTROL Y CONTROLES			
Objetivos de control		**Controles**	**Aplicabilidad**
A.5. Política de la seguridad de la información.	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	SI
	Objetivo. Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	SI

Tabla 20. (Continuación)

A.6. Organización de la seguridad de la información.	A.6.1. Organización Interna.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	**SI**
	Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.	A.6.1.2. Separación de deberes. Las tareas 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.	SI
		A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.	SI
		A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	SI
		A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,	SI
	A.6.2. Dispositivos Móviles y Teletrabajo.	A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SI
	Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	A.6.2.2. Teletrabajo. Se deben implementar una política y 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.	SI
A.7. Seguridad de los recursos humanos.	A.7.1. Antes de asumir el empleo.	A.7.1.1. Selección. Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos 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
	Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	A.7.1.2. Términos y condiciones del empleo. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.	SI

Tabla 20. (Continuación)

	A.7.2. Durante la ejecución del empleo.	A.7.2.1. Responsabilidades de la Dirección. La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	**SI**
	Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información. Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	SI
		A.7.2.3. Proceso disciplinario. Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI
	A.7.3. Terminación y cambio de empleo.	A.7.3.1. Terminación o cambio de responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	SI
	Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.		
A.8. Gestión de activos.	A.8.1. Responsabilidad por los Activos.	A.8.1.1. Inventario de Activos. 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.	SI
	Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.	A.8.1.2. Propiedad de los activos. Los activos mantenidos en el inventario deben ser propios.	SI
		A.8.1.3. Uso Aceptable de los Activos. 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.	SI

Tabla 20. (Continuación)

		A.8.1.4. Devolución de Activos. 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.	**SI**
	A.8.2. Clasificación de la Información.	A.8.2.1. Clasificación de la Información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	SI
	Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.	A.8.2.2. Etiquetado de la Información. Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI
		A.8.2.3. Manejo de Activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI
	A.8.3. Manejo de medios de soporte.	A.8.3.1. Gestión de medios de Soporte Removibles. Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	SI
	Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.	A.8.3.2. Disposición de los medios de soporte. Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.	SI
		A.8.3.3. Transferencia de medios de soporte físicos. Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	SI
A.9. Control de acceso.	A.9.1. Requisitos del Negocio para Control de Acceso.	A.9.1.1. Política de Control de Acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	SI
	Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1.2. Acceso a redes y a servicios en red. Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	SI

Tabla 20. (Continuación)

	A.9.2. Gestión de Acceso de Usuarios.	A.9.2.1. Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.	SI
	Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.	A.9.2.2. Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	SI
		A.9.2.3. Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	SI
		A.9.2.4. Gestión de información de autenticación secreta de usuarios. La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.	SI
		A.9.2.5. Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	SI
		A.9.2.6. Cancelación o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	SI
	A.9.3. Responsabilidades de los usuarios.	A.9.3.1. Uso de información secreta. Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	SI
	Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.		
	A.9.4. Control de Acceso a Sistemas y Aplicaciones.	A.9.4.1. Restricción de acceso a información. 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.	SI
	Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones.	A.9.4.2. Procedimiento de Conexión Segura. Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.	SI

Tabla 20. (Continuación)

		A.9.4.3. Sistema de Gestión de Contraseñas. Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	SI
		A.9.4.4. Uso de programas utilitarios privilegiados. Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	SI
		A.9.4.5. Control de Acceso a Códigos Fuente de Programas. Se debe restringir el acceso a códigos fuente de programas.	SI
A.10. Criptografía	A.10.1. Controles Criptográficos.	A.10.1.1. Política sobre el uso de controles Criptográficos. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.	SI
	Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.	A.10.1.2. Gestión de Claves. Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.	SI
A.11. Seguridad física y ambiental.	A.11.1. Áreas Seguras.	A.11.1.1. Perímetro de Seguridad Física. Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	SI
	Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	A.11.1.2. Controles Físicos de entrada. Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	SI
		A.11.1.3. Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.	SI
		A.11.1.4. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI
		A.11.1.5. Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	SI

Tabla 20. (Continuación)

		A.11.1.6. Áreas de despacho y carga. Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	SI
	A.11.2. Equipos.	A.11.2.1. Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.	SI
	Objetivo. Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2.2. Servicios Públicos de soporte. Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.	SI
		A.11.2.3. Seguridad del cableado. El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.	SI
		A.11.2.4. Mantenimiento de equipos. Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI
		A.11.2.5. Retiro de Activos. Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	SI
		A.11.2.6. Seguridad de equipos y activos fuera del predio. Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.	NO – Los Equipos Siempre están Dentro de la organizacion
		A.11.2.7. Disposición segura o reutilización de equipos. Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre	SI

		escrito en forma segura antes de su disposición o reúso.	
		A.11.2.8. Equipos sin supervisión de los usuarios. Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.	SI

Tabla 20. (Continuación)

		A.11.2.9. Política de escritorio limpio y pantalla limpia. Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	SI
A.12. Seguridad de las operaciones.	A.12.1. Procedimientos operacionales y responsabilidades.	A.12.1.1. Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.	SI
	Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1.2. Gestión de Cambios. 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.	SI
		A.12.1.3. Gestión de Capacidad. 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.	SI
		A.12.1.4. Separación de los ambientes de desarrollo, ensayo y operación. Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.	NO – Todos los desarrollos se realizan en Confecá-maras
	A.12.2. Protección contra códigos maliciosos.	A.12.2.1. Controles contra códigos maliciosos. Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	SI
	Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información		

	estén protegidas contra códigos maliciosos.		
	A.12.3. Copias de Respaldo.	A.12.3.1. Copias de respaldo de la información. 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

Tabla 20. (Continuación)

	Objetivo. Proteger contra la pérdida de datos.		
	A.12.4. Registro y Seguimiento.	A.12.4.1. Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.	SI
	Objetivo. Registrar eventos y generar evidencia.	A.12.4.2. Protección de la información de registro. Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	SI
		A.12.4.3. Registros del administrador y del operador. Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.	SI
		A.12.4.4. Sincronización de relojes. 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
	A.12.5. Control de Software Operacional.	A.12.5.1. Instalación de software en sistemas operativos. Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI
	Objetivo. Asegurarse de la integridad de los sistemas operacionales.		
	A.12.6. Gestión de vulnerabilidad técnica.	A.12.6.1. Gestión de las vulnerabilidades técnicas. 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,	SI

		y tomar las medidas apropiadas para tratar el riesgo asociado.	
	Objetivo. Prevenir el aprovechamiento de las vulnerabilidades técnicas.	A.12.6.2. Restricciones sobre la instalación de Software. Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.	SI

Tabla 20. (Continuación)

	A.12.7. Consideraciones sobre auditorías de sistemas de información.	A.12.7.1. Controles sobre auditorías de Sistemas de Información. Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	SI
	Objetivo. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.		
A.13. Seguridad de las comunicaciones.	A.13.1. Gestión de Seguridad de Redes.	A.13.1.1. Controles de redes. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI
	Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	A.13.1.2. Seguridad de los servicios de red. 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 servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	SI
		A.13.1.3. Separación en las redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	SI
	A.13.2. Transferencia de información.	A.13.2.1. Políticas y procedimientos de transferencia de información. Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.	SI

	Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	A.13.2.2. Acuerdos sobre transferencia de información. Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	SI
		A.13.2.3. Mensajes electrónicos. Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	SI
		A.13.2.4. Acuerdos de confidencialidad o de no divulgación. 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.	SI
A.14. Adquisición, desarrollo y mantenimiento de sistemas.	A.14.1. Requisitos de seguridad de los sistemas de información.	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información. 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.	SI
	Objetivo. Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.	A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	SI
		A.14.1.3. Protección de transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.	SI
	A.14.2. Seguridad en los procesos de desarrollo y de soporte.	A.14.2.1. Política de desarrollo seguro. Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.	NO – Todos los desarrollos se realizan por parte de Confecamaras
	Objetivo. Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A.14.2.2. Procedimiento de control de cambios en sistemas. Los cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas a los desarrollos dentro de la organización.	NO – Todos los desarrollos se realizan por parte de Confecamaras

		A.14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacionales.	SI
		A.14.2.4. Restricciones sobre los cambios de paquetes de software. Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	SI

Tabla 20. (Continuación)

		A.14.2.5. Principios de construcción de sistemas de seguros. Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.	SI
		A.14.2.6. Ambiente de desarrollo seguro. Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	NO – Los desarrollos se realizan en Confecamaras
		A.14.2.7. Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.	SI
		A.14.2.8. Pruebas de seguridad de sistemas. Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad.	SI
		A.14.2.9. Pruebas de aceptación de sistemas. Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados.	SI
	A.14.3. Datos de ensayo.	A.14.3.1. Protección de datos de ensayo. Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	SI
	Objetivo. Asegurar la protección de los datos usados para ensayos.		

A.15. Relaciones con los proveedores.	A.15.1. Seguridad de la información en las relaciones con los proveedores.	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores. 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.	SI
	Objetivo. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores. Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	SI

Tabla 20. (Continuación)

		A.15.1.3. Cadena de suministro de tecnología de información y comunicación. 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.	SI
	A.15.2. Gestión de la prestación de servicios de proveedores.	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores. Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	SI
	Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.	A.15.2.2. Gestión de cambios a los servicios de los proveedores. Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.	SI
A.16. Gestión de incidentes de seguridad de la información.	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información.	A.16.1.1. Responsabilidades y procedimientos. 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.	SI

	Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.	A.16.1.2. Informe de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.	SI
		A.16.1.3. Informe de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	SI

		A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. 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.	SI
		A.16.1.5. Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	SI
		A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	SI
		A.16.1.7. Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	SI
A.17. Aspectos de seguridad de la información de la gestión de la continuidad de negocio.	A.17.1. Continuidad de seguridad de la información	A.17.1.1. Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.	SI

	Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.	A.17.1.2. Implementación de la continuidad de la seguridad de la información. 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.	SI
		A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que los válidos y eficaces durante situaciones adversas.	SI

Tabla 20. (Continuación)

	A.17.2. Redundancia	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI
	Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información.		
A.18. Cumplimiento.	A.18.1. Cumplimiento de requisitos legales y contractuales.	A.18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.	SI
	Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	A.18.1.2. Derechos de Propiedad Intelectual. 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 licenciados.	SI

		A.18.1.3. Protección de registros. Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	SI
		A.18.1.4. Privacidad y protección de la información identificable personalmente. Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	SI
		A.18.1.5. Reglamentación de Controles Criptográficos. Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos	SI

Tabla 20. (Continuación)

	A.18.2. Revisiones de seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información. 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, la políticas, los procesos y los procedimientos para seguridad de la información se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	SI
	Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.	A.18.2.2. Cumplimiento con las políticas y normas de seguridad. 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.	SI
		A.18.2.3. Revisión del Cumplimiento Técnico. Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.	SI

Fuente: Los autores

8.3.5 Listas de Chequeo

- Política de seguridad A5

Tabla 21. Lista de Chequeo Política de Seguridad A5

ASPECTO A EVALUAR	SI	NO
La Política de seguridad de la información de la Cámara de Comercio de La Dorada se encuentra documentada	X	
¿Las políticas para la seguridad de la información de la Cámara de Comercio han sido aprobadas por la dirección de la entidad?	X	
La Política de seguridad de la información es comunicada y conocida por todos los funcionarios y proveedores de la Cámara de Comercio de La Dorada	X	
La Política de seguridad de la información de la Cámara de Comercio de La Dorada es revisada a intervalos periódicos.	X	

Tabla 21. (Continuación)

La Política de seguridad de la información de la Cámara de Comercio está aprobada por la alta dirección	X	
La Política de seguridad de la información de la Cámara de Comercio declara el compromiso de la dirección.	X	

Fuente: Los autores

- Organización de la seguridad de la información A6

Tabla 22. Lista de Chequeo Organización de la seguridad de la información A6

Aspecto a Evaluar	SI	NO
¿La Cámara de Comercio tiene definidas y asignadas las responsabilidades de seguridad de la información dentro de las obligaciones contractuales de sus funcionarios?	X	
Se presenta dualidad de funciones y/o áreas de responsabilidad en conflicto en la entidad?		X
¿Existe un protocolo de comunicación con las autoridades pertinentes en caso de incidentes que comprometan la seguridad de la información?		X

Aspecto a Evaluar	SI	NO
Existen comunicaciones periódicas con grupos, foros y asociaciones profesionales especializadas en seguridad.		X
Se incluyen ítems y/o actividades referentes a la seguridad de la información en la gestión de los diferentes proyectos que gestiona la entidad?	X	
¿Existe una política para el uso de dispositivos móviles al interior de la entidad?		X
¿Existen medidas de seguridad de soporte para la gestión de riesgos introducidos por el uso de dispositivos móviles al interior de la entidad?		X
¿Se ha publicado, comunicado y divulgado la política de teletrabajo en la entidad?		X
¿Existen políticas y procedimientos para la implementación del teletrabajo en la entidad?		X
¿Existen medidas de seguridad de soporte para la protección de la información disponible mediante teletrabajo?		X
En los procesos de convocatorias y/o de contratación de personal se verifican los antecedentes de los candidatos, según las leyes, reglamentos y normas éticas pertinentes?	X	
Dentro de los contratos de los empleados se incluyen funciones y/u obligaciones referentes a las responsabilidades en cuanto a la seguridad de la información de la entidad?	X	

Tabla 22. (Continuación)

Se realiza seguimiento por la dirección a la aplicación de las políticas y/o procedimientos de seguridad de la información establecidos en la entidad, por parte de los empleados?	X	
Existen capacitaciones y actualizaciones periódicas respecto a las políticas y/o procedimientos de seguridad de información a cargo de cada funcionario de la entidad?	X	
¿Se ha definido y comunicado un proceso formal de tipo disciplinario a seguir, en caso de presentarse alguna violación a la seguridad de la información, por parte de los funcionarios de la entidad?		X
Se han definido responsabilidades sobre la seguridad de la información, que se incluyan en las funciones y/u obligaciones contractuales de los empleados, y que permanezcan válidas después de la terminación del vínculo contractual con la entidad?		X

Fuente: Los autores

- Gestión de activos A8

Tabla 23. Lista de Chequeo Gestión de activos A8

ASPECTO A EVALUAR	SI	NO

La organización cuenta con un inventario de activos de información actualizado.	X	
Todos los activos de información tienen adecuadamente identificado un responsable asignado.	X	
Existen políticas sobre el manejo de activos de información	X	
¿Existe un procedimiento establecido para la devolución de activos que se encuentran bajo responsabilidad de los funcionarios de la entidad?	X	
¿Se realiza identificación, valoración y clasificación de la información de la entidad?		X
¿Existen manuales para el uso correcto de los diferentes activos identificados en la entidad?		X
Existen manuales y/o procedimientos para el uso de medios de soporte removibles (memoria flash, CD, DVD, disco duro externo, entre otros), que garanticen la gestión, disponibilidad, integridad y confidencialidad de la información de la entidad?	X	

Fuente: Los autores

- Control de acceso A9

Tabla 24. Lista de Chequeo Control de Acceso A9

Aspecto a Evaluar	SI	NO
Existen procedimientos y/o políticas de control de acceso a la información y a las instalaciones de gestión de la información de la entidad?	X	
Existen controles sobre los funcionarios y/o usuarios para el acceso a la red y los servicios para los que tengan autorización?	X	
Existe un proceso de registro y cancelación de registro de usuarios y funcionarios para la asignación de privilegios y derechos de acceso sobre la información, sistemas de información y/o servicios de la entidad?	X	
Existe una política de gestión para la asignación de derechos de acceso a los funcionarios sobre los sistemas de información y/o servicios de la entidad?	X	
Existe un manual, política o procedimiento de gestión para la autenticación de funcionarios y/o usuarios en cada uno de los servicios y/o sistemas de información de la entidad?	X	
Se realiza revisión periódica de los derechos de acceso de los funcionarios y usuarios de la entidad sobre los diferentes servicios y/o sistemas de información?		X

Aspecto a Evaluar	SI	NO
Se realiza cancelación y/o ajustes en los derechos de acceso de funcionarios y/o usuarios, una vez terminada su vinculación con la entidad, y/o se ajustan al momento de presentarse cambios internos?	X	
Existen procedimientos y/o políticas de uso de información confidencial de la entidad?	X	
¿Se realiza seguimiento a los funcionarios respecto al uso de la información confidencial de la entidad?		X
Existen procedimientos de conexión segura para aplicar sobre los diferentes aplicativos y/o sistemas de información de la entidad?	X	
¿Existen políticas de gestión de contraseñas que se implementan en la entidad?	X	
¿Existen restricciones sobre el uso de programas utilitarios que afecten los sistemas de información y controles sobre los mismos, al interior de la entidad?	X	
Existen restricciones para acceso a códigos fuente de los aplicativos y/o sistemas de información de la entidad?	X	

Fuente: Los autores

- Criptografía A10

Tabla 25. Lista de Chequeo Criptografía A10

Aspecto a Evaluar	SI	NO
Se aplican claves criptográficas para protección de los sistemas de información y/o activos de la entidad?		X
¿Existe una política de gestión y uso de claves criptográficas al interior de la entidad?		X

Fuente: Los autores

- Seguridad física y del entorno A11

Tabla 26. Lista de Chequeo Seguridad Física y del Entorno A11

Aspecto a Evaluar	SI	NO
¿Se encuentra definido algún perímetro de seguridad sobre las áreas con información confidencial en la entidad?		X

Aspecto a Evaluar	SI	NO
Existen medidas y/o controles de entrada para asegurar que solo funcionarios autorizados tengan acceso a áreas con información confidencial o de manejo de información en la entidad?	X	
¿Existen políticas de seguridad de oficinas e instalaciones físicas de la entidad?	X	
Existen procedimientos y/o medidas de contingencia definidas para la protección física contra desastres naturales, accidentes y/o ataques?		X
Existen medidas y/o procedimientos para trabajo en áreas seguras en la entidad?		X
¿Se efectúan medidas de control de acceso a personal no autorizado en las diferentes áreas al interior de la entidad?	X	
¿Se encuentran aisladas las áreas de acceso a usuarios internos y externos de aquellas áreas con información confidencial y procesamiento de información?	X	
¿Existe mobiliario adecuado para la ubicación y protección de equipos de las diferentes áreas de la entidad?	X	
Los equipos de la entidad se encuentran conectados a equipos de respaldo eléctrica, como reguladores y estabilizadores de voltaje, UPS y/o plantas de soporte eléctrico?	X	
¿El cableado eléctrico y de red se encuentra debidamente protegido contra interferencia y (daños externos, de acuerdo a la normatividad respectiva (RETIE y ANSI-TIA)?	X	
¿Existe un plan de mantenimiento periódico preventivo y correctivo en la entidad, con el fin de mantener la disponibilidad e integridad de los equipos?	X	

Tabla 26. (Continuación)

¿Se realizan controles de retiro de equipos y activos tecnológicos de la entidad?	X	
Existe un procedimiento establecido para la disposición segura o reutilización de equipos, software licenciado y/o elementos que contengan medios de almacenamiento de información confidencial de la entidad?	X	
¿Existe una política de escritorio limpio y pantalla limpia en la entidad?		X

Fuente: Los autores

- Seguridad de las operaciones A12

Tabla 27. Lista de Chequeo Seguridad de las Operaciones A12

Aspecto a Evaluar	SI	NO
¿Existen procedimientos operativos documentados, publicados y a disposición de los usuarios internos y externos, así como a los funcionarios de la entidad?	X	
¿Existe una política de gestión de cambios a los procesos, procedimientos, instalaciones y sistemas de procesamiento de información al interior de la entidad?	X	
¿Se hace seguimiento y control al uso de recursos y requisitos de capacidad para el funcionamiento de los sistemas de información de la entidad?	X	
¿Existe algún tipo de control de detección, prevención y recuperación contra códigos maliciosos al interior de la entidad?	X	
Se realiza promoción y/o divulgación de medidas y procedimientos de uso seguro de los equipos, para protegerlos de códigos y software malicioso?	X	
¿Existe un plan o política vigente de copias de respaldo de información, software y sistemas de información de la entidad, y que se ponga a prueba periódicamente?	X	
Se realizan registros de actividades de usuarios y/o funcionarios, fallas y eventos de seguridad de la información de la entidad?		X
¿La información de registro de actividades y demás de la entidad, se conserva y protege adecuadamente, de modo que se conserve su integridad y confidencialidad?		X
¿La información de registro de actividades y demás de la entidad se revisa periódicamente?		X

Tabla 27. (Continuación)

¿Se encuentran sincronizados los relojes de los sistemas de información de la entidad, respecto a una única fuente de referencia de tiempo?	X	
Existen restricciones, controles y/o procedimientos de control para la instalación de software por parte de funcionarios y/o usuarios no autorizados, en sistemas operativos de la entidad?	X	
¿Se realizan procedimientos de verificación periódica de vulnerabilidades técnicas de los sistemas de información de la entidad?		X
¿Se aplican medidas de mitigación y tratamiento de riesgos asociados a las vulnerabilidades técnicas de los sistemas de información de la entidad?		X

¿Se realizan auditorías periódicas sobre los sistemas de información de la entidad?		X
Las auditorías sobre los sistemas de información se realizan de manera planificada y acordada con los funcionarios y/o usuarios de la entidad, de modo que se minimicen las interrupciones en los procesos y servicios?		X

Fuente: Los autores

- Seguridad de las comunicaciones A13

Tabla 28. Lista de Chequeo Seguridad de las Comunicaciones A13

Aspecto a Evaluar	SI	NO
¿Existe una política de gestión de redes documentada, aceptada, publicada y divulgada al interior de la entidad?		X
¿Los servicios de red se prestan internamente?	X	
Están definidos mecanismos y/o herramientas de seguridad para los servicios de red de la entidad?	X	
¿Están definidos los niveles de servicio y requisitos de gestión en los acuerdos de servicios de red?		X
Existe separación de red para los sistemas de información, funcionarios y/o usuarios, y servicios de la entidad?	X	
Existen procedimientos, controles y/o políticas formales de transferencia de información a través de la infraestructura de comunicaciones dispuesta en la entidad?		X
¿Existen acuerdos preestablecidos para la transferencia segura de información entre la entidad y partes externas?		X
¿Se aplican medidas de protección para la información que se incluye en mensajes electrónicos de la entidad?		X

Tabla 28. (Continuación)

¿Existen acuerdos de confidencialidad y no divulgación, documentados y con revisión periódica planificada, para la protección de la información de la entidad?		X

Fuente: Los autores

- Adquisición, desarrollo y mantenimiento de sistemas A14

Tabla 29. Lista de Chequeo Adquisición, desarrollo y mantenimiento de sistemas A14

Aspecto a Evaluar	SI	NO
Se incluyen requisitos y/o medidas de seguridad de información en los procesos de adquisición de nuevos sistemas de información o mejoras en los existentes?	X	
¿Existen procedimientos, manuales o políticas para la implementación de sistemas de información seguros en la entidad?		X
¿Existen medidas de protección sobre la información dispuesta en aplicativos de la entidad, y que transite por redes públicas?	X	
¿Se realizan revisiones y pruebas técnicas a los aplicativos de la entidad, posteriormente a cambios de plataformas de operación?	X	
Existen restricciones y/o controles sobre los cambios de software o modificaciones de los mismos en los equipos de la entidad?	X	
¿La entidad supervisa y realiza el seguimiento pertinente de actividades de desarrollo de sistemas de información contratados externamente?	X	
¿La entidad supervisa y realiza el seguimiento pertinente de ensayos de funcionalidades de seguridad sobre sistemas de información contratados externamente?		X
¿La entidad realiza pruebas de aceptación de sistemas de información nuevos, actualizaciones y versiones nuevas, mediante ensayos programados y criterios establecidos?		X
¿La entidad selecciona y resguarda la información usada para ensayos de aplicativos?		X
Se realiza análisis y valoración de la información para definir una clasificación apropiada de la misma.		X
Existen directrices claras sobre el manejo adecuado de la información institucional	X	

Fuente: Los autores

- Relaciones con los proveedores A15

Tabla 30. Lista de Chequeo Relación con los Proveedores A15

Aspecto a Evaluar	SI	NO
¿Existe una política de seguridad de la información acordada y documentada, para mitigar riesgos asociados con el acceso de proveedores a activos de la entidad?		X

Aspecto a Evaluar	SI	NO
¿La entidad acuerda y establece requisitos pertinentes de seguridad de la información con los diferentes proveedores de servicios y activos?		X
¿Los requisitos de seguridad de la información establecidos entre la entidad y proveedores, incluyen tratamiento de riesgos asociados a la cadena de suministraos de productos y servicios TI?		X
¿La entidad realiza seguimiento y revisión de los servicios de los proveedores?	X	
¿La entidad gestiona los cambios en el suministro de servicios por parte de los proveedores?	X	
¿La entidad realiza revisión periódica de la política de seguridad de la información acordada con los proveedores, de acuerdo a la criticidad de los activos involucrados y a los riesgos que se reevalúan?		X

Fuente: Los autores

- Gestión de incidentes de seguridad de la información.

Tabla 31. Lista de Chequeo Gestión de incidentes de seguridad de la información A17

LISTA DE CHEQUEO				
DOMINIOS		**Aspectos a evaluar**	**SI**	**NO**
A16	Gestión de incidentes de seguridad de la información.	Los eventos de seguridad de información, son reportados a través de los canales correspondientes lo más rápido posible?	X	
		Son desarrollados e implementados procedimientos formales de reporte, respuesta y escalación en incidentes de seguridad?		X
		Existen procedimientos que aseguren que todos los empleados deben reportar cualquier vulnerabilidad en la seguridad en los servicios o sistemas de información?		X
		Están claramente establecidos los procedimientos y responsabilidades de gestión para asegurar una rápida, efectiva y ordenada respuesta a los incidentes de seguridad de información?		X
		Es utilizado el monitoreo de sistemas, alertas y vulnerabilidades para detectar incidentes de seguridad?	X	
		Existen mecanismos establecidos para identificar y cuantificar el tipo, volumen y costo de los incidentes de seguridad?		X
		La información obtenida de la evaluación de incidentes de seguridad que ocurrieron en el pasado, es utilizada para determinar el impacto recurrente de incidencia y corregir errores?		X

Tabla 31. (Continuación)

		Si las medidas de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica una acción legal (ya sea civil o penal)	X	

		Las evidencias relacionadas con incidentes, son recolectadas, retenidas y presentadas conforme las disposiciones legales vigentes en las jurisdicciones pertinentes?		X

Fuente: Los autores

- Aspectos de seguridad de la información de la gestión de la continuidad de negocio.

Tabla 32. Lista de Chequeo Aspectos de seguridad de la información de la gestión de la continuidad de negocio A17

LISTA DE CHEQUEO				
DOMINIOS		**Aspectos a evaluar**	**SI**	**NO**
A17	Aspectos de seguridad de la información de la gestión de la continuidad de negocio	Existen procesos que direccionan los requerimientos de seguridad de información para el desarrollo y mantenimiento de la Continuidad del Negocio dentro de la Organización?		X
		Estos procesos, entienden cuáles son los riesgos que la organización enfrenta, identifican los activos críticos, los impactos de los incidentes, consideran la implementación de controles preventivos adicionales y la documentación de los Planes de Continuidad del Negocio direccionando los requerimientos de seguridad?		
		Los eventos que puedan causar interrupción al negocio, son identificados sobre la base de probabilidad, impacto y posibles consecuencias para la seguridad de información?		X
		Son desarrollados planes para mantener y restaurar las operaciones de negocio, asegurar disponibilidad de información dentro de un nivel aceptable y en el rango de tiempo requerido siguiente a la interrupción o falla de los procesos de negocio?	X	
		Considera el Plan, la identificación y acuerdo de responsabilidades, identificación de pérdida aceptable, implementación de procedimientos de recuperación y restauración, documentación de procedimientos y testeo periódico realizado regularmente?		X
		Existe un marco único del Plan de Continuidad de Negocios?		X
		El Plan de Continuidad del Negocio direccionan los requerimientos de seguridad de información identificados?		X
		Los Planes de Continuidad del Negocio, son probados regularmente para asegurarse de que están actualizados y son efectivos?		X
		Los test de planes de continuidad de negocio, aseguran que todos los miembros del equipo de recuperación y otros equipos relevantes sean advertidos del contenido y sus responsabilidades para la continuidad del negocio y la seguridad de información, son conscientes de sus roles y funciones dentro del plan cuando este se ejecuta?		X

Fuente: Los autores

- Cumplimiento.

Tabla 33. Lista de Chequeo Gestión Cumplimiento. A18

LISTA DE CHEQUEO				
DOMINIOS		**Aspectos a evaluar**	**SI**	**NO**
A18	Cumplimiento.	Todas las leyes relevantes, regulaciones, requerimientos contractuales y organizacionales son tenidos en cuenta de modo a que estén documentados para cada sistema de información en la organización?	X	
		Los controles específicos y responsabilidades individuales de modo a cumplir con estos requerimientos, son debidamente definidos y documentados?	X	
		Existen procedimientos para asegurar el cumplimiento de los requerimientos legales, regulatorios y contractuales sobre el uso de materiales y software que estén protegidos por derechos de propiedad intelectual?	X	
		Controles tales como: Política de Cumplimiento de Derechos de Propiedad Intelectual, Procedimientos de Adquisición de Software, Política de concientización, Mantenimiento de Prueba de la Propiedad, Cumplimiento con Términos y Condiciones, son consideradas?	X	
		Los registros importantes de la organización están protegidos contra pérdida, destrucción y falsificación en concordancia con los requerimientos legales, regulatorios, contractuales y de negocio?		X
		Los sistemas de almacenamiento son elegidos de modo a que los datos requeridos puedan ser recuperados en un rango de tiempo aceptable y en el formato necesario, dependiendo de los requerimientos a ser cumplidos?		X
		La protección de los datos y la privacidad, están asegurados por legislaciones relevantes, regulaciones y si son aplicables, por cláusulas contractuales?	X	
		Los Administradores, revisan regularmente el cumplimiento de las instalaciones de procesamiento de información dentro del área de su responsabilidad de modo a cumplir con los procedimientos y políticas de seguridad pertinentes?	X	

Fuente: Los autores

8.4 RESULTADOS OBTENIDOS DURANTE LA APLICACIÓN DE LOS INSTRUMENTOS DE ANÁLISIS

8.4.1 Análisis y Evaluación de Riesgos de la Cámara de Comercio

Una vez definida la frecuencia con la que se presentan las vulnerabilidades y amenazas en la empresa de estudio, se procede a calcular el riesgo de cada amenaza para cada uno de los activos identificados y valorados. Posteriormente se calcula el nivel de riesgo total para cada activo, y definir el tratamiento a aplicar de acuerdo al tipo de activo y al nivel de riesgo identificado.

Tabla 34. Mapa de riesgos

Riesgo = Probabilidad * Impacto						
Probabilidad	5	5	10	15	25	40
	4	4	8	12	20	32
	3	3	6	9	15	24
	2	2	4	6	10	16
	1	1	2	3	5	8
		1	2	3	5	8
		Impacto				

Fuente: Manual Magerit

Tabla 35. Niveles de riesgos totales

Nivel de Riesgo	
4	Extremo
3	Intolerable
2	Tolerable
1	Aceptable

Fuente: Manual Magerit

Tabla 36. Tratamiento de Riesgos

NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO
Aceptable	• FIN: Finaliza el proceso.
Tolerable	• TR: Se transfiere el riesgo por ejemplo tomando un seguro.
Intolerable	• EV: Se evita el riesgo retirando el activo de información.
Extremo	• MIT: Se reduce o mitiga el riesgo por medio de controles.

Fuente: Manual Magerit

A continuación, se realiza el análisis y evaluación de riesgos basados en la metodología MAGERIT, teniendo en cuenta lo indicado se calcula el impacto de acuerdo a la probabilidad de presentación del riesgo.

Tabla 37. Análisis y Evaluación de Riesgos en Software y/o Aplicaciones

		Riesgo																Nivel de Riesgo											
		[app]						[dbms]							[office]					[av]		[os]								
		[Server_App]		[SII]		[SRP]		[SAC]	[S_BaseDeDatos]		[AS_AG]		[NS_AG]		[EC]		[Office_2007]		[Office_2010]		[Office_2013]		[Antivirus]		[OS_Win7_Win8]		[OS_WinSer2008]		[OS_LinUS_14]		[OS_LinUS_12]		[OS_SuseLin_11]	
Impacto		5		5		5		3	5		3		3		3		2		2		2		3		2		5		5		5		8	
AMENAZAS	[I.5]	10	3	10	3	10	3	6	2	10	3	6	2	6	2	6	2	2	1	2	1	2	1	9	3	6	2	15	4	15	4	15	4	24	4
	[E.2]	5	2	5	2	5	2	3	2	10	3	6	2	6	2	6	2	2	1	2	1	2	1	6	2	4	2	10	3	10	3	10	3	16	4
	[E.8]	5	2	5	2	5	2	3	2	5	2	3	2	3	2	3	2	2	1	2	1	2	1	3	2	8	3	20	4	20	4	20	4	32	4
	[E.9]	10	3	10	3	10	3	6	2	10	3	6	2	6	2	6	2	2	1	2	1	2	1	6	2	6	2	15	4	15	4	15	4	24	4
	[E.18]	5	2	5	2	5	2	3	2	5	2	3	2	3	2	3	2	6	2	6	2	6	2	9	3	4	2	10	3	10	3	10	3	16	4
	[E.19]	15	4	15	4	15	4	9	3	10	3	6	2	6	2	6	2	6	2	6	2	6	2	6	2	2	1	5	2	5	2	5	2	8	3
	[E.20]	15	4	15	4	15	4	9	3	10	3	6	2	6	2	6	2	8	3	8	3	8	3	6	2	8	3	20	4	20	4	20	4	32	4
	[E.21]	20	4	20	4	20	4	12	3	10	3	6	2	6	2	6	2	6	2	6	2	6	2	9	3	8	3	20	4	20	4	20	4	32	4
	[A.5]	5	2	5	2	5	2	3	2	5	2	3	2	3	2	3	2	4	2	4	2	4	2	6	2	6	2	15	4	15	4	15	4	24	4
	[A.6]	15	4	15	4	15	4	9	3	5	2	3	2	3	2	3	2	4	2	4	2	4	2	6	2	6	2	15	4	15	4	15	4	24	4
	[A.7]	10	3	10	3	10	3	6	2	10	3	6	2	6	2	6	2	6	2	6	2	6	2	3	2	6	2	15	4	15	4	15	4	24	4
	[A.8]	5	2	5	2	5	2	3	2	5	2	3	2	3	2	3	2	4	2	4	2	4	2	3	2	6	2	15	4	15	4	15	4	24	4
	[A.11]	10	3	10	3	10	3	6	2	10	3	6	2	6	2	6	2	8	3	8	3	8	3	3	2	4	2	10	3	10	3	10	3	16	4
	[A.15]	5	4	5	2	5	2	3	2	5	2	3	2	3	2	3	2	8	3	8	3	8	3	3	2	2	1	5	2	5	2	5	2	8	3
	[A.18]	5	2	5	2	5	2	3	2	5	2	3	2	3	2	3	2	8	3	8	3	8	3	9	3	2	1	5	2	5	2	5	2	8	3
	[A.22]	5	2	5	2	5	2	3	2	5	2	3	2	3	2	3	2	8	3	8	3	8	3	6	2	4	2	10	3	10	3	10	3	16	4
Nivel de Riesgo Total		2,88		2,88		2,88		2,25	2,5		2		2		2		2,06		2,06		2,06		2,25		2		3,38		3,38		3,38		3,81	
		T		T		T		T	T		T		T		T		T		T		T		T		T		I		I		I		I	
Tratamiento del Riesgo		MIT		TR		TR		TR	MIT		MIT		MIT		MIT		MIT		MIT		MIT		MIT		MIT		EV		MIT		MIT		MIT	

Fuente: Los autores

Tabla 38. Análisis y Evaluación de Riesgos en Hardware

		Riesgo																	
		Nivel de Riesgo																	
		[host]		[mid]				[pc]				[print]		[switch]		[router]		[pabx]	
		[Servidor]		[PC escritorio]		[PC todoenuno]		[PC portatiles]		[Tablets]		[Impresoras]		[Switches]		[Routers]		[Troncal SIP]	
Impacto		5		3		3		2		2		1		5		5		2	
AMENAZAS	[N.1]	5	2	3	2	3	2	2	1	2	1	1	1	5	2	5	2	2	1
	[N.2]	5	2	3	2	3	2	4	2	4	2	1	1	5	2	5	2	2	1
	[N.7]	5	2	3	2	3	2	2	1	2	1	1	1	5	2	5	2	2	1
	[I.1]	5	2	3	2	3	2	2	1	2	1	1	1	5	2	5	2	2	1
	[I.2]	5	2	6	2	6	2	4	2	4	2	1	1	5	2	5	2	4	2
	[I.3]	10	3	9	3	9	3	6	2	6	2	2	1	10	3	10	3	4	2
	[I.4]	5	2	3	2	3	2	2	1	2	1	1	1	5	2	5	2	2	1
	[I.5]	10	3	6	2	6	2	4	2	4	2	4	2	10	3	10	3	4	2
	[I.6]	15	4	9	3	9	3	4	2	4	2	3	2	15	4	15	4	6	2
	[I.7]	10	3	6	2	6	2	4	2	4	2	2	1	10	3	10	3	4	2
	[E.23]	5	2	6	2	6	2	4	2	4	2	2	1	5	2	5	2	4	2
	[E.24]	10	3	6	2	6	2	4	2	4	2	2	1	10	3	10	3	4	2
	[E.25]	5	2	3	2	3	2	4	2	4	2	1	1	5	2	5	2	2	1
	[A.6]	5	2	3	2	3	2	2	1	2	1	1	1	5	2	5	2	2	1
	[A.7]	5	2	6	2	6	2	4	2	4	2	2	1	5	2	5	2	2	1
	[A.11]	5	2	3	2	3	2	2	1	2	1	1	1	5	2	10	3	4	2
	[A.23]	5	2	6	2	6	2	4	2	4	2	2	1	5	2	5	2	4	2
	[A.24]	5	2	3	2	3	2	2	1	2	1	1	1	5	2	5	2	2	1
	[A.25]	5	2	3	2	3	2	4	2	4	2	1	1	5	2	5	2	2	1
	[A.26]	5	2	3	2	3	2	2	1	2	1	1	1	5	2	5	2	2	1
Nivel de Riesgo Total		2,3		2,1		2,1		1,6		1,6		1,1		2,3		2,35		1,45	
		T		T		T		A		A		A		T		T		A	
Tratamiento del Riesgo		MIT		MIT		MIT		FIN		FIN		FIN		MIT		MIT		FIN	

Fuente: Los autores

Tabla 39. Análisis y Evaluación de Riesgos en Equipos Auxiliares

		Riesgo		Nivel de Riesgo			
		[ups]		[wire]		[suplly]	
		[UPS Servidores]		[Cab electrico]		[Consumibles]	
Impacto		5		3		2	
AMENAZAS	[N.1]	5	2	3	2	2	1
	[N.2]	10	3	6	2	4	2
	[N.7]	5	2	3	2	2	1
	[I.1]	5	2	3	2	2	1
	[I.2]	10	3	6	2	4	2
	[I.3]	10	3	6	2	4	2
	[I.4]	5	2	3	2	2	1
	[I.5]	10	3	3	2	6	2
	[I.6]	15	4	9	3	2	1
	[I.7]	10	3	9	3	6	2
	[I.9] [E.23]	5	2	6	2	4	2
	[E.25]	10	3	6	2	2	1
	[A.7]	5	2	3	2	8	3
	[A.11]	5	2	6	2	6	2
	[A.23]	5	2	3	2	1	1
	[A.25]	10	3	3	2	6	2
	[A.26]	5	2	3	2	8	3
		5	2	3	2	2	1
Nivel de Riesgo Total		2,5		2,11		1,67	
		T		T		A	
Tratamiento del Riesgo		MIT		MIT		FIN	

Fuente: Los autores

Tabla 40. Análisis y Evaluación de Riesgos en Servicios contratados

		Riesgo		Nivel de Riesgo	
		[internet]		[ADSL]	
Impacto		2		2	
AMENAZAS	I.8]	6	2	4	2
	[E.2]	4	2	4	2
	[E.9]	2	1	2	1
	[E.24]	2	1	2	1
	[A.5]	2	1	2	1
	[A.6]	4	2	4	2
	[A.7]	6	2	4	2
	[A.11]	2	1	2	1
	[A.12]	2	1	2	1
	[A.14]	2	1	2	1
	[A.15]	2	1	2	1
	[A.19]	2	1	2	1
	[A.24]	2	1	2	1
Nivel de Riesgo Total		1,31		1,31	
		A		A	
Tratamiento del Riesgo		FIN		FIN	

Fuente: Los autores

Tabla 41. Análisis y Evaluación de Riesgos en Personal

		Riesgo		Nivel de Riesgo			
		[UE]		[UFI]		[DS]	
Impacto		2		3		3	
AMENAZAS	E.7]	2	1	6	2	6	2
	[E.19]	4	2	6	2	3	2
	[E.28]	2	1	9	3	9	3
	[A.28]	4	2	9	3	9	3
	[A.29]	2	1	3	2	3	2
	[A.30]	2	1	6	2	6	2
Nivel de Riesgo Total		1,33		2,33		2,33	
		A		T		T	

Fuente: Los autores

8.4.2 Implantación de un Sistema de Controles Internos Informáticos

Para implantación del sistema de controles interno informáticos, se debe conocer acerca de:

- **Gestión de sistema de información**: Para poder establecer políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas de información y de los controles correspondientes.
- **Administración de sistemas**: Para poder implementar controles en la actividad de los centros de datos incluyendo la administración de las redes.
- **Seguridad**: Lo cual permite mejorar los controles implementados en los diferentes sistemas aumentando su confidencialidad y disponibilidad.
- **Gestión del cambio**: Para poder afrontar los cambios y afrontar las amenazas que aparecen continuamente.

8.4.3 Declaración de Aplicabilidad

La presente declaración muestra los controles que son relevantes para la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas, y aplicables al mismo. 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 42. Declaración de aplicabilidad

Declaración de Aplicabilidad	Vigente para el: 29/11/2016
La presente declaración los controles que son relevantes para el SGSI de la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas, y aplicables al mismo. 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; **TSE**: hasta cierto punto	

ISO 27001:2013 Controles de Seguridad			**Controles actuales**	**Comentarios (justificación de exclusión)**	**Controles seleccionados y razones de selección**				**Comentarios (visión general de la implementación)**
					LR	**CO**	**BR/BP**	**RRA**	
Cláusula	**Sección**	**Objetivo de control / control**							
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.			X		X		Actualizar las políticas de SI.
	5.1.2	Revisión de las políticas de seguridad de la información.			X		X		Actualizar las políticas de SI que incluyan procedimientos actuales en el SIG.
6 Organización de la Seguridad de la Información	6,1	Organización interna							
	6.1.1	Roles y responsabilidad de seguridad de la información.					X		Incluir las responsabilidades incluidas en las políticas en los contratos de los funcionarios.
	6.1.2	Segregación de deberes.					X		Establecer verificación de no duplicidad de funciones entre funcionarios.

Tabla 42. (Continuación)

	6.1.3	Contacto con autoridades.			X		X		Establecer y documentar procedimientos.
	6.1.4	Contacto con grupos de interés especial.					X		Establecer y documentar procedimientos.
	6.1.5	Seguridad de la información en la gestión de proyectos.			X	X	X	X	Incluir cláusulas de seguridad y confidencialidad en los proyectos.
	6,2	Dispositivos móviles y teletrabajo							
	6.2.1	Política de dispositivos móviles.			X	X	X	X	Establecer y documentar e implementar una Política de dispositivos móviles
	6.2.2	Teletrabajo.							
7 Seguridad en los Recursos Humanos	7,1	Previo al empleo							
	7.1.1	Verificación de antecedentes.			X	X	X		Verificar autenticidad de documentos.
	7.1.2	Términos y condiciones del empleo.			X	X	X		Incluir responsabilidades en contratos de los funcionarios.
	7,2	Durante el empleo							
	7.2.1	Responsabilidades de la Alta Gerencia.			X	X	X		Seguimiento a las responsabilidades de alta gerencia.
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información.			X	X	X		Plan de capacitación y circulares internas
	7.2.3	Proceso disciplinario.			X	X			Proveer lineamientos jurídicos y establecer procesos de seguimiento disciplinario.
	7,3	Terminación y cambio de empleo							
	7.3.1	Termino de responsabilidades o cambio de empleo.			X	X			Incluir responsabilidades en contratos de los funcionarios.
8 Gestión de Activos	8,1	Responsabilidad de los activos							

Tabla 42. (Continuación)

	8.1.1	Inventario de activos.				X	X		Actualización de inventario con perfiles destinados a la gestión de activos TI por parte de la Oficina TIC.
	8.1.2	Propiedad de activos.							
	8.1.3	Uso aceptable de los activos.				X	X		Establecer, documentar e implementar política de uso de activos TI.
	8.1.4	Devolución de activos.			X	X	X		Verificar su cumplimiento.
	8,2	Clasificación de la información							
	8.2.1	Clasificación de la información.			X	X	X	X	Establecer y documentar procedimientos para la clasificación de la información.
	8.2.2	Etiquetado de la información.			X	X	X		Establecer y documentar procedimientos para la clasificación de la información.
	8.2.3	Manejo de activos.					X		Establecer y documentar política de uso de activos TI.
	8,3	Manejo de medios							
	8.3.1	Gestión de medios removibles.			X	X	X		Establecer, documentar e implementar política de uso de activos TI.
	8.3.2	Eliminación de medios.			X	X	X		Establecer, documentar e implementar política de uso de activos TI.
	8.3.3	Transporte de medios físicos.			X	X	X	X	Establecer, documentar e implementar política de uso de activos TI.
9 Control de Acceso	9,1	Requerimientos de negocio para el control de acceso							
	9.1.1	Política de control de acceso.			X	X	X	X	Establecer, documentar e implementar política de control de acceso.
	9.1.2	Acceso a redes y servicios de red.				X	X	X	Establecer, documentar e implementar política de control de acceso.
	9,2	Gestión de accesos de usuario							

Tabla 42. (Continuación)

	9.2.1	Registro y baja del usuario.			X	X	X	X	Establecer, documentar e implementar política de control de acceso.
	9.2.2	Provisión de acceso a usuarios.							Incluir en la política de control de acceso.
	9.2.3	Gestión de derechos de acceso privilegiados.							Incluir en la política de control de acceso.
	9.2.4	Gestión de información de autenticación secreta de usuarios.			X	X	X		Establecer, documentar e implementar política de control de acceso.
	9.2.5	Revisión de derechos de acceso de usuarios.				X	X		Establecer, documentar e implementar política de control de acceso.
	9.2.6	Eliminación o ajuste de derechos de acceso.				X	X		Establecer, documentar e implementar política de control de acceso.
	9,3	Responsabilidades del usuario							
	9.3.1	Uso de información de autenticación secreta.			X	X	X		Establecer, documentar e implementar política de control de acceso.
	9,4	Control de acceso de sistemas y aplicaciones							
	9.4.1	Restricción de acceso a la información.			X	X	X		Establecer, documentar e implementar política de control de acceso.
	9.4.2	Procedimientos de inicio de sesión seguro.			X	X	X	X	Establecer, documentar e implementar política de control de acceso.
	9.4.3	Sistema de gestión de contraseñas.					X	X	Establecer, documentar e Implementar política de control de contraseñas.
	9.4.4	Uso de programas y utilidades privilegiadas.			X	X	X	X	Establecer, documentar e implementar política de control de acceso.
	9.4.5	Control de acceso al código fuente del programa.							
10 Criptografía	10,1	Controles criptográficos							

Tabla 42. (Continuación)

	10.1.1	Política en el uso de controles criptográficos.			X	X	X	X	Establecer, documentar e implementar política de controles criptográficos.
	10.1.2	Gestión de llaves.		NO					
11 Seguridad Física y del Entorno	11,1	Áreas seguras							
	11.1.1	Perímetro de seguridad físico.			X	X	X	X	Definir y aplicar de perímetro de seguridad físico.
	11.1.2	Controles físicos de entrada.			X	X	X	X	Establecer, documentar e implementar control de acceso a oficinas de gestión de información.
	11.1.3	Seguridad de oficinas, habitaciones y facilidades.				X	X		Establecer, documentar e implementar control de acceso a oficinas de gestión de información.
	11.1.4	Protección contra amenazas externas y del ambiente.			X	X	X	X	
	11.1.5	Trabajo en áreas seguras.				X	X		Establecer, documentar y definir procesos de trabajo en áreas seguras.
	11.1.6	Áreas de entrega y carga.					X		Establecer, documentar e implementar control de acceso a oficinas de gestión de información.
	11,2	Equipo							
	11.2.1	Instalación y protección de equipo.				X	X	X	Realizar chequeo de mobiliario para uso de activos TI.
	11.2.2	Servicios de soporte.				X	X		Realizar verificación y mantenimiento preventivo periódico de sistemas de respaldo eléctrico.
	11.2.3	Seguridad en el cableado.				X	X	X	Realizar verificación y mantenimiento preventivo periódico de cableado estructurado.

Tabla 42. (Continuación)

	11.2.4	Mantenimiento de equipos.				X	X	X	Realizar verificación y mantenimiento preventivo periódico de equipos.
	11.2.5	Retiro de activos.				X	X		Establecer procedimientos de retiro de activos.
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones.		No se encuentran equipos fuera de las instalaciones.					
	11.2.7	Eliminación segura o reúso del equipo.			X	X	X		Establecer procedimientos para la eliminación segura o reúso de activos TI.
	11.2.8	Equipo de usuario desatendido.				X	X	X	Establecer procedimientos para control de sesión de usuario en equipos.
	11.2.9	Política de escritorio limpio y pantalla limpia.				X	X	X	Adoptar procedimientos para escritorio y pantalla limpios.
12 Seguridad en las Operaciones	12,1	Procedimientos Operacionales y Responsabilidades							
	12.1.1	Documentación de procedimientos operacionales.			X	X	X		Incluir funciones y obligaciones contractuales de seguridad informática.
	12.1.2	Gestión de cambios.				X	X		
	12.1.3	Gestión de la capacidad.				X	X		Establecer diagnostico periódico de equipos.
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.		No se desarrolla software.					
	12,2	Protección de Software Malicioso							
	12.2.1	Controles contra software malicioso.				X	X		Adquisición y mantenimiento de aplicativo de protección contra software malicioso.
	12,3	Respaldo							
	12.3.1	Respaldo de información.			X	X	X	X	Estandarizar y promover mediante políticas.

Tabla 42. (Continuación)

	12,4	Bitácoras y monitoreo							
	12.4.1	Bitácoras de eventos.			X	X	X	X	Establecer monitoreo de usuarios y eventos de seguridad.
	12.4.2	Protección de información en bitácoras.			X		X	X	Establecer monitoreo de usuarios y eventos de seguridad.
	12.4.3	Bitácoras de administrador y operador.			X		X	X	Establecer monitoreo de usuarios y eventos de seguridad.
	12.4.4	Sincronización de relojes.					X		Establecer monitoreo de usuarios y eventos de seguridad.
	12,5	Control de software operacional							
	12.5.1	Instalación de software en sistemas operacionales.				X	X		Establecer política de uso de activos TI y de control de acceso.
	12,6	Gestión de vulnerabilidades técnicas							
	12.6.1	Gestión de vulnerabilidades técnicas.				X	X	X	Realizar análisis y evaluación de riesgos TI.
	12.6.2	Restricciones en la instalación de software.			X	X	X	X	Establecer política de uso de activos TI y de control de acceso.
	12,7	Consideraciones de auditoria de sistemas de información							
	12.7.1	Controles de auditoría de sistemas de información.				X	X		Realizar auditoría de sistemas de información.
13 Seguridad en las Comunicaciones	13,1	Gestión de seguridad en red							
	13.1.1	Controles de red.							
	13.1.2	Seguridad en los servicios en red.				X	X	X	Realizar verificación y mantenimiento preventivo periódico de cableado estructurado.

Tabla 42. (Continuación)

	13.1.3	Segregación en redes.					X	X	Realizar verificación y mantenimiento preventivo periódico de cableado estructurado.
	13,2	Transferencia de información							
	13.2.1	Políticas y procedimientos para la transferencia de información.				X	X	X	Establecer políticas de transferencia de información al interior de la Administración Municipal.
	13.2.2	Acuerdos en la transferencia de información.			X	X	X	X	Establecer políticas de transferencia de información al interior de la Administración Municipal.
	13.2.3	Mensajería electrónica.				X	X	X	Establecer políticas de uso del correo electrónico institucional.
	13.2.4	Acuerdos de confidencialidad o no-revelación.			X	X	X	X	Establecer políticas de uso del correo electrónico institucional, acuerdos de confidencialidad en los procesos contractuales.
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.			X	X	X	X	Incluir en estudios de conveniencia previos y procesos contractuales.
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas.			X	X	X		Incluir encriptación de comunicaciones en características técnicas de aplicaciones que trabajen sobre redes públicas.
	14.1.3	Protección de transacciones en servicios de aplicación.			X	X	X	X	Establecer e implementar medidas de protección de transacciones.
	14,2	Seguridad en el proceso de desarrollo y soporte							
	14.2.1	Política de desarrollo seguro.		No se desarrolla software					

Tabla 42. (Continuación)

	14.2.2	Procedimientos de control de cambios del sistema.		No se desarrolla software					
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa.				X	X		Establecer lista de chequeo para revisión de aplicaciones.
	14.2.4	Restricción de cambios en paquetes de software.				X	X		
	14.2.5	Principios de seguridad en la ingeniería de sistemas.							
	14.2.6	Entorno de desarrollo seguro.		No se desarrolla software					
	14.2.7	Desarrollo tercerizado.				X	X		Establecer lista de chequeo para revisión de aplicaciones.
	14.2.8	Pruebas de seguridad del sistema.							Establecer lista de chequeo para revisión de aplicaciones.
	14.2.9	Pruebas de aceptación del sistema.				X	X		Establecer lista de chequeo para revisión de aplicaciones.
	14,3	Datos de prueba							
	14.3.1	Protección de datos de prueba.				X	X		Establecer procedimiento para el almacenamiento seguro de datos de prueba.
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.				X	X		Establecer e implementar.
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor.				X	X		Establecer e implementar.
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones.				X	X		Establecer e implementar.
	1522	Gestión de entrega de servicios de proveedor							
	15.2.1	Monitoreo y revisión de servicios del proveedor.			X	X	X		Establecer lista de chequeo para revisión de servicios.

Tabla 42. (Continuación)

	15.2.2	Gestión de cambios a los servicios del proveedor.			X	X	X		Establecer e implementar Política de seguridad de la información en las relaciones con el proveedor.
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.				X	X	X	Establecer plan de contingencia.
	16.1.2	Reporte de eventos de seguridad de la información.				X	X	X	Establecer plan de contingencia.
	16.1.3	Reporte de debilidades de seguridad de la información.				X	X	X	Establecer plan de contingencia.
	16.1.4	Valoración y decisión de eventos de seguridad de la información.				X	X	X	Establecer plan de contingencia.
	16.1.5	Respuesta a incidentes de seguridad de la información.				X	X	X	Establecer plan de contingencia.
	16.1.6	Aprendizaje de incidentes de seguridad de la información.				X	X	X	Establecer plan de contingencia.
	16.1.7	Colección de evidencia.				X	X	X	Establecer plan de contingencia.
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	Planeación de la continuidad de la seguridad de la información.			X		X		Establecer plan de continuidad del negocio.
	17.1.2	Implementación de la continuidad de la seguridad de la información.			X		X		Establecer plan de continuidad del negocio.
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.			X		X		Establecer plan de continuidad del negocio.
	17,2	Redundancias							
	17.2.1	Disponibilidad de facilidades de procesamiento de información.			X		X	X	

Tabla 42. (Continuación)

18 Cumplimiento	18,1	Cumplimiento con Requerimientos Legales y Contractuales							
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales.			X	X	X		Incluir normatividad, reglamentación y legislación respectiva.
	18.1.2	Derechos de propiedad intelectual (IPR).			X	X	X		Establecer verificación y seguimiento a licenciamiento de aplicaciones y software.
	18.1.3	Protección de registros.			X	X	X		Establecer verificación y seguimiento a licenciamiento de aplicaciones y software.
	18.1.4	Privacidad y protección de información personal identificable (PIR).			X	X	X		Realizar capacitación, promoción, divulgación y aplicación de Ley 1273 de 2009.
	18.1.5	Regulación de controles criptográficos.			X	X	X		
	18,2	Revisiones de seguridad de la información							
	18.2.1	Revisión independiente de seguridad de la información.			X	X	X		Realizar auditoría externa a las políticas de SI.
	18.2.2	Cumplimiento con políticas y estándares de seguridad.			X	X	X		Realizar auditoría externa a las políticas de SI.
	18.2.3	Revisión del cumplimiento técnico.			X	X	X		Realizar auditoría externa a las políticas de SI.

Fuente: Los autores

8.5 Nivel de Madurez

Tabla 43. Nivel de Madurez

ISO 27001:2013 Controles de Seguridad			Nivel de Madurez por Objetivo de Control		Nivel de Madurez por Cláusula o Dominio de Control	
Cláusula	**Sección**	**Objetivo de control / control**	**Cualitativo**	**Cuantitativo**	**Cualitativo**	**Cuantitativo**
5 Políticas de Seguridad	5,1	Dirección de la alta gerencia para la seguridad de la información	**INICIAL**	**20%**	**INICIAL**	**20%**
	5.1.1	Políticas de seguridad de la información.	Inicial	20%		
	5.1.2	Revisión de las políticas de seguridad de la información.	Inicial	20%		
6 Organización de la Seguridad de la Información	6,1	Organización interna	**INICIAL**	**20%**	**INICIAL**	**17%**
	6.1.1	Roles y responsabilidad de seguridad de la información.	Inicial	20%		
	6.1.2	Segregación de deberes.	Inicial	20%		
	6.1.3	Contacto con autoridades.	Inicial	20%		
	6.1.4	Contacto con grupos de interés especial.	Inicial	20%		
	6.1.5	Seguridad de la información en la gestión de proyectos.	Inicial	20%		
	6,2	Dispositivos móviles y teletrabajo	**INICIAL**	**10%**		
	6.2.1	Política de dispositivos móviles.	Inicial	20%		
	6.2.2	Teletrabajo.	Inexistente	0%		
7 Seguridad en los Recursos Humanos	7,1	Previo al empleo	**ADMIINISTRADO**	**80%**	**ADMIINISTRADO**	**67%**
	7.1.1	Verificación de antecedentes.	Administrado	80%		
	7.1.2	Términos y condiciones del empleo.	Administrado	80%		
	7,2	Durante el empleo	**DEFINIDO**	**60%**		
	7.2.1	Responsabilidades de la Alta Gerencia.	Definido	60%		
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información.	Definido	60%		
	7.2.3	Proceso disciplinario.	Definido	60%		
	7,3	Terminación y cambio de empleo	**DEFINIDO**	**40%**		
	7.3.1	Termino de responsabilidades o cambio de empleo.	Definido	60%		

Tabla 43. (Continuación)

8 Gestión de Activos	8,1	Responsabilidad de los activos	**INICIAL**	**20%**	**INICIAL**	**20%**
	8.1.1	Inventario de activos.	Inicial	20%		
	8.1.2	Propiedad de activos.	Inicial	20%		
	8.1.3	Uso aceptable de los activos.	Inicial	20%		
	8.1.4	Devolución de activos.	Inicial	20%		
	8,2	Clasificación de la información	**INICIAL**	**20%**		
	8.2.1	Clasificación de la información.	Inicial	20%		
	8.2.2	Etiquetado de la información.	Inicial	20%		
	8.2.3	Manejo de activos.	Inicial	20%		
	8,3	Manejo de medios	**INICIAL**	**20%**		
	8.3.1	Gestión de medios removibles.	Inicial	20%		
	8.3.2	Eliminación de medios.	Inicial	20%		
	8.3.3	Transporte de medios físicos.	Inicial	20%		
9 Control de Acceso	9,1	Requerimientos de negocio para el control de acceso	**INICIAL**	**20%**	**INICIAL**	**19%**
	9.1.1	Política de control de acceso.	Inicial	20%		
	9.1.2	Acceso a redes y servicios de red.	Inicial	20%		
	9,2	Gestión de accesos de usuario	**INICIAL**	**20%**		
	9.2.1	Registro y baja del usuario.	Inicial	20%		
	9.2.2	Provisión de acceso a usuarios.	Inicial	20%		
	9.2.3	Gestión de derechos de acceso privilegiados.	Inicial	20%		
	9.2.4	Gestión de información de autenticación secreta de usuarios.	Inicial	20%		
	9.2.5	Revisión de derechos de acceso de usuarios.	Inicial	20%		
	9.2.6	Eliminación o ajuste de derechos de acceso.	Inicial	20%		
	9,3	Responsabilidades del usuario	**INICIAL**	**20%**		
	9.3.1	Uso de información de autenticación secreta.	Inicial	20%		
	9,4	Control de acceso de sistemas y aplicaciones	**INICIAL**	**16%**		
	9.4.1	Restricción de acceso a la información.	Inicial	20%		
	9.4.2	Procedimientos de inicio de sesión seguro.	Inicial	20%		

Tabla 43. (Continuación)

	9.4.3	Sistema de gestión de contraseñas.	Inicial	20%		
	9.4.4	Uso de programas y utilidades privilegiadas.	Inicial	20%		
	9.4.5	Control de acceso al código fuente del programa.	Inexistente	0%		
10 Criptografía	10,1	Controles criptográficos	**INICIAL**	**10%**	**INICIAL**	**10%**
	10.1.1	Política en el uso de controles criptográficos.	Inicial	20%		
	10.1.2	Gestión de llaves.	Inexistente	0%		
11 Seguridad Física y del Entorno	11,1	Áreas seguras	**INICIAL**	**17%**	**INICIAL**	**17%**
	11.1.1	Perímetro de seguridad físico.	Inicial	20%		
	11.1.2	Controles físicos de entrada.	Inicial	20%		
	11.1.3	Seguridad de oficinas, habitaciones y facilidades.	Inicial	20%		
	11.1.4	Protección contra amenazas externas y del ambiente.	Inexistente	0%		
	11.1.5	Trabajo en áreas seguras.	Inicial	20%		
	11.1.6	Áreas de entrega y carga.	Inicial	20%		
	11,2	Equipo	**INICIAL**	**18%**		
	11.2.1	Instalación y protección de equipo.	Inicial	20%		
	11.2.2	Servicios de soporte.	Inicial	20%		
	11.2.3	Seguridad en el cableado.	Inicial	20%		
	11.2.4	Mantenimiento de equipos.	Inicial	20%		
	11.2.5	Retiro de activos.	Inicial	20%		
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones.	Inexistente	0%		
	11.2.7	Eliminación segura o reúso del equipo.	Inicial	20%		
	11.2.8	Equipo de usuario desatendido.	Inicial	20%		
	11.2.9	Política de escritorio limpio y pantalla limpia.	Inicial	20%		
12 Seguridad en las Operaciones	12,1	Procedimientos Operacionales y Responsabilidades	**INICIAL**	**7%**	**INICIAL**	**17%**
	12.1.1	Documentación de procedimientos operacionales.	Inicial	20%		
	12.1.2	Gestión de cambios.	Inexistente	0%		
	12.1.3	Gestión de la capacidad.	Inicial	20%		

Tabla 43. (Continuación)

	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.	Inexistente	0%		
	12,2	Protección de Software Malicioso	**INICIAL**	**20%**		
	12.2.1	Controles contra software malicioso.	Inicial	20%		
	12,3	Respaldo	**INICIAL**	**20%**		
	12.3.1	Respaldo de información.	Inicial	20%		
	12,4	Bitácoras y monitoreo	**INICIAL**	**20%**		
	12.4.1	Bitácoras de eventos.	Inicial	20%		
	12.4.2	Protección de información en bitácoras.	Inicial	20%		
	12.4.3	Bitácoras de administrador y operador.	Inicial	20%		
	12.4.4	Sincronización de relojes.	Inicial	20%		
	12,5	Control de software operacional	**INICIAL**	**20%**		
	12.5.1	Instalación de software en sistemas operacionales.	Inicial	20%		
	12,6	Gestión de vulnerabilidades técnicas	**INICIAL**	**20%**		
	12.6.1	Gestión de vulnerabilidades técnicas.	Inicial	20%		
	12.6.2	Restricciones en la instalación de software.	Inicial	20%		
	12,7	Consideraciones de auditoria de sistemas de información	**INICIAL**	**20%**		
	12.7.1	Controles de auditoría de sistemas de información.	Inicial	20%		
13 Seguridad en las Comunicaciones	13,1	Gestión de seguridad en red	**INICIAL**	**13%**	**INICIAL**	**17%**
	13.1.1	Controles de red.	Inexistente	0%		
	13.1.2	Seguridad en los servicios en red.	Inicial	20%		
	13.1.3	Segregación en redes.	Inicial	20%		
	13,2	Transferencia de información	**INICIAL**	**20%**		
	13.2.1	Políticas y procedimientos para la transferencia de información.	Inicial	20%		
	13.2.2	Acuerdos en la transferencia de información.	Inicial	20%		
	13.2.3	Mensajería electrónica.	Inicial	20%		
	13.2.4	Acuerdos de confidencialidad o no-revelación.	Inicial	20%		

Tabla 43. (Continuación)

14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14,1	Requerimientos de seguridad en sistemas de información	**INICIAL**	**20%**	**INICIAL**	**12%**
	14.1.1	Análisis y especificación de requerimientos de seguridad.	Inicial	20%		
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas.	Inicial	20%		
	14.1.3	Protección de transacciones en servicios de aplicación.	Inicial	20%		
	14,2	Seguridad en el proceso de desarrollo y soporte	**INICIAL**	**9%**		
	14.2.1	Política de desarrollo seguro.	Inexistente	0%		
	14.2.2	Procedimientos de control de cambios del sistema.	Inexistente	0%		
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa.	Inicial	20%		
	14.2.4	Restricción de cambios en paquetes de software.	Inexistente	0%		
	14.2.5	Principios de seguridad en la ingeniería de sistemas.	Inexistente	0%		
	14.2.6	Entorno de desarrollo seguro.	Inexistente	0%		
	14.2.7	Desarrollo tercerizado.	Inicial	20%		
	14.2.8	Pruebas de seguridad del sistema.	Inicial	20%		
	14.2.9	Pruebas de aceptación del sistema.	Inicial	20%		
	14,3	Datos de prueba	**INICIAL**	**20%**		
	14.3.1	Protección de datos de prueba.	Inicial	20%		
15 Relaciones con Proveedores	15,1	Seguridad de la información en relaciones con el proveedor	**INICIAL**	**20%**	**INICIAL**	**20%**
	15.1.1	Política de seguridad de la información en las relaciones con el proveedor.	Inicial	20%		
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor.	Inicial	20%		
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones.	Inicial	20%		
	15,2	Gestión de entrega de servicios de proveedor	**INICIAL**	**20%**		
	15.2.1	Monitoreo y revisión de servicios del proveedor.	Inicial	20%		
	15.2.2	Gestión de cambios a los servicios del proveedor.	Inicial	20%		

Tabla 43. (Continuación)

16 Gestión de Incidentes de Seguridad de la Información	16,1	Gestión de incidentes de seguridad de la información y mejoras	**INICIAL**	**20%**	**INICIAL**	**20%**
	16.1.1	Responsabilidades y procedimientos.	Inicial	20%		
	16.1.2	Reporte de eventos de seguridad de la información.	Inicial	20%		
	16.1.3	Reporte de debilidades de seguridad de la información.	Inicial	20%		
	16.1.4	Valoración y decisión de eventos de seguridad de la información.	Inicial	20%		
	16.1.5	Respuesta a incidentes de seguridad de la información.	Inicial	20%		
	16.1.6	Aprendizaje de incidentes de seguridad de la información.	Inicial	20%		
	16.1.7	Colección de evidencia.	Inicial	20%		
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17,1	Continuidad de la seguridad de la información	**INICIAL**	**20%**	**INICIAL**	**15%**
	17.1.1	Planeación de la continuidad de la seguridad de la información.	Inicial	20%		
	17.1.2	Implementación de la continuidad de la seguridad de la información.	Inicial	20%		
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Inicial	20%		
	17,2	Redundancias	**INEXISTENTE**	**0%**		
	17.2.1	Disponibilidad de facilidades de procesamiento de información.	Inexistente	0%		
18 Cumplimiento	18,1	Cumplimiento con Requerimientos Legales y Contractuales	**INICIAL**	**20%**	**INICIAL**	**20%**
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales.	Inicial	20%		
	18.1.2	Derechos de propiedad intelectual (IPR).	Inicial	20%		

Tabla 43. (Continuación)

	18.1.3	Protección de registros.	Inicial	20%		
	18.1.4	Privacidad y protección de información personal identificable (PIR).	Inicial	20%		
	18.1.5	Regulación de controles criptográficos.	Inicial	20%		
	18,2	Revisiones de seguridad de la información	**INICIAL**	**20%**		
	18.2.1	Revisión independiente de seguridad de la información.	Inicial	20%		
	18.2.2	Cumplimiento con políticas y estándares de seguridad.	Inicial	20%		
	18.2.3	Revisión del cumplimiento técnico.	Inicial	20%		

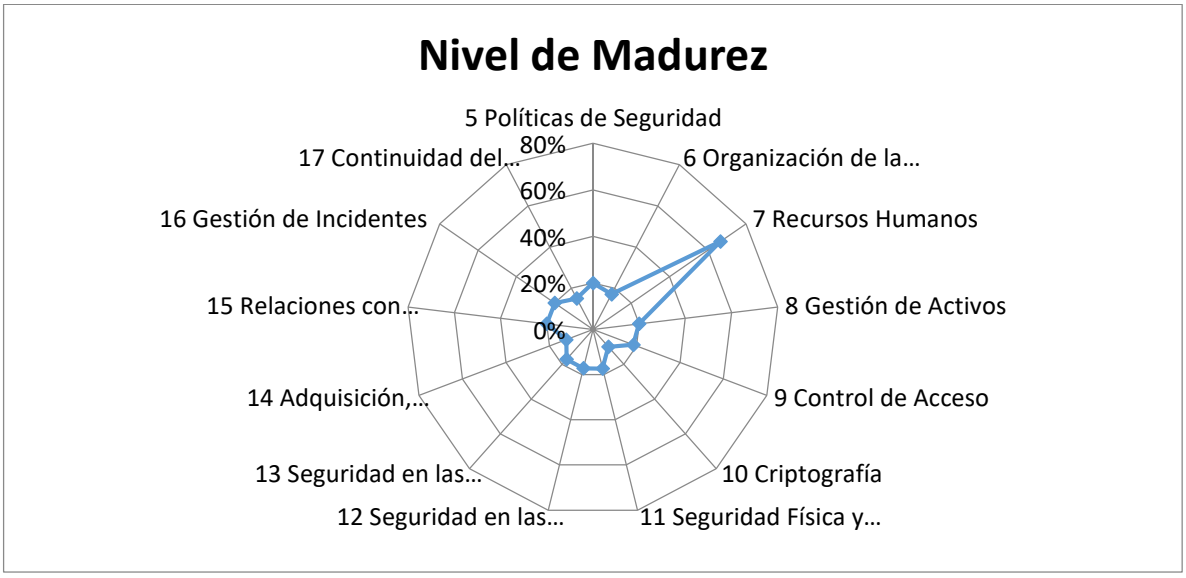
Fuente: Los autores

Tabla 44. Consolidado nivel de madurez

Cláusula	Nivel de Madurez
5 Políticas de Seguridad	**20%**
6 Organización de la Seguridad de la Información	**17%**
7 Recursos Humanos	**67%**
8 Gestión de Activos	**20%**
9 Control de Acceso	**19%**
10 Criptografía	**10%**
11 Seguridad Física y del Entorno	**17%**
12 Seguridad en las Operaciones	**17%**
13 Seguridad en las Comunicaciones	**17%**
14 Adquisición, Desarrollo y Mantenimiento	**12%**
15 Relaciones con Proveedores	**20%**
16 Gestión de Incidentes	**20%**
17 Continuidad del Negocio	**15%**
18 Cumplimiento	**20%**

Fuente: Los autores

Figura 5. Nivel de Madurez



Fuente: Los autores

8.5.1 Plan de Tratamiento de Riesgos

Tabla 45. Plan de Tratamiento de Riesgos para la CCD

ISO 27001:2013 Controles de Seguridad			Activos de Información	Actividad/Descripción	Prioridad	Estado	Responsable	Fecha de Término
Cláusula	**Sección**	**Objetivo de control / control**						
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.	Inexistente	Establecer y documentar políticas de SI.	A	Iniciado	Dirección de Sistemas	jun-17
	5.1.2	Revisión de las políticas de seguridad de la información.	Inexistente	Establecer y documentar políticas de SI.	A	Iniciado	Dirección de Sistemas	jun-17
6 Organización de la Seguridad de la Información	6,1	Organización interna						
	6.1.1	Roles y responsabilidad de seguridad de la información.	Director de Sistemas - Usuarios Finales - Usuarios Externos	Incluir las responsabilidades incluidas en las políticas en los contratos de los funcionarios.	A	Iniciado	Dirección de Sistemas	jun-17
	6.1.2	Segregación de deberes.	Director de Sistemas - Usuarios Finales - Usuarios Externos	Establecer verificación de no duplicidad de funciones entre funcionarios.	A	Iniciado	Dirección de Sistemas	jun-18
	6.1.3	Contacto con autoridades.	Director de Sistemas - Usuarios Finales - Usuarios Externos	Establecer y documentar procedimientos.	A	Iniciado	Dirección de Sistemas	jun-17
	6.1.4	Contacto con grupos de interés especial.	Director de Sistemas	Establecer y documentar procedimientos.	M	Iniciado	Dirección de Sistemas	jun-17
	6.1.5	Seguridad de la información en la gestión de proyectos.	Director de Sistemas	Incluir cláusulas de seguridad y confidencialidad en los proyectos.	A	Iniciado	Dirección de Sistemas	dic-17
	6,2	Dispositivos móviles y teletrabajo						
	6.2.1	Política de dispositivos móviles.	Director de Sistemas - Usuarios Finales	Establecer, documentar e implementar.	A	Iniciado	Dirección de Sistemas	dic-18

Tabla 45. (Continuación)

7 Seguridad en los Recursos Humanos	7,1	Previo al empleo						
	7.1.1	Verificación de antecedentes.	Documentos Contractuales - Estudios previos y de conveniencia	Verificar autenticidad de documentos.	A	Administrado	Dirección Administrativa	dic-16
	7.1.2	Términos y condiciones del empleo.	Estudios previos y de conveniencia - Contratos de Personal - Contrato de Servicios con Terceros	Incluir responsabilidades en contratos de los funcionarios.	A	Administrado	Dirección Administrativa	dic-18
	7,2	Durante el empleo						
	7.2.1	Responsabilidades de la Alta Gerencia.	Manual de Gestión de Calidad	Seguimiento a las responsabilidades de alta gerencia.	A	Realizado	Dirección Administrativa	jun-17
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información.	Plan de Capacitación y Sensibilización en Seguridad de la Información al personal, contratistas y terceros.	Plan de capacitación y circulares internas.	A	Realizado	Dirección Administrativa	dic-17
	7.2.3	Proceso disciplinario.	Manual de Funciones	Proveer lineamientos jurídicos y establecer procesos de seguimiento disciplinario.	A	Realizado	Dirección Administrativa	dic-18
	7,3	Terminación y cambio de empleo						
	7.3.1	Termino de responsabilidades o cambio de empleo.	Contratos de Personal - Contrato de Servicios con Terceros	Incluir responsabilidades en contratos de los funcionarios.	M	Realizado	Dirección Administrativa	jun-17
8 Gestión de Activos	8,1	Responsabilidad de los activos						
	8.1.1	Inventario de activos.	Inventario de Activos de Información	Actualización de inventario con perfiles destinados a la gestión de activos TI por parte de la Oficina TIC.	A	Iniciado	Dirección de Sistemas	jun-17

Tabla 45. (Continuación)

	8.1.3	Uso aceptable de los activos.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer, documentar e implementar política de uso de activos TI.	A	Iniciado	Dirección de Sistemas	jun-17
	8.1.4	Devolución de activos.	Hardware - Equipos auxiliares	Verificar su cumplimiento.	A	Iniciado	Dirección de Sistemas	jun-17
	8,2	Clasificación de la información						
	8.2.1	Clasificación de la información.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer y documentar procedimientos para la clasificación de la información.	A	Iniciado	Dirección de Sistemas	jun-17
	8.2.2	Etiquetado de la información.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer y documentar procedimientos para la clasificación de la información.	A	Iniciado	Dirección de Sistemas	jun-17
	8.2.3	Manejo de activos.	Aplicaciones y Software - Hardware - Equipos auxiliares - Internet	Establecer y documentar política de uso de activos TI.	A	Iniciado	Dirección de Sistemas	jun-17
	8,3	Manejo de medios						
	8.3.1	Gestión de medios removibles.	Hardware	Establecer, documentar e implementar política de uso de activos TI.	A	Iniciado	Dirección de Sistemas	jun-17
	8.3.2	Eliminación de medios.	Hardware	Establecer, documentar e implementar política de uso de activos TI.	A	Iniciado	Dirección de Sistemas	jun-17
	8.3.3	Transporte de medios físicos.	Hardware - Equipos auxiliares	Establecer, documentar e implementar política de uso de activos TI.	A	Iniciado	Dirección de Sistemas	jun-17
9 Control de Acceso	9,1	Requerimientos de negocio para el control de acceso						
	9.1.1	Política de control de acceso.	Aplicaciones y Software - Hardware - Equipos auxiliares – Internet	Establecer, documentar e implementar política de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17

Tabla 45. (Continuación)

	9.1.2	Acceso a redes y servicios de red.	Aplicaciones y Software - Hardware - Equipos auxiliares - Internet	Establecer, documentar e implementar política de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17
	9,2	Gestión de accesos de usuario						
	9.2.1	Registro y baja del usuario.	Aplicaciones y Software - Hardware	Establecer, documentar e implementar política de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17
	9.2.2	Provisión de acceso a usuarios.	Aplicaciones y Software - Hardware - Internet	Incluir en la política de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17
	9.2.3	Gestión de derechos de acceso privilegiados.	Aplicaciones y Software - Hardware - Internet	Incluir en la política de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17
	9.2.4	Gestión de información de autenticación secreta de usuarios.	Aplicaciones y Software - Hardware - Internet	Establecer, documentar e implementar política de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17
	9.2.5	Revisión de derechos de acceso de usuarios.	Aplicaciones y Software - Hardware - Internet	Establecer, documentar e implementar política de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17
	9.2.6	Eliminación o ajuste de derechos de acceso.	Aplicaciones y Software - Hardware – Internet	Establecer, documentar e implementar política de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17
	9,3	Responsabilidades del usuario						
	9.3.1	Uso de información de autenticación secreta.	Aplicaciones y Software - Hardware - Internet	Establecer, documentar e implementar política de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17

Tabla 45. (Continuación)

	9,4	Control de acceso de sistemas y aplicaciones						
	9.4.1	Restricción de acceso a la información.	Aplicaciones y Software - Hardware - Internet	Establecer, documentar e implementar política de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17
	9.4.2	Procedimientos de inicio de sesión seguro.	Aplicaciones y Software - Hardware - Internet	Establecer, documentar e implementar política de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17
	9.4.3	Sistema de gestión de contraseñas.	Aplicaciones y Software - Hardware - Internet	Establecer, documentar e Implementar política de control de contraseñas.	A	Iniciado	Dirección de Sistemas	jun-17
	9.4.4	Uso de programas y utilidades privilegiadas.	Aplicaciones y Software - Hardware - Internet	Establecer, documentar e implementar política de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17
10 Criptografía	10,1	Controles criptográficos						
	10.1.1	Política en el uso de controles criptográficos.	Aplicaciones y Software - Hardware - Internet	Establecer, documentar e implementar política de controles criptográficos.	A	Iniciado	Dirección de Sistemas	jun-17
11 Seguridad Física y del Entorno	11,1	Áreas seguras						
	11.1.1	Perímetro de seguridad físico.	Aplicaciones y Software - Hardware - Equipos auxiliares	Definir y aplicar de perímetro de seguridad físico.	A	Iniciado	Dirección Administrativa	jun-18
	11.1.2	Controles físicos de entrada.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer, documentar e implementar control de acceso a oficinas de gestión de información.	A	Iniciado	Dirección Administrativa	jun-18
	11.1.3	Seguridad de oficinas, habitaciones y facilidades.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer, documentar e implementar control de acceso a oficinas de gestión de información.	A	Iniciado	Dirección Administrativa	jun-18

Tabla 45. (Continuación)

	11.1.5	Trabajo en áreas seguras.	Inexistente	Establecer, documentar y definir procesos de trabajo en áreas seguras.	M	Iniciado	Dirección Administrativa	jun-18
	11.1.6	Áreas de entrega y carga.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer, documentar e implementar control de acceso a oficinas de gestión de información.	M	Iniciado	Dirección Administrativa	jun-18
	11,2	Equipo						
	11.2.1	Instalación y protección de equipo.	Hardware - Equipos auxiliares	Realizar chequeo de mobiliario para uso de activos TI.	M	Iniciado	Dirección de Sistemas	dic-17
	11.2.2	Servicios de soporte.	Hardware - Equipos auxiliares	Realizar verificación y mantenimiento preventivo periódico de sistemas de respaldo eléctrico.	A	Iniciado	Dirección de Sistemas	dic-17
	11.2.3	Seguridad en el cableado.	Hardware - Equipos auxiliares	Realizar verificación y mantenimiento preventivo periódico de cableado estructurado.	A	Iniciado	Dirección de Sistemas	dic-17
	11.2.4	Mantenimiento de equipos.	Hardware - Equipos auxiliares	Realizar verificación y mantenimiento preventivo periódico de equipos.	A	Iniciado	Dirección de Sistemas	dic-17
	11.2.5	Retiro de activos.	Hardware - Equipos auxiliares	Establecer procedimientos de retiro de activos.	A	Iniciado	Dirección de Sistemas	dic-17
	11.2.7	Eliminación segura o reúso del equipo.	Hardware - Equipos auxiliares	Establecer procedimientos para la eliminación segura o reúso de activos TI.	A	Iniciado	Dirección de Sistemas	jun-17
	11.2.8	Equipo de usuario desatendido.	Aplicaciones y Software - Hardware	Establecer procedimientos para control de sesión de usuario en equipos.	A	Iniciado	Dirección de Sistemas	jun-17
	11.2.9	Política de escritorio limpio y pantalla limpia.	Aplicaciones y Software	Adoptar procedimientos para escritorio y pantalla limpios.	M	Iniciado	Dirección de Sistemas	dic-17
12 Seguridad en las Operaciones	12,1	Procedimientos Operacionales y Responsabilidades						
	12.1.1	Documentación de procedimientos operacionales.	Director de Sistemas - Usuarios Finales - Usuarios Externos	Incluir funciones y obligaciones contractuales de seguridad informática.	A	Iniciado	Dirección Administrativa	jun-19

Tabla 45. (Continuación)

	12.1.3	Gestión de la capacidad.	Hardware - Equipos auxiliares	Establecer diagnostico periódico de equipos.	A	Iniciado	Dirección de Sistemas	dic-17
	12,2	Protección de Software Malicioso						
	12.2.1	Controles contra software malicioso.	Aplicaciones y Software	Adquisición y mantenimiento de aplicativo de protección contra software malicioso.	A	Iniciado	Dirección de Sistemas	dic-17
	12,3	Respaldo						
	12.3.1	Respaldo de información.	Aplicaciones y Software	Estandarizar y promover mediante políticas.	A	Iniciado	Dirección de Sistemas	dic-17
	12,4	Bitácoras y monitoreo						
	12.4.1	Bitácoras de eventos.	Aplicaciones y Software	Establecer monitoreo de usuarios y eventos de seguridad.	A	Iniciado	Dirección de Sistemas	jun-18
	12.4.2	Protección de información en bitácoras.	Aplicaciones y Software	Establecer monitoreo de usuarios y eventos de seguridad.	A	Iniciado	Dirección de Sistemas	jun-18
	12.4.3	Bitácoras de administrador y operador.	Aplicaciones y Software	Establecer monitoreo de usuarios y eventos de seguridad.	A	Iniciado	Dirección de Sistemas	jun-18
	12.4.4	Sincronización de relojes.	Aplicaciones y Software	Establecer monitoreo de usuarios y eventos de seguridad.	A	Iniciado	Dirección de Sistemas	jun-18
	12,5	Control de software operacional						
	12.5.1	Instalación de software en sistemas operacionales.	Aplicaciones y Software	Establecer política de uso de activos TI y de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17
	12,6	Gestión de vulnerabilidades técnicas						
	12.6.1	Gestión de vulnerabilidades técnicas.	Aplicaciones y Software - Hardware - Equipos auxiliares	Realizar análisis y evaluación de riesgos TI.	A	Iniciado	Dirección de Sistemas	dic-17
	12.6.2	Restricciones en la instalación de software.	Aplicaciones y Software	Establecer política de uso de activos TI y de control de acceso.	A	Iniciado	Dirección de Sistemas	jun-17
	12,7	Consideraciones de auditoria de sistemas de información						

Tabla 45. (Continuación)

	12.7.1	Controles de auditoría de sistemas de información.	Aplicaciones y Software	Realizar auditoría de sistemas de información.	A	Iniciado	Dirección de Sistemas	jun-18
13 Seguridad en las Comunicaciones	13,1	Gestión de seguridad en red						
	13.1.2	Seguridad en los servicios en red.	Contratos de Personal - Contratos de servicios con terceros	Realizar verificación y mantenimiento preventivo periódico de cableado estructurado.	A	Iniciado	Dirección de Sistemas	dic-17
	13.1.3	Segregación en redes.	Contratos de Personal - Contratos de servicios con terceros	Realizar verificación y mantenimiento preventivo periódico de cableado estructurado.	A	Iniciado	Dirección de Sistemas	dic-17
	13,2	Transferencia de información						
	13.2.1	Políticas y procedimientos para la transferencia de información.	Aplicaciones y Software	Establecer políticas de transferencia de información al interior de la Administración Municipal.	A	Iniciado	Dirección de Sistemas	jun-17
	13.2.2	Acuerdos en la transferencia de información.	Aplicaciones y Software	Establecer políticas de transferencia de información al interior de la Administración Municipal.	A	Iniciado	Dirección de Sistemas	jun-17
	13.2.3	Mensajería electrónica.	Aplicaciones y Software	Establecer políticas de uso del correo electrónico institucional.	A	Iniciado	Dirección de Sistemas	jun-17
	13.2.4	Acuerdos de confidencialidad o no-revelación.	Aplicaciones y Software - Contrato de Personal - Contrato de Servicios con Terceros	Establecer políticas de uso del correo electrónico institucional, acuerdos de confidencialidad en los procesos contractuales.	A	Iniciado	Dirección de Sistemas	jun-17

Tabla 45. (Continuación)

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.	Estudios contractuales previos y de conveniencia	Incluir en estudios de conveniencia previos y procesos contractuales.	A	Iniciado	Dirección Administrativa	dic-18
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas.	Aplicaciones y Software	Incluir encriptación de comunicaciones en características técnicas de aplicaciones que trabajen sobre redes públicas.	A	Iniciado	Dirección de Sistemas	dic-19
	14.1.3	Protección de transacciones en servicios de aplicación.	Aplicaciones y Software	Establecer e implementar medidas de protección de transacciones.	A	Iniciado	Dirección de Sistemas	jun-18
	14,2	Seguridad en el proceso de desarrollo y soporte						
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa.	Aplicaciones y Software	Establecer lista de chequeo para revisión de aplicaciones.	A	Iniciado	Dirección de Sistemas	dic-17
	14.2.7	Desarrollo tercerizado.	Aplicaciones y Software	Establecer lista de chequeo para revisión de aplicaciones.	A	Iniciado	Dirección de Sistemas	dic-17
	14.2.8	Pruebas de seguridad del sistema.	Aplicaciones y Software	Establecer lista de chequeo para revisión de aplicaciones.	A	Iniciado	Dirección de Sistemas	dic-17
	14.2.9	Pruebas de aceptación del sistema.	Aplicaciones y Software	Establecer lista de chequeo para revisión de aplicaciones.	A	Iniciado	Dirección de Sistemas	dic-17
	14,3	Datos de prueba						

Tabla 45. (Continuación)

	14.3.1	Protección de datos de prueba.	Aplicaciones y Software	Establecer procedimiento para el almacenamiento seguro de datos de prueba.	A	Iniciado	Dirección de Sistemas	dic-17
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.	Estudios contractuales previos y de conveniencia	Establecer e implementar política de seguridad de la información en relaciones con proveedores.	M	Iniciado	Dirección de Sistemas	jun-17
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor.	Estudios contractuales previos y de conveniencia	Establecer e implementar política de seguridad de la información en relaciones con proveedores.	M	Iniciado	Dirección de Sistemas	jun-17
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones.	Estudios contractuales previos y de conveniencia	Establecer e implementar política de seguridad de la información en relaciones con proveedores.	M	Iniciado	Dirección de Sistemas	jun-17
	15,2	Gestión de entrega de servicios de proveedor						
	15.2.1	Monitoreo y revisión de servicios del proveedor.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer lista de chequeo para revisión de servicios.	A	Iniciado	Dirección de Sistemas	jun-17

Tabla 45. (Continuación)

	15.2.2	Gestión de cambios a los servicios del proveedor.	Aplicaciones y Software - Hardware - Equipos auxiliares - Estudios contractuales previos y de conveniencia - Contrato de Servicios con Terceros	Establecer e implementar Política de seguridad de la información en las relaciones con el proveedor.	A	Iniciado	Dirección de Sistemas	jun-17
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.	Director de Sistemas - Usuarios Finales - Usuarios Externos	Establecer plan de contingencia.	A	Iniciado	Dirección de Sistemas	jun-18
	16.1.2	Reporte de eventos de seguridad de la información.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer plan de contingencia.	A	Iniciado	Dirección de Sistemas	jun-18
	16.1.3	Reporte de debilidades de seguridad de la información.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer plan de contingencia.	A	Iniciado	Dirección de Sistemas	jun-18
	16.1.4	Valoración y decisión de eventos de seguridad de la información.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer plan de contingencia.	A	Iniciado	Dirección de Sistemas	jun-18
	16.1.5	Respuesta a incidentes de seguridad de la información.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer plan de contingencia.	A	Iniciado	Dirección de Sistemas	jun-18
	16.1.6	Aprendizaje de incidentes de seguridad de la información.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer plan de contingencia.	A	Iniciado	Dirección de Sistemas	jun-18

Tabla 45. (Continuación)

	16.1.7	Colección de evidencia.	Aplicaciones y Software - Hardware - Equipos auxiliares	Establecer plan de contingencia.	A	Iniciado	Dirección de Sistemas	jun-18
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	Planeación de la continuidad de la seguridad de la información.	Director de Sistemas - Usuarios Finales - Usuarios Externos	Establecer plan de continuidad del negocio.	A	Iniciado	Dirección de Sistemas	jun-18
	17.1.2	Implementación de la continuidad de la seguridad de la información.	Director de Sistemas - Usuarios Finales - Usuarios Externos - Aplicaciones y Software - Hardware - Equipos auxiliares - Estudios previos y de conveniencia - Contratos de Personal - Contrato de Servicios con Terceros -	Establecer plan de continuidad del negocio.	A	Iniciado	Dirección de Sistemas	jun-18
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Director de Sistemas - Usuarios Finales - Usuarios Externos - Aplicaciones y Software - Hardware - Equipos auxiliares - Estudios previos y de conveniencia - Contratos de Personal - Contrato de Servicios con Terceros	Establecer plan de continuidad del negocio.	A	Iniciado	Dirección de Sistemas	jun-18

Tabla 45. (Continuación)

18 Cumplimiento	18,1	Cumplimiento con Requerimientos Legales y Contractuales						
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales.	Aplicaciones y Software - Hardware - Equipos auxiliares - Contratos de Personal - Contrato de Servicios con Terceros	Incluir normatividad, reglamentación y legislación respectiva.	A	Iniciado	Dirección Administrativa	dic-18
	18.1.2	Derechos de propiedad intelectual (IPR).	Aplicaciones y Software	Establecer verificación y seguimiento a licenciamiento de aplicaciones y software.	A	Iniciado	Dirección de Sistemas	dic-17
	18.1.3	Protección de registros.	Aplicaciones y Software	Establecer verificación y seguimiento a licenciamiento de aplicaciones y software.	A	Iniciado	Dirección de Sistemas	dic-17
	18.1.4	Privacidad y protección de información personal identificable (PIR).	Inexistente	Realizar capacitación, promoción, divulgación y aplicación de Ley 1273 de 2009.	A	Iniciado	Dirección de Sistemas	jun-18
	18,2	Revisiones de seguridad de la información						
	18.2.1	Revisión independiente de seguridad de la información.	Manual de Gestión de Calidad	Realizar auditoría externa a las políticas de SI.	A	Iniciado	Dirección Administrativa	jun-19
	18.2.2	Cumplimiento con políticas y estándares de seguridad.	Manual de Gestión de Calidad	Realizar auditoría externa a las políticas de SI.	A	Iniciado	Dirección Administrativa	jun-19
	18.2.3	Revisión del cumplimiento técnico.	Manual de Gestión de Calidad	Realizar auditoría externa a las políticas de SI.	A	Iniciado	Dirección Administrativa	jun-19

Fuente: Los autores

8.6 INFORME DE RESULTADOS OBTENIDOS DURANTE LA APLICACIÓN DE LOS INSTRUMENTOS DE ANÁLISIS Y CONTROLES PARA MITIGAR LOS RIESGOS A QUE ESTÁ EXPUESTA LA CÁMARA DE COMERCIO

El 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 se realizó con el ánimo de conocer el estado actual de la seguridad informática de la entidad, buscando fortalecer lo que se tiene actualmente y así prevenir el riego o mitigar el impacto en caso de presentarse algún incidente.

8.6.1 Metodologías Utilizadas

Para el análisis de seguridad informática se utiliza Magerit combinado con la herramienta EAR/PILAR las cuales permitieron conocer el panorama real de la seguridad informática en la Cámara de Comercio de La Dorada.

También se utiliza la norma ISO 27001:2013 la cual establece los parámetros para la implementación un SGSI (Sistema de Gestión de la Seguridad de la Información), la cual se utiliza para establecer los controles a evaluar y así encontrar los hallazgos y proponer soluciones a los mismos.

8.6.2 Hallazgos encontrados

Una vez definida la frecuencia con la que se presentan las vulnerabilidades y amenazas en la Cámara de Comercio, se procede a calcular el riesgo de cada amenaza para cada uno de los activos identificados y valorados. Posteriormente se calcula el nivel de riesgo total para cada activo, y definir el tratamiento a aplicar de acuerdo al tipo de activo y al nivel de riesgo identificado.

Cuando el nivel de riesgo es menor o igual a uno se entiende por aceptable, cuando es mayor a uno y menor o igual a dos se considera tolerable, cuando es mayor a dos y menor igual a tres se considera intolerable y mayor a 3 extremo.

Obteniendo como consolidado los siguientes resultados:

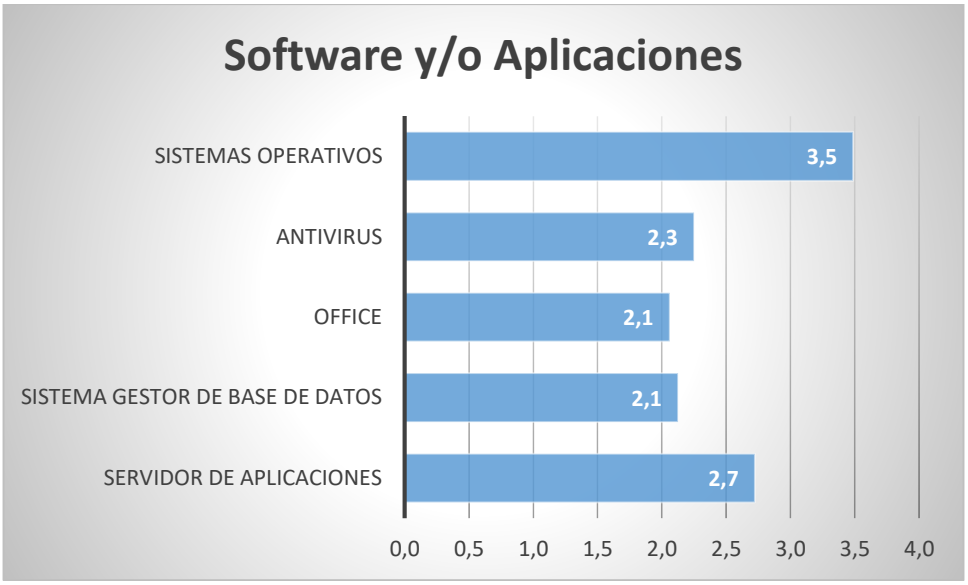
Tabla 46. Consolidado Riesgos en Software y/o Aplicaciones

Criterio Evaluado	Nivel de Riesgo
Servidor de Aplicaciones	2,7
Sistema Gestor de Base de Datos	2,1

Criterio Evaluado	Nivel de Riesgo
Office	2,1
Antivirus	2,3
Sistemas Operativos	3,5

Fuente: Los autores

Figura 6. Riesgos en Software y/o Aplicativos



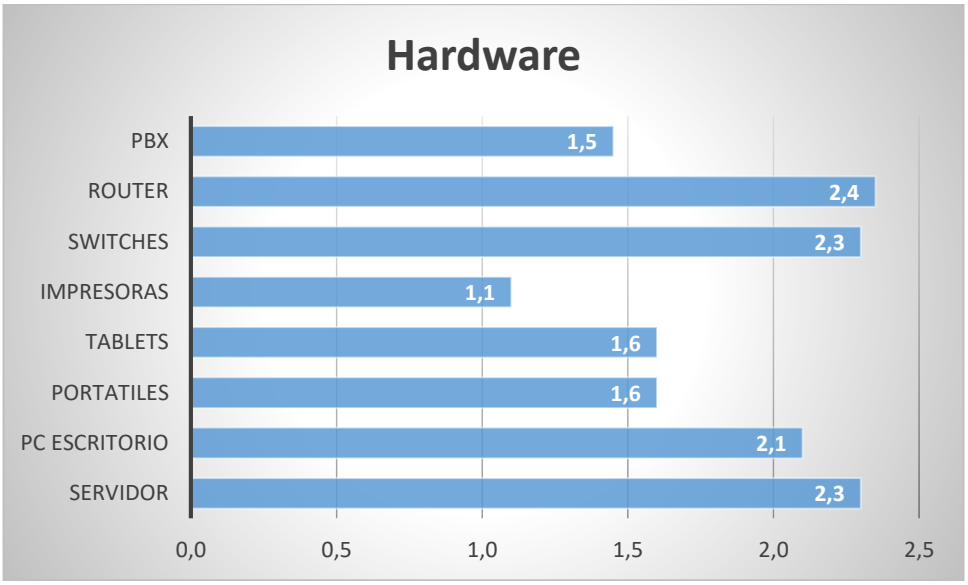
Fuente: Los autores

Tabla 47. Consolidado Riesgos en Software y/o Aplicaciones

Criterio Evaluado	Nivel de Riesgo
Servidor	2,3
PC escritorio	2,1
Portátiles	1,6
Tablets	1,6
Impresoras	1,1
Switches	2,3
Router	2,4
PBX	1,5

Fuente: Los autores

Figura 7. Riesgos en Hardware



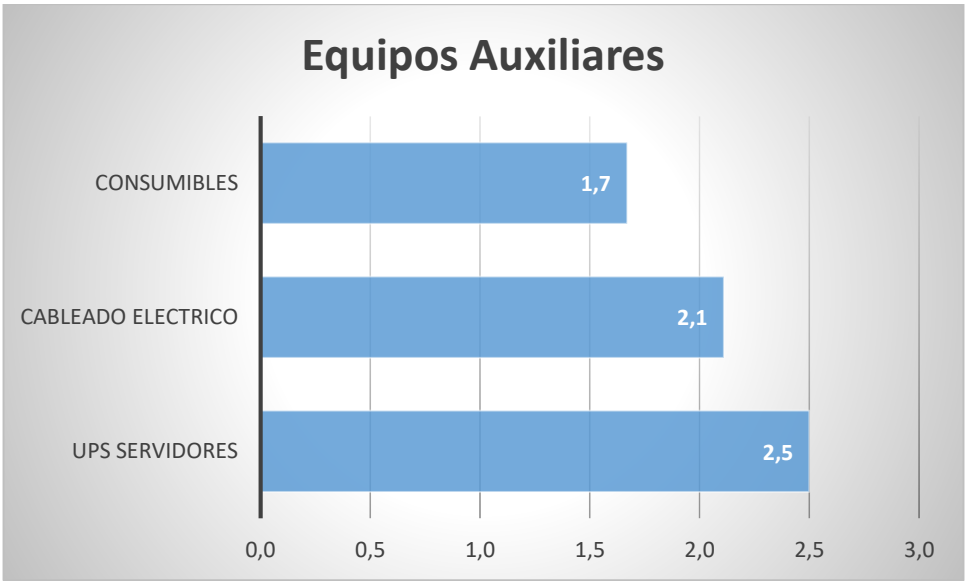
Fuente: Los autores

Tabla 48. Consolidado Riesgos en Equipos Auxiliares

Criterio Evaluado	Nivel de Riesgo
Ups Servidores	2,5
Cableado Eléctrico	2,1
Consumibles	1,7

Fuente: Los autores

Figura 8. Riesgos en Equipos Auxiliares



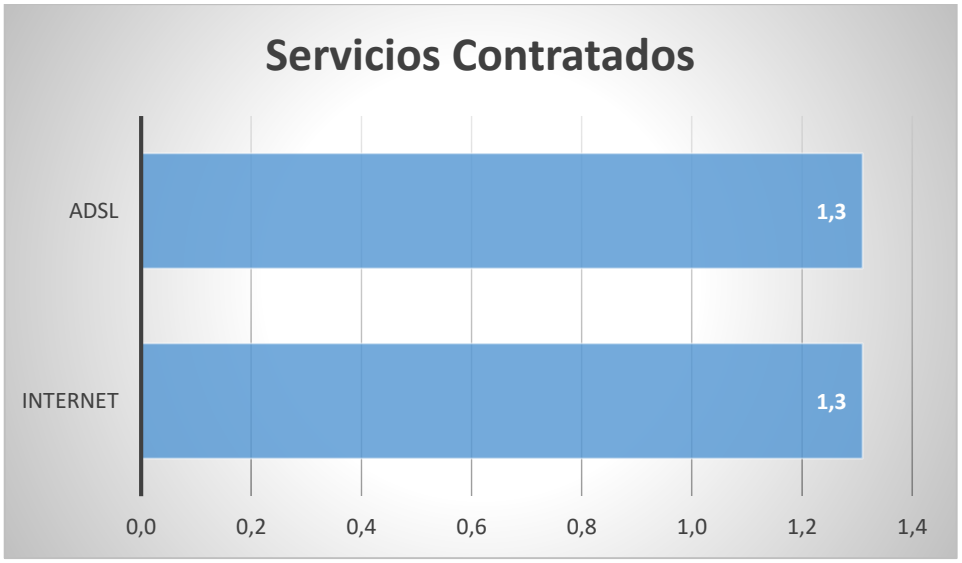
Fuente: Los autores

Tabla 49. Consolidado Riesgos en Servicios Contratados

Criterio Evaluado	Nivel de Riesgo
Internet	1,3
ADSL	1,3

Fuente: Los autores

Figura 9. Riesgos en Servicios Contratados



Fuente: Los autores

8.6.3 Tratamiento de Riesgos

Basado en los controles de seguridad según la norma ISO 27001:2013 se proponen las siguientes actividades para el tratamiento de los riesgos:

Tabla 50. Actividades para el tratamiento de riesgos según ISO 27001:2013

Políticas de Seguridad
Establecer y documentar políticas de Seguridad Informática
Organización de la Seguridad de la Información
Incluir las responsabilidades incluidas en las políticas en los contratos de los funcionarios
Establecer verificación de no duplicidad de funciones entre funcionarios
Establecer y documentar procedimientos para establecer contacto con grupos de interés y autoridades.
Incluir cláusulas de seguridad y confidencialidad en los proyectos
Establecer y documentar políticas de dispositivos móviles.
Gestión de Activos
Actualización de inventario con perfiles destinados a la gestión de activos TI por parte de la Oficina TIC
Establecer, documentar e implementar política de uso de activos TI
Establecer y documentar procedimientos para la clasificación de la información
Establecer y documentar política de uso de activos TI
Establecer, documentar e implementar política de control de acceso
Criptografía
Establecer, documentar e implementar política de controles criptográficos
Seguridad Física y del Entorno
Definir y aplicar de perímetro de seguridad físico
Establecer, documentar e implementar control de acceso a oficinas de gestión de información
Seguridad en las Comunicaciones
Establecer políticas de transferencia de información al interior de la Administración Municipal
Establecer políticas de uso del correo electrónico institucional
Establecer políticas de uso del correo electrónico institucional, acuerdos de confidencialidad en los procesos contractuales
Relaciones con Proveedores
Establecer e implementar política de seguridad de la información en relaciones con proveedores
Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio
Establecer un Plan de Continuidad del Negocio

Fuente: Los autores

Se anexa propuesta de Política de Seguridad Informática.

8.6.4 Conclusiones

Vale la pena destacar la total disposición de los funcionarios de la Cámara de Comercio, especialmente de la Presidencia Ejecutivo, quienes estuvieron atentos y colaboraron con las entrevistas y suministrando la información solicitada.

Aunque la entidad tiene algunas herramientas documentadas como la Política de Seguridad Informática, Procedimiento de Copias de Seguridad, Inventario de Activos entre otros, estos documentos deben ser adecuados y actualizados con requisitos de las diversas normas.

Una vez se realicen las actividades sugeridas, se deben socializar e iniciar con la aplicación de los nuevos instrumentos.

9 PRODUCTO RESULTADO A ENTREGAR

Como producto final del proyecto se entrega un informe final con los riesgos encontrados y sus posibles impactos, que sirve como insumo para que la Cámara de Comercio genere su Plan de Riesgos con el fin de mitigar los eventos encontrados.

10 RECURSOS NECESARIOS PARA EL DESARROLLO

10.1 RECURSOS HUMANOS

El grupo para el desarrollo del proyecto está compuesto por:

- Dos Ingenieros de Sistemas encargados del desarrollo de la investigación.
- Un funcionario de la entidad que hará las veces de facilitador.
- El Director de Sistemas de la Cámara de Comercio.

10.2 RECURSOS TECNOLÓGICOS

- Dos equipos portátiles.
- Una impresora láser a color.
- Disco duro y memorias USB.
- Suite Ofimática.
- Software para diagramas.
- Canales de Internet.

10.3 INSUMOS

- Tóner para impresora láser a color.
- Resmas de papel.
- CD y DVD.
- Marcadores.

10.4 RECURSOS LOGÍSTICOS

- Sala para reuniones, con capacidad mínima de cuatro personas, dotada con internet, video proyector, tablero acrílico y conexión a internet.

10.5 RECURSOS FINANCIEROS

Tabla 51. Recursos Financieros

DESCRIPCIÓN	VALOR
Canal de internet	600.000
Resmas de papel	32.000
Tóner para impresora	280.000
Marcadores	20.000
CD y DVD	35.000
Disco duro externo USB	180.000
Memorias USB	25.000
TOTAL	**1.172.000**

Fuente: Los autores

11 DIVULGACIÓN DEL PROYECTO

Para la divulgación del proyecto se realizan las siguientes actividades:

- Presentación y socialización al Presidente Ejecutivo y al Comité de Presidencia, en una de las reuniones que realizan periódicamente.

- Socialización al interior de la organización con el resto del personal mediante reuniones generales donde se darán a conocer tanto el resultado del análisis y evaluación de riesgos, como también la Política de Seguridad aprobada.

- Impresión de plegables con los puntos más importantes de los hallazgos.

- Envío de los documentos al correo electrónico institucional de los funcionarios.

- Publicación en la intranet de los documentos para que todos los funcionarios puedan consultarlos.

12 CONCLUSIONES

Al terminar el proyecto se logran alcanzar todos los objetivos planteados, los controles permiten mejorar los niveles de seguridad de la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas.

El análisis realizado permite conocer el estado actual de la seguridad informática en la Cámara de Comercio.

Aunque la Cámara de Comercio tiene algunos instrumentos como Política de Seguridad Informática y Política para Manejo de Copias de Seguridad, estos se deben ajustar a las normas técnicas existentes.

Una vez se cuente con los anteriores instrumentos y que estén debidamente aprobados por la Presidencia Ejecutiva, estos deben ser dados a conocer al interior de la organización.

Se deben solucionar en el menor tiempo posible las fallas de seguridad detectadas como resultado del análisis y evaluación de las mismas.

13 BIBLIOGRAFÍA

Red Seguridad.com.¿Sabes diferenciar la ISO 27001 y la ISO 27002?. Home Red Seguridad. Revista especializada en Seguridad TIC [en línea], septiembre 25 de 2016. Disponible en Internet: http://www.redseguridad.com/opinion/articulos/sabes-diferenciar-la-iso-27001-y-la-iso-27002.

VPizarro. Citas y Referencias Referencias electrónicas en normas ICONTEC. Citas y Referencias Referencias electrónicas en normas ICONTEC [en línea], noviembre 20 de 2017. Disponible en Internet: http://www.normasicontec.org/referencias-electronicas-normas-icontec/.

Gaona Vásquez Karina del Rocio. Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la Empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala. Dspace.ups.edu.ec [en línea], Julio 10 de 2016. Disponible en Internet: http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.

Howard Taylor Sandra. Decreto 2042 de 2014. Decreto_2042.pdf, [en línea], agosto 5 de 2016. Disponible en Internet: http://www.sic.gov.co/drupal/sites/default/files/normatividad/Decreto_2042_2014.pdf.

Santos Calderón Juan Manuel, Granados Guida Sergio Díaz. Decreto Reglamentario 1377 de 2013. Consulta de la norma, [en línea], agosto 5 de 2016. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646.

Centro Criptológico Nacional. EAR/PILAR. EAR – Herramientas para el Análisis de Riesgos, [en línea], septiembre 25 de 2016. Disponible en Internet: http://www.ar-tools.com/es/index.html.

Pritesh Gupta. ISO27000.es. ISO27000.es – El portal de ISO 27001 en español. Gestión de Seguridad de la Información, [en línea], septiembre 12 de 2016. Disponible en Internet: http://www.iso27000.es.

Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. Estructura Orgánica Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Calda. ORGANIGRAMA-si-cod.png (1344x717), [en línea], agosto 29 de 2016. Disponible en Internet: http://www.camaradorada.org.co/version2/wp-content/uploads/2016/02/ORGANIGRAMA-sin-cod.png

Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. Funciones y Deberes. Cámara de Comercio de La Dorada, Puerto Boyacá,

Puerto Salgar y Oriente de Caldas | Ley de Transparencia, [en línea], julio 11 de 2016. Disponible en Internet: http://www.camaradorada.org.co/transparencia#1456754723032-586984d6-dc4b.

Cámara de Comercio Internacional. Guía de Seguridad ICC para los negocios. ICC_CSG_ESP01_PR.pdf, [en línea], septiembre 23 de 2016. Disponible en Internet: http://www.camara.es/sites/default/files/publicaciones/guia_ciberseguridad_icc_esp.pdf.

Calderón Onofre Diana, Estrella Ochoa Martín, Flores Villamarín Manuel. Implementación de Sistema de Gestión de Seguridad de la Información aplicada al área de recursos humanos de la empresa DECEVALE S.A. dspace.espol.edu.ec, [en línea], septiembre 30 de 2016. Disponible en Internet: https://www.dspace.espol.edu.ec/bitstream/123456789/24204/1/1PROYECTO%20DE%20GRADUACION%20IMPLEMENTACION%20DE%20SGSI%20A%20LA%20EMPRESA.docx.

Es.ccm.net. Introducción a la Seguridad Informática. Introducción a la Seguridad Informática, [en línea], septiembre 4 de 2016. Disponible en Internet: http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica.

ISO. Standards. International Organization for Standardization, [en línea], septiembre 23 de 2016. Disponible en Internet: http://www.iso.org/iso/home/standards.htm.

Santos Calderón Juan Manuel, Correa Palacio Ruth Stella, Cárdenas Santa María Mauricio, Diaz-Granados Guida Sergio, Molano Vega Diego. Ley 1581 de 2012. Consulta de la Norma, [en línea], agosto 5 de 2016. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. Ley de Transparencia. Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas | Ley de Transparencia, [en línea], julio 11 de 2016. Disponible en Internet: http://www.camaradorada.org.co/transparencia.

Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. Manual de Calidad. . Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas | Ley de Transparencia, [en línea], julio 11 de 2016. Disponible en Internet: http://www.camaradorada.org.co/transparencia#1456782161292-d90558ab-825c.

Normas APA. Normas APA 2016 actualizadas. Normas APA 2016 (Formato APA) para la presentación de trabajos escritos, [en línea], septiembre 17 de 2016. Disponible en Internet: http://www.normasapa.com.

Cámara de Comercio de Dosquebradas. Políticas de Seguridad de la Información. POLÍTICAS-SEGURIDAD.pdf, [en línea], septiembre 3 de 2016. Disponible en Internet: http://www.camado.org.co/web/wp-content/uploads/2016/02/POLITICAS-SEGURIDAD.pdf.

DNVGL. Sistema de Gestión de Seguridad de la Información ISO 27001. ISO 27001 – Sistema de Gestión de Seguridad de la Información – Business Assurance – DNV GL, [en línea], agosto 13 de 2016. Disponible en Internet: http://www.dnvba.com/es/Certificacion/Sistemas-de-Gestion/Seguridad-de-la-Informacion/Pages/Sistema-de-Gestion-de-Seguridad-de-la-Informacion-ISO-27001.aspx.

Ferrer Jesús. Tipos de Muestreo. Metodología De La Investigación: TIPOS DE MUESTREO, [en línea], junio 15 de 2016. Disponible en Internet: http://metodologia02.blogspot.com.co/p/tipos-de-muestreo.html.

Andrade Serrano Hernán, Otero Dajud Emilio Ramón, Varón Cotrino Germán, Rodríguez Camargo Jesús Alfonso, Uribe Vélez Álvaro, Valencia Cossio Fabio. Ley 1273 de 2009. Ley-1273-2009.pdf, [en línea], agosto 5 de 2016. Disponible en Internet: http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf.

ANEXOS

ANEXO A. CARTA DE AUTORIZACIÓN PROYECTO

Cámara de Comercio
de La Dorada, Puerto Boyacá,
Puerto Salgar y Oriente de Caldas

La Dorada, Caldas, 15 de marzo de 2016

Ingenieros
JOSÉ NAYID CARDONA CASTAÑEDA y
WILIS ALBERTO SALCEDO RUIZ
La Dorada, Caldas

Ref: Autorizacion Realización Proyecto

Cordial saludo Ingenieros

En respuesta a su solicitud de autorización para la realización del Proyectos de Análisis de Riesgos Informáticos en la Cámara de Comercio de La Dorada, Puerto Boyaca, Puerto Salgar y Oriente de Caldas dentro del marco de la Especialización en Auditoría Informática que cursan en la Universidad Nacional Abierta y a Distancia, me permito informarle que ha sido autorizada su realización.

Atentamente,

JOHN JAIRO PERDOMO GONZALEZ
Director Jurídico y de Registros Públicos

ANEXO B. POLÍTICA DE SEGURIDAD INFORMÁTICA

1. OBJETIVO

Este documento formaliza el compromiso de la dirección frente a la gestión de la seguridad de la información y presenta de forma escrita a los usuarios de sistemas de información el compendio de acciones con las cuales la Cámara de Comercio establece las normas para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de la Entidad, los cuales están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos de la Entidad.

El presente documento define los lineamientos que debe seguir la Cámara de Comercio con relación a la seguridad de la Información. Estos lineamientos están escritos en forma de políticas.[8]

2. ALCANCE

El documento de Política de Seguridad de la Información reglamenta la protección y uso de los activos de información de la Cámara de Comercio, y por tanto está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos. Los usuarios de los activos de información de la Entidad deberán diligenciar un acuerdo de confidencialidad, que los compromete con el cumplimiento de las políticas de seguridad aquí descritas. Los usuarios de los activos de información de la Entidad se han clasificado así:

- **Colaboradores de Planta:** se definen como colaboradores de planta aquellas personas que han suscrito un contrato laboral con la Entidad.

- **Funcionarios de la Cámara de Comercio:** Se definen como los empleados de la Cámara de Comercio que son susceptibles de manipular sistemas de información.

- **Contratistas:** se definen como contratistas a aquellas personas que han suscrito un contrato con la Entidad y que pueden ser:

✓ Colaboradores en Misión
✓ Colaboradores por Outsourcing: son aquellas personas que laboran en la Entidad y tienen contrato con empresas de suministro de servicios y que dependen de ellos
✓ Personas naturales que prestan servicios independientes a la Entidad

[8] Cámara de Comercio de Dos Quebradas (2016). Política de Seguridad de la Información.

- ✓ Proveedores de recursos informáticos

- **Entidades de Control**

- ✓ Procuraduría
- ✓ Revisoría Fiscal
- ✓ Contraloría General de la República
- ✓ Superintendencia de Industria y Comercio

- **Otras Entidades**

- ✓ DIAN[9]

3. DEFINICIONES

Para los propósitos de este documento se aplican los siguientes términos y definiciones:

- **ACTIVO**: Cualquier bien que tenga valor para la organización.
- **ACUERDO DE CONFIDENCIALIDAD**: Es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de La Cámara de Comercio.
- **ADMINISTRADORES:** Usuarios a quienes la Cámara de Comercio ha dado la tarea de administrar los recursos informáticos y poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos de la Cámara de Comercio quienes estarán bajo la dirección de la Vicepresidencia de tecnología y soluciones de información de la Entidad.
- **AMENAZA:** Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.
- **BACKUP:** Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.
- La Dirección de Sistemas y Gestión Documental es la responsable de velar por el cumplimiento de esta Política, documentar el Manual de Seguridad de la Información, los procesos, procedimientos, instructivos y formatos específicos alineados al estándar internacional ISO 27001 y sus normas derivadas además de los otros marcos generalmente aceptados como: COBIT, ITIL, NIST, ASNZ y DRII, así como liderar la implementación de los controles exigidos por la Ley y la Regulación Vigente.

[9] Cámara de Comercio de Dos Quebradas (2016). Política de Seguridad de la Información.

- **COMITÉ DE SEGURIDAD:** Equipo de trabajo conformado por el Presidente Ejecutivo, Director de Sistemas y Gestión Documental o los funcionarios que hagan sus veces.
- **CONTRASEÑA**: Clave de acceso a un recurso informático.
- **CONTROL:** Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- **DIRECTRICES:** Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.
- **SERVICIOS DE PROCESAMIENTO DE INFORMACIÓN**: Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.
- **SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.
- **EVENTO DE SEGURIDAD DE LA INFORMACIÓN**: Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.
- **FIREWALL:** Conjunto de recursos de hardware y software que protegen recursos informáticos de accesos indebidos.
- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN**: Está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **INFORMACIÓN CONFIDENCIAL (RESERVADA):** Información administrada por La Cámara de Comercio en cumplimiento de sus deberes y funciones y que en razón de aspectos legales debe permanecer reservada y puede ser únicamente compartida con previa autorización del titular de la misma.
- **INFORMACIÓN CONFIDENCIAL (CONFIDENCIAL):** Información generada por La Cámara de Comercio en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.
- **INFORMACIÓN PRIVADA (USO INTERNO):** Información generada por La Cámara de Comercio en cumplimiento de sus deberes y funciones, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.
- **INFORMACIÓN PÚBLICA:** Es la información administrada por La Cámara de Comercio en cumplimiento de sus deberes y funciones que está a disposición del público en general; por ejemplo, la información de los registros públicos y la

información vinculada al Registro Único Empresarial y Social – RUES.

- **LAN:** Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio o una oficina).
- **LICENCIA DE SOFTWARE:** Es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación.
- **COPYRIGHT:** Son el conjunto de derechos de exclusividad con que la ley regula el uso de una particular expresión, de una idea o información. En términos más generalizados se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones de audio, pintura, escultura, fotografía, software, radio, televisión, y otras formas de expresión de una idea o concepto), sin importar el medio de soporte utilizado (Impreso, Digital), en muchos de los casos la protección involucra un periodo de duración en el tiempo. En muchos casos el copyright hace referencia directa a la protección de los derechos patrimoniales de una obra.
- **PROPIEDAD INTELECTUAL:** Es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humana, dignos de reconocimiento jurídico.
- **OPEN SOURCE** (Fuente Abierta): Es el término por el que se conoce al software que es distribuido y desarrollado de forma libre, en el cual la licencia específica el uso que se le puede dar al software.
- **SOFTWARE LIBRE:** Software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.
- **SOFTWARE PIRATA:** Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley.
- **SOFTWARE DE DOMINIO PÚBLICO:** Tipo de software en que no se requiere ningún tipo de licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales software de dominio público es aquel en el cual existe una libertad total de usufructo de la propiedad intelectual.
- **FREEWARE:** Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.
- **SHAREWARE:** Clase de software o programa, cuyo propósito es evaluar por un determinado lapso de tiempo, o con unas funciones básicas permitidas. para adquirir el software de manera completa es necesario un pago económico.
- **MÓDEM (MODULADOR - DEMODULADOR DE SEÑALES):** Elemento de comunicaciones que permite transferir información a través de líneas telefónicas.
- **MONITOREO:** Verificación de las actividades de un usuario con respecto a los recursos informáticos de La Cámara de Comercio.
- **OTP (ONE TIME PASSWORD):** Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.

- **PLAN DE CONTINGENCIA:** Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de La Cámara de Comercio en casos de desastres y otros casos que impidan el funcionamiento normal.
- **POLÍTICA:** Toda intención y directriz expresada formalmente por la dirección.
- **PROTECTOR DE PANTALLA:** Programa que se activa a voluntad del usuario, ó automáticamente después de un tiempo en el que no ha habido actividad.
- **PROXY:** Servidor que actúa como puerta de entrada a la Red Internet.
- **RECURSOS INFORMÁTICOS:** Son aquellos elementos de tecnología de Información tales como: computadores servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, elementos de comunicaciones, elementos de los sistemas de imágenes, elementos de almacenamiento de información, programas y datos.
- **RIESGO:** Combinación de la probabilidad de un evento y sus consecuencias.
- **ANÁLISIS DE RIESGOS:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- **Evaluación de Riesgos:** Todo proceso de análisis y valoración del riesgo.
- **VALORACIÓN DEL RIESGO:** Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.
- **GESTIÓN DEL RIESGO:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **ROUTER:** Equipo que permite la comunicación entre dos o más redes de computadores.
- **SESIÓN:** Conexión establecida por un usuario con un Sistema de Información.
- **Sistema de control de acceso:** Elementos de hardware o software que autorizan o niegan el acceso a los recursos informáticos de acuerdo con políticas definidas.
- **SISTEMA DE DETECCIÓN DE INTRUSOS (IDS):** Es un conjunto de hardware y software que ayuda en la detección de accesos ó intentos de acceso no autorizados a los recursos informáticos de La Cámara de Comercio.
- **SISTEMA DE ENCRIPCIÓN:** Elementos de hardware o software que permiten cifrar la información, para evitar que usuarios no autorizados tengan acceso a la misma.
- **SISTEMA MULTIUSUARIO:** Computador y su software asociado, que permiten atender múltiples usuarios a la vez a través de las redes de comunicación.
- **SISTEMA OPERATIVO:** Software que controla los recursos físicos de un computador.
- **SISTEMA SENSIBLE:** Es aquel que administra información confidencial ó de uso interno que no debe ser conocida por el público en general.
- **TERCERA PARTE:** Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.
- **USUARIO:** toda persona que pueda tener acceso a un recurso informático de La Cámara de Comercio

- **USUARIOS DE RED Y CORREO:** Usuarios a los cuales La Cámara de Comercio les entrega un identificador de cliente para acceso a sus recursos informáticos.
- **USUARIOS EXTERNOS:** Son aquellos clientes externos que utilizan los recursos informáticos de La Cámara de Comercio a través de Internet ó de otros medios y tienen acceso únicamente a información clasificada como pública.
- **USUARIOS EXTERNOS CON CONTRATO:** Usuarios externos con los cuales La Cámara de Comercio establece un contrato y a quienes se da acceso limitado a recursos informáticos de uso interno.
- **VULNERABILIDAD:** Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.[10]

4. INTRODUCCION

Con el ánimo de mejorar la estrategia de Seguridad de la información de la CAMARA DE COMERCIO DE LA DORADA, PUERTO BOYACA, PUERTO SALGAR Y ORIENTE DE CALDAS. En adelante La Cámara de Comercio, surge la necesidad de buscar un modelo base que permita alinear los procesos hacia un mismo objetivo de seguridad en el manejo de la información.

Para tal fin, se establece una Política de la Seguridad de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los recursos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

5. REQUISITOS LEGALES Y/O REGLAMENTARIOS

Para la implementación de la estrategia de seguridad de la información, la Cámara de Comercio debe regirse por lo dispuesto en el marco jurídico y normativo aplicable a las Cámaras de Comercio o entidades que las regulan y aglutinan

6. RESPONSABLE

6.1. COMPROMISO DE LA DIRECCION

La Presidencia Ejecutiva debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento

[10] Cámara de Comercio de Dos Quebradas (2016). Política de Seguridad de la Información.

y mejora de los mecanismos para asegurar información:

- Mediante el establecimiento de una política de seguridad de la información
- Asegurando que se establezcan objetivos y planes de seguridad de la información
- Estableciendo funciones y responsabilidades de la seguridad de la información
- Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y las necesidades de la mejora continua
- Asegurando que se realizan auditorías internas

6.2. GESTIÓN DE LOS RECURSOS

- Asegurar que las políticas de seguridad de la información brindan apoyo al cumplimiento de la misión y visión de La Cámara de Comercio
- Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales
- Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados
- Asegurar que todo el personal tiene conciencia de la importancia de la seguridad de la información

7. PROCEDIMIENTOS

- **Comunicación de las políticas de seguridad:** Los miembros del Comité de Seguridad, conscientes que los recursos de información son utilizados de manera permanente por los usuarios que acceden a diferentes servicios, definidos en este documento, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.

- **Aplicación de las políticas de seguridad:** Las políticas de seguridad informática se orientan a reducir el riesgo de incidentes de seguridad y minimizar su efecto. Establecen las reglas básicas con las cuales la organización debe operar sus recursos informáticos. El diseño de las políticas de seguridad informática está encaminado a disminuir y eliminar muchos factores de riesgo, principalmente la ocurrencia.

7.1. POLÍTICA DE SEGURIDAD DE LA CÁMARA DE COMERCIO

La Cámara de Comercio reconoce abiertamente la importancia de la seguridad de la información, así como la necesidad de su protección para constituir un activo estratégico de la organización y todas las partes interesadas, el no uso adecuado de los activos de información puede poner en peligro la continuidad del negocio o

al menos suponer daños muy importantes que afecten el normal funcionamiento de los procesos.

Los funcionarios, terceros y usuarios en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen según las funciones que realicen para la organización, el desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado.

Igualmente se implementarán los controles de seguridad encaminados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información de La Cámara de Comercio con el objetivo de lograr un nivel de riesgo aceptable de acuerdo con la visión, misión, planeación y estrategia de la compañía, y dando cumplimiento al marco jurídico aplicable a los estándares nacionales.

7.2. POLÍTICAS GENERALES DE SEGURIDAD INFORMÁTICA

Estas normas son de obligatorio cumplimiento por parte de todos los usuarios de recursos informáticos y se han clasificado en:

- Políticas de Cumplimiento y Sanciones
- Políticas de uso de recursos informáticos.
- Políticas de contraseñas.
- Políticas de uso de la información.
- Políticas del uso de Internet y correo electrónico.
- Políticas Generales de la Presidencia. Políticas para Desarrolladores de Software.
- Políticas para Administradores de Sistemas.
- Políticas de Copias de respaldo.
- Políticas para Usuarios previstos en el numeral tercero.
- Políticas de Acceso Físico.

7.3 POLÍTICAS DE CUMPLIMIENTO Y SANCIONES

7.3.1. Cumplimiento con la seguridad de la información

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Presidencia Ejecutiva de La Cámara de Comercio y al comité de seguridad.

7.3.2. Medidas disciplinarias por incumplimiento de políticas de seguridad

Todo incumplimiento de una política de seguridad de la información por parte de un funcionario o contratista, así como de cualquier estándar o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Si el incumplimiento se origina en alguna sede de La Cámara de Comercio, esta podrá suspender la prestación de cualquier servicio de información.

7.4. POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

7.4.1. Instrucciones para el uso de recursos informáticos

El uso de cualquier sistema de información y demás recursos informáticos por parte del empleado, trabajadores o usuarios de los sistemas de la Cámara de Comercio, debe someterse a todas las instrucciones técnicas, que imparta el comité de seguridad.

7.4.2. Uso personal de los recursos

Los recursos informáticos de La Cámara de Comercio, dispuestos para la operación, solo deben ser usados para fines laborales. El producto del uso de dichos recursos tecnológicos será de propiedad de la Entidad y estará catalogado como lo consagran las políticas de la Entidad. Cualquier otro uso está sujeto a previa autorización de la Presidencia.

7.4.3. Acuerdo de confidencialidad

- Para el uso de los recursos tecnológicos de La Cámara de Comercio, todo usuario debe firmar un acuerdo de confidencialidad y un acuerdo de Seguridad de los sistemas de información antes de que le sea otorgado su Login de acceso a la red y sus respectivos privilegios o medios de instalación.

- Prohibición de instalación de software y hardware en los computadores de La Cámara de Comercio: La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada por el Director de Sistemas y Gestion Documental.

7.4.4. Uso del aplicativo entregado.

La Cámara de Comercio ha suscrito con los fabricantes y proveedores un contrato de “LICENCIA DE USO” para los aplicativos que utiliza (Windows, Office, Kaspersky, Digiturno, WorkManager ED). Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores de la Entidad, esto

se asegura con la firma del Acuerdo de Confidencialidad para los usuarios y con la firma del contrato realizado con los proveedores que maneje información de uso restringido a La Cámara de Comercio Adicional a esto cada usuario, dependiendo de las actividades que realice sobre las aplicaciones maneja un perfil limitado, de esta forma es controlado el acceso.

7.4.5. El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados.

Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien esta le fue otorgada. Los usuarios no deben permitir que ninguna otra persona realice labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de La Cámara de Comercio.

7.4.6. Declaración de reserva de derechos de La Cámara de Comercio

La Cámara de Comercio usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información. Para mantener estos objetivos La Cámara de Comercio se reserva el derecho y la autoridad de: 1. Restringir o revocar los privilegios de cualquier usuario; 2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados; y, 3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de La Cámara de Comercio. Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad del comité de seguridad siempre con el concurso de la Presidencia o de quién él delegue esta función.

7.4.7. Todo monitoreo debe ser registrado e informado al jefe inmediato del usuario

Un usuario puede ser monitoreado bajo previa autorización del comité de seguridad.

7.4.8. Acceso no autorizado a los sistemas de información de la Entidad

Está totalmente prohibido obtener acceso a sistemas de información a los que no se tiene privilegios y de alguna forma dañar o alterar la operación de dichos sistemas. Esto implica la prohibición de capturar contraseñas, llaves de encripción y otros mecanismos de control de acceso que le puedan permitir obtener ingreso a sistemas no autorizados.

7.4.9. Posibilidad de acceso no implica permiso de uso.

Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario sin la debida autorización de este.

7.4.10. Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos

A no ser que exista una aprobación por escrito para ello o sea parte de su función laboral, los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato al comité de seguridad.

7.4.11. Manejo de sesiones en sistemas informáticos

Si el usuario está conectado a un sistema que contiene información sensible, éste no debe dejar el computador desatendido sin cerrar primero la sesión iniciada.

7.4.12. Notificación de sospecha de pérdida, divulgación ó uso indebido de información.

Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico del comité de seguridad.

7.4.13. Etiquetado y presentación de información de tipo confidencial a los usuarios de computadores

Toda la información que sea crítica para la organización debe ser etiquetada de acuerdo a los niveles establecidos en el presente documento: USO INTERNO y CONFIDENCIAL.

7.4.14. Traslado de equipos debe estar autorizado

Ningún equipo de cómputo debe ser reubicado o trasladado dentro o fuera de las instalaciones de La Cámara de Comercio sin previa autorización. Así mismo, ningún equipo de cómputo debe ser reubicado o trasladado de las instalaciones de la sede a la cual fue asignado. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal de sistemas autorizado.

7.4.15. Control de recursos informáticos entregados a los usuarios

Cuando un usuario inicie su relación laboral con La Cámara de Comercio se debe diligenciar el documento de entrega de inventario.

Cuando un empleado termine su vinculación laboral con la Entidad, sea trasladado a otra dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el formato de descargue de inventario (Firmado). El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

7.4.16. Configuración de sistema operativo de las estaciones de trabajo

Solamente el Director de Sistemas y Gestion Documental es el autorizado para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.

Queda prohibido el uso de módems en las estaciones de trabajo que permitan obtener una conexión directa a redes externas como Internet a menos que se cuente con aprobación escrita por parte de Presidencia Ejecutiva.

7.4.17. Protección por Defecto de Copyright

Todos los colaboradores de La Cámara de Comercio deben revisar, e investigar los derechos de propiedad intelectual para todo material como libros, artículos, informes, imágenes, software y/o sitio Web encontrado en Internet antes de ser usado para cualquier propósito con el fin de asegurar el cumplimiento de las leyes que aplican para este tipo de información.

Regularmente se deben realizar actividades de monitoreo sobre el software instalado en cada uno de los equipos de la organización, lo anterior para asegurar que los programas instalados correspondan correctamente con las licencias adquiridas por la empresa.

7.4.18. Custodia de Licencias de Software

Las licencias deben ser custodiadas y controladas por el área de sistemas y gestión documental. Esta área debe realizar auditorías de licencia de software como mínimo una vez al año generando las evidencias respectivas, lo anterior para garantizar que los funcionarios solo tienen instalado software legal y autorizado por el jefe de cada área.

7.4.19. Apagado de equipos en la noche

Con fin de proteger la seguridad y distribuir bien los recursos de la empresa, los equipos de cómputo deben quedar apagados cada vez que no haya presencia de funcionarios en la oficina durante la noche.

7.4.20. Tiempo limitado de conexión en aplicaciones de alto riesgo

Si el usuario está conectado a un sistema que contiene información sensible, y este presenta un tiempo de inactividad corto la aplicación deberá cerrar la sesión iniciada por el usuario.

7.5. POLÍTICAS DE USO DE LAS CONTRASEÑAS

7.5.1. Confidencialidad de las contraseñas

La contraseña que cada usuario asigna para el acceso a los sistemas de información, debe ser personal, confidencial e intransferible. Cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.

7.5.2. Uso de diferentes contraseñas para diferentes recursos informáticos

Para impedir el compromiso de múltiples recursos informáticos, cada usuario deberá utilizar diferentes contraseñas para cada recurso al que tiene acceso. Esto involucra así mismo a los equipos de comunicación (firewall, routers, servidores de control de acceso) y a los administradores de los mismos.

7.5.3. Identificación única para cada usuario

Cada usuario tendrá una identificación única en cada sistema al que tenga acceso (usuario), acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores. Esta política rige para aplicativos implementados hasta la fecha de liberación de este documento. Los funcionarios contarán con una identificación única personal y su respectiva contraseña asignada por el encargado por el área de tecnología de La Cámara de Comercio.

7.5.4. Cambios periódicos de contraseñas.

Todos los usuarios deben cambiar su contraseña por lo menos una vez cada 30 días.

7.5.5. Longitud mínima de contraseñas.

Todas las contraseñas deben tener una longitud mínima de OCHO (8) caracteres que debe cumplir con algunas de las siguientes características: Incluir combinación de números, letras mayúsculas, minúsculas y caracteres especiales. Este tamaño

debe ser validado por el sistema en el momento de generar la contraseña para impedir un tamaño menor.

7.5.6. Contraseñas fuertes

Las contraseñas no deben ser nombres propios ni palabras del diccionario, debe ser una mezcla de números, letras y caracteres especiales.

7.5.7. Prohibición de contraseñas cíclicas

No se debe generar contraseñas compuestas por una combinación fija de caracteres y una combinación variable pero predecible. Un ejemplo de este tipo de contraseñas prohibidas es “Enero-2004” que según la política “Contraseñas fuertes”, es una contraseña válida, pero al mes siguiente pasa a ser “Febrero-2004” y así sucesivamente.

7.5.8. Las contraseñas creadas por usuarios no deben ser reutilizadas

El usuario no debe generar una contraseña idéntica o sustancialmente similar a una que ya haya utilizado anteriormente. Esta política es complementada por la política “Prohibición de contraseñas cíclicas”.

7.5.9. Almacenamiento de contraseñas

Ninguna contraseña debe ser guardada de forma legible en archivos “batch”, scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Ningún usuario bajo ninguna circunstancia está autorizado para tener su contraseña en cualquier medio impreso, con excepción de lo contemplado en la política “Almacenamiento de contraseñas de administrador”.

7.5.10. Sospechas de compromiso deben forzar cambios de contraseña

Toda contraseña deberá ser cambiada de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.

7.5.11. Revelación de contraseñas prohibida.

Bajo ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean funcionarios de la Entidad. Ningún usuario deberá intentar obtener contraseñas de otros usuarios, excluyendo lo contemplado en la política “Auditoria periódica a las contraseñas de los usuarios”.

7.5.12. Bloqueo estación de trabajo

Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 3 min. Por otra parte, el escritorio del equipo de trabajo debe estar despejado y ordenado, de tal forma que la información que se encuentre en el puesto de trabajo o en la pantalla (escritorio) del equipo sea estrictamente la suficiente y necesaria para la labor desempeñada.

7.5.13. Reporte de cambio en las responsabilidades de los usuarios al Administrador del Sistema

El área Administrativa y Financiera debe reportar por medio de un correo electrónico, de manera oportuna al área de Sistemas y Gestion Documental, todos los cambios significantes en las responsabilidades de un usuario, de su estado laboral, de su ubicación dentro de la organización, con el fin de mantener el principio de seguridad de la información.

7.6. POLÍTICAS DE USO DE LA INFORMACIÓN

7.6.1. Divulgación de la información manejada por los usuarios de La Cámara de Comercio

La Cámara de Comercio podrá divulgar la información de un usuario almacenada en los sistemas de acuerdo con la autorización suscrita por él mismo, por disposición legal, por solicitud de autoridad judicial o administrativa salvo las excepciones indicadas en este documento y las disposiciones legales de protección de datos personales. Se deja claridad que la información pública proveniente de la función registral es administrada exclusivamente para los fines propios de los registros públicos de acuerdo con las normas legales y reglamentarias vigentes sobre la materia. La información proveniente de las demás funciones de la Cámara de Comercio es administrada y conservada, observando las disposiciones propias del régimen de protección de datos personales, garantizando la privacidad de la información, previamente clasificada, salvó autorización del titular de la misma para su divulgación.

7.6.2. Transferencia de datos solo a organizaciones con suficientes controles

La Cámara de Comercio puede transmitir información privada solamente a terceros que por escrito se comprometan a mantener dicha información bajo controles adecuados de protección. Se da una excepción en casos en los que la divulgación de información es forzada por la ley.

7.6.3. Registro de las compañías que reciben información privada

El personal de La Cámara de Comercio que liberó información privada a terceros debe mantener un registro de toda divulgación y este debe contener qué información fue revelada, a quién fue revelada y la fecha de divulgación.

7.6.4. Transferencia de la custodia de información de un funcionario que deja La Cámara de Comercio

Cuando un empleado se retira de La Cámara de Comercio, su jefe inmediato debe revisar tanto los archivos magnéticos, correo electrónico como documentos impresos para determinar quién se encargará de dicha información o para ejecutar los métodos para la destrucción de la información.

7.6.5. Transporte de datos sensibles en medios legibles.

Si se transporta información sensible en medios legibles por el computador (disquetes, cintas magnéticas, CD´s, memorias USB), la información deberá ser encriptada, siempre y cuando el receptor acepte el intercambio de datos cifrados. Para equipos portátiles este tipo de información es asegurada mediante una aplicación de cifrado.

7.6.6. Clasificación de la Información

- Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.
- Toda la información y los activos asociados con los servicios de procesamiento de la información deben ser “propiedad”3 de una parte designada de La Cámara de Comercio.
- Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.
- Cualquier uso de servicio de procesamiento de información debe ser autorizado por el Director de Sistemas y Gestión Documental, por lo anterior cualquier acceso a un servicio no autorizado es prohibido y de esto deben tener conocimiento todos los usuarios involucrados.

7.6.7. Eliminación Segura de la Información en Medios Informáticos

Todo medio informático reutilizable de terceros como equipos rentados, discos externos, memorias USB, etc. utilizados por La Cámara de Comercio, antes de su entrega se les realizara un proceso de borrado seguro en la información.

7.6.8. Eliminación segura de la información en medios físicos

Cualquier documento físico que haya sido considerado y clasificado de carácter

confidencial y que necesite ser destruido, debe realizarse en la respectiva máquina destruye papel o cualquier otro método seguro de destrucción aprobado por el comité de seguridad.

7.7. POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO

7.7.1. Prohibición de uso de Internet para propósitos personales.

El uso de Internet está limitado exclusivamente para propósitos laborales. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas. Esta política se complementa con la política “Instrucciones para el uso de recursos informáticos”.

7.7.2. Formalidad del correo electrónico

Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto podrá ser supervisada por el superior inmediato del empleado.

7.7.3. Preferencia por el uso del correo electrónico.

Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.

7.7.4. Uso de correo electrónico

La cuenta de correo asignada es de carácter individual por lo cual ningún empleado bajo ninguna circunstancia debe usar la cuenta de otro empleado.

7.7.5. Revisión del correo electrónico.

Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo al menos tres veces diarias. Así mismo, es su responsabilidad mantener espacio libre en el buzón.

7.7.6. Mensajes prohibidos

Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros o que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.

7.7.7. Acciones para frenar el SPAM

En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al área de Sistemas Gestión Documental

7.7.8. Todo buzón de correo debe tener un responsable

Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones de las aplicaciones.

7.7.9. Enviando software e información sensible a través de Internet.

Software e información sensible de La Cámara de Comercio que requiera ser enviado por Internet debe transmitirse con la mayor seguridad posible acordada entre las partes.

7.7.10. Intercambio de información a través de Internet.

La información interna puede ser intercambiada a través de Internet, pero exclusivamente para propósitos laborales, con la debida aprobación y usando los mecanismos de seguridad apropiados.

7.8. POLÍTICAS GENERALES DE LA PRESIDENCIA EJECUTIVA

7.8.1. Evaluación y tratamiento del riesgo

La evaluación de riesgos debe identificar, cuantificar y priorizar los riesgos frente a los criterios de aceptación del riesgo y los objetivos pertinentes para la organización. Los resultados deben guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos.

El alcance de la evaluación de riesgos puede abarcar a toda la organización, partes de la organización, un sistema individual de información, componentes específicos del sistema o servicios, cuando es factible, realista y útil.

Se debe realizar una evaluación de riesgos a los recursos informáticos de La Cámara de Comercio por lo menos una vez al año utilizando el procedimiento Interno: “Análisis de riesgos”.

7.8.2. Restricción por acceso telefónico e Internet sobre recursos tecnológicos de uso interno a clientes externos.

No se otorgarán privilegios de acceso telefónico o Internet a terceros a no ser que la necesidad de dicho acceso sea justificada y aprobada. En tal caso se deben habilitar privilegios específicos para ese usuario, con vigencia solamente del período de tiempo necesario para la actividad justificada y mediante el uso de los mecanismos de control de acceso aprobados por la Presidencia.

7.8.3. Los computadores multiusuario y sistemas de comunicación deben tener controles de acceso físico apropiados

Todos los computadores multiusuario, equipos de comunicaciones, otros equipos que contengan información sensible y el software licenciado de propiedad de la Entidad deben ubicarse en centros de cómputo con puertas cerradas y controles de acceso físico apropiados.

7.8.4. Entrenamiento compartido para labores técnicas críticas

Al menos dos personas deben tener la misma capacidad técnica para la adecuada administración de los sistemas de información críticos de La Cámara de Comercio.

7.8.5. Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias

Todo sistema o recurso informático debe tener definido un plan de contingencia para la restauración de la operación. Se debe preparar, actualizar y probar periódicamente un plan para la recuperación de desastres que permita que sistemas y computadores críticos puedan estar operativos en la eventualidad de un desastre. De igual forma se debe crear planes de respuesta a emergencia con el fin de que se pueda dar una pronta notificación de problemas y solución a los mismos en la eventualidad de emergencias informáticas. Estos planes de respuesta a emergencias pueden llevar a la formación de un equipo dedicado a esta labor. La contingencia de sistemas que se acuerdan con terceros deberá disponer de una infraestructura y de un modelo de soporte acorde a las necesidades de la Cámara de Comercio.

7.8.6. Personal competente en el Centro de Cómputo para dar pronta solución a problemas.

Con el fin de garantizar la continuidad de los sistemas de información, La Cámara de Comercio deben contar con personal técnico competente que pueda detectar problemas y buscar la solución de una forma eficiente.

7.8.7. Chequeo de virus en archivos recibidos en correo electrónico

La Cámara de Comercio debe procurar y disponer de los medios para que todos los archivos descargados de Internet sean chequeados por un software de detección de virus informático, antes de ser transferidos a los computadores de los usuarios.

7.8.8. Contacto con grupos especializados en seguridad informática

El personal involucrado con la seguridad de la información deberá tener contacto con grupos especializados o foros relacionados con la seguridad de la información. Esto con el objetivo de conocer las nuevas medidas en cuanto a seguridad de la información se van presentando.

7.9. POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS

7.9.1. Soporte para usuarios con privilegios especiales

Todos los sistemas y computadores multiusuarios deben soportar un usuario con privilegios superiores a un usuario normal con el fin de poder ejercer las correspondientes labores administrativas y por lo cual estos privilegios deben ser asignados únicamente a los administradores.

7.9.2. Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la Entidad.

Todos los privilegios sobre los recursos informáticos de La Cámara de Comercio otorgados a un usuario deben eliminarse en el momento que éste abandone la Entidad y la información almacenada queda en manos de su jefe inmediato para aplicar los procedimientos de retención o destrucción de información.

7.9.3. Cuando y como pueden asignar contraseñas los administradores

Las contraseñas iniciales otorgadas por el administrador deben servir únicamente para el primer ingreso del usuario al sistema. En ese momento el sistema debe obligar al usuario a cambiar su contraseña.

7.9.4. Límite de intentos consecutivos de ingreso al sistema

El sistema debe limitar el número de intentos consecutivos de introducir una contraseña valida. Después de tres (3) intentos el usuario debe pasar a alguno de los siguientes estados: a) ser suspendido hasta nueva reactivación por parte del administrador; b) ser temporalmente bloqueado (no menos de 5 minutos); c) ser desconectado si se trata de una conexión telefónica.

7.9.5. Cambio de contraseñas por defecto

Todas las contraseñas por defecto que incluyen equipos y sistemas nuevos deberán ser cambiadas antes de su utilización siguiendo los lineamientos de la política “Contraseñas fuertes”.

7.9.6. Cambio de contraseñas después de compromiso detectado en un sistema multiusuario

Si un sistema multiusuario utiliza contraseñas como su sistema de control de acceso principal, el administrador del sistema debe asegurarse de que todas las contraseñas del mismo sean cambiadas de forma inmediata si se conoce evidencia de que el sistema ha sido comprometido. En este caso los usuarios deben ser advertidos de cambiar su contraseña en otros sistemas en los que estuvieran utilizando la misma contraseña del sistema en cuestión.

7.9.7. Administración de los buzones de correo

Los administradores deben establecer y mantener un proceso sistemático para la creación y mantenimiento de los buzones de correo electrónico, mensualmente se realizará una revisión de control sobre cada uno de los buzones creados para determinar cuáles requieren una depuración para que no alcancen su límite de espacio asignado.

7.9.8. Brindar acceso a personal externo

El web master velará porque individuos que no sean empleados, contratistas o consultores de La Cámara de Comercio no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la Entidad a menos que exista una aprobación escrita de la Presidencia o el comité de seguridad.

7.9.9. Acceso a terceros a los sistemas de la Entidad requiere de un contrato firmado

Antes de otorgarle acceso a un tercero a los recursos tecnológicos de La Cámara de Comercio se requiere la firma de un formato, acuerdo o autorización de la Dirección de Sistemas. Es obligatoria la firma del acuerdo de confidencialidad.

7.9.10. Restricción de administración remota a través de Internet

La administración remota desde Internet no es permitida a menos que se utilicen mecanismos para encripción del canal de comunicaciones.

7.9.11. Dos usuarios requeridos para todos los administradores

Administradores de sistemas multiusuarios deben tener dos identificaciones de

usuario: una con privilegios de administración y otra con privilegios de usuario normal.

7.9.12. Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito

Sin autorización escrita por parte de la Dirección de Sistemas y Gestión Documental de la Cámara de comercio, los administradores no deben otorgarle privilegios de administración a ningún usuario.

7.9.13. Negación por defecto de privilegios de control de acceso a sistemas cuyo funcionamiento no es apropiado 1

Si un sistema de control de acceso no está funcionando adecuadamente, el administrador debe negar todo intento de acceso hasta que su operación normal se haya recuperado.

7.9.14. Remoción de software para la detección de vulnerabilidades cuando no esté en uso

Las herramientas de detección de vulnerabilidades usadas por los administradores se deben desinstalar cuando no estén operativas o implementar un mecanismo de control de acceso especial basado en contraseñas o en encripción del software como tal.

7.9.15. Manejo administrativo de seguridad para todos los componentes de la red

Los parámetros de configuración de todos los dispositivos conectados a la red de La Cámara de Comercio deben cumplir con las políticas y estándares internos de seguridad.

7.9.16. Información a capturar cuando un crimen informático o abuso es sospechado

Para suministrar evidencia para investigación, persecución y acciones disciplinarias, cierta información debe ser capturada inmediatamente cuando se sospecha un crimen informático o abuso. Esta información se deberá almacenar de forma segura en algún dispositivo fuera de línea. La información a recolectar incluye configuración actual del sistema, copias de backup y todos los archivos potencialmente involucrados.

7.9.17. Sincronización de relojes para un registro exacto de eventos en la red

Los dispositivos multiusuario conectados a la red interna de La Cámara de Comercio deben tener sus relojes sincronizados con la hora oficial.

7.9.18. Revisión regular de los registros del sistema

El área de Sistemas y Gestión Documental debe revisar regularmente los registros de cada uno de los diferentes sistemas para tomar acción oportuna sobre los eventos relevantes de seguridad informática.

7.9.19. Confidencialidad en la información relacionada con investigaciones internas

Hasta que no se hayan presentado cargos o se haya tomado alguna acción disciplinaria, toda investigación relacionada con abusos de los recursos tecnológicos o actividad criminal debe ser confidencial para mantener la reputación del empleado.

7.9.20. Información con múltiples niveles de clasificación en un mismo sistema

Si un sistema o computador maneja información con diferentes niveles de sensibilidad, los controles usados deben ser los adecuados para proteger la información más sensible.

7.9.21. Segmentación de recursos informáticos por prioridad de recuperación

Se debe establecer y usar un marco lógico para la segmentación de recursos informáticos por prioridad de recuperación. Esto hará que los sistemas más críticos sean recuperados primero. Todos los departamentos deberán usar el mismo marco para preparar los planes de contingencia a los sistemas de información.

7.9.22. Software de identificación de vulnerabilidades

Para asegurar que el equipo técnico de La Cámara de Comercio ha tomado las medidas preventivas adecuadas, a todos los sistemas conectados a Internet se les debe correr un software de identificación de vulnerabilidades por lo menos una vez al año; adicionalmente en las estaciones de trabajo se cuenta con un software de Cortafuegos y Antivirus que cuente con una consola de administración en la cual se visualizan los reportes de eventos relacionados con vulnerabilidades.

7.9.23. En dónde usar controles de acceso para sistemas informáticos

Todo computador que almacene información sensible de La Cámara de, debe tener un sistema de control de acceso para garantizar que esta información no sea modificada, borrada o divulgada.

7.9.24. Mantenimiento preventivo en computadores, sistemas de comunicación y sistemas de condiciones ambientales

Se debe realizar mantenimiento preventivo regularmente en todos los computadores y sistemas para que el riesgo de falla se mantenga en un nivel bajo.

7.9.25. Habilitación de Logs en Sistemas y Aplicaciones

Se debe habilitar la gestión de logs (archivos de transacción) en los sistemas y aplicaciones críticas de La Cámara de Comercio

7.9.26. Monitoreo de Sistemas

Se debe mantener una adecuada aplicación de monitoreo configurada que identifique el mal funcionamiento de los sistemas controlados.

7.9.27. Mantenimiento de los Sistemas

Se debe realizar periódicamente el mantenimiento en las bases de datos, antivirus, servidores de correo y servicios de La Cámara de Comercio.

7.9.28. Verificación física de equipos críticos

Se debe verificar periódicamente el estado físico de los equipos de cómputo críticos.

7.9.29. Servicios de Red

Se debe garantizar que el servicio de red utilizado por La Cámara de Comercio se encuentre disponible y operando adecuadamente, el administrador del sistema o una persona autorizada por el comité de seguridad puede efectuar escaneos de la red con la finalidad de: resolver problemas de servicio, como parte de las operaciones normales del sistema y del mantenimiento, para mejorar la seguridad de los sistemas o para investigar incidentes de seguridad.

7.9.30. Revisión de accesos de usuarios

Se debe realizar por control de auditoría la revisión de los accesos de los usuarios a las aplicaciones utilizadas, por lo menos dos veces por año.

7.10. POLÍTICAS DE COPIAS DE SEGURIDAD

7.10.1. Período de almacenamiento de registros de auditoria

Registros de aplicación que contengan eventos relevantes de seguridad deben ser almacenados por un período no menor a tres (3) meses. Durante este período los registros deben ser asegurados para evitar modificaciones y para que puedan ser vistos solo por personal autorizado. Estos registros son importantes para la corrección de errores, auditoría forense, investigaciones sobre fallas u omisiones de seguridad y demás esfuerzos relacionados.

7.10.2. Tipo de datos a los que se les debe hacer copias de seguridad y con qué frecuencia

A toda información sensible y software crítico de La Cámara de Comercio residente en los recursos informáticos, se le debe hacer backup con la frecuencia necesaria soportada por el procedimiento de copias de respaldo. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada.

7.10.3. Copias de información sensible

Se deben elaborar una copia de cada backup con el fin de minimizar el riesgo por daño del medio de almacenamiento en disco y cinta, según procedimiento de copias de respaldo.

7.11. POLÍTICAS PARA USUARIOS EXTERNOS

7.11.1. Términos y condiciones para clientes de Internet

La Cámara de Comercio asume que todos los clientes que usan Internet para establecer relación con Confecámaras o realizan operaciones con las cámaras de comercio aceptan los términos y condiciones impuestos por La Cámara de Comercio en sus términos y condiciones de uso del portal de internet, antes de realizarse cualquier transacción.

7.11.2. Acuerdos con terceros que manejan información o cualquier recurso informático de La Cámara de Comercio

Todos los acuerdos relacionados con el manejo de información o de recursos de informática de La Cámara de Comercio por parte de terceros, deben incluir una cláusula especial que involucre confidencialidad y derechos reservados. Esta cláusula debe permitirle a La Cámara de Comercio ejercer auditoría sobre los controles usados para el manejo de la información y específicamente de cómo será protegida la información de La Cámara de Comercio.

7.11.3. Definición clara de las responsabilidades de seguridad informática de terceros

Socios de negocios, proveedores, clientes y otros asociados a los negocios de La Cámara de Comercio deben tener conocimiento de sus responsabilidades relacionadas con la seguridad informática y esta responsabilidad se debe ver reflejada en los contratos con La Cámara de Comercio y verificada por la Presidencia, el responsable del manejo de estos terceros deberá realizar un acompañamiento controlado durante su estadía en las instalaciones de La Cámara de Comercio, y de esta manera podrá verificar la calidad en la entrega de los servicios contratados.

7.12. POLÍTICAS DE ACCESO FÍSICO

7.12.1. Reporte de pérdida o robo de identificación

Todo empleado debe reportar con la mayor brevedad, cualquier sospecha de pérdida o robo de carnés de identificación y tarjetas de acceso físico a las instalaciones.

7.12.2. Orden de salida para equipos electrónicos

Ningún equipo electrónico podrá salir de las instalaciones de La Cámara de Comercio sin una orden de salida otorgada por el personal adecuado o sin haber sido registrado en el momento de su ingreso.

7.12.3. Orden de salida de activos

Todos los activos que afecten la seguridad de la información de La Cámara de Comercio como medios de almacenamiento, CDs, DVDs., entre otros, y que necesiten ser retirados de la entidad, se debe realizar la autorización de salida por medio del formato de Autorización de salida de activos dispuesto para estos casos.

7.12.4. Cuando se da una terminación laboral, los privilegios de acceso a la sede de La Cámara de Comercio deben ser revocados

Cuando exista una terminación laboral, el usuario deberá devolver los objetos de acceso físico a las instalaciones (carnés, tarjetas de acceso, etc.) y a su vez todos sus privilegios de acceso deberán ser revocados enviando (funcionarios autorizados) correo electrónico al área de Sistemas (sistemas@camaradorada.org.co)

7.12.5. Ingreso de equipos de grabación y fotografías al Cuarto de servidores

Cualquier miembro de La Cámara de Comercio y/o tercero debe estar autorizado por el área de seguridad de la información para ingresar con equipos donde puedan obtener información, estos pueden ser (video cámaras, celulares, cámaras fotográficas etc.).

8. POLITICA DE USO DE PORTATILES

8.1. Protección de la información

- El antivirus siempre debe estar activo y actualizado
- No permitir que personas extrañas lo observen mientras trabaja en el equipo portátil, especialmente si esta fuera de las instalaciones de La Cámara de Comercio.
- Seguir las políticas de acceso remoto
- Toda la información que es confidencial debe ir cifrada
- Cuando el equipo deba ser devuelto a La Cámara de Comercio para reparación, mantenimiento etc. La información confidencial deberá ser borrada y respectivamente guardada en una copia de respaldo
- De la información de usuario debe generarse copia de respaldo, por solicitud del usuario al área de sistemas

8.2. Protección del equipo portátil

- No dejar el computador portátil en lugares públicos
- Cuando viaje el computador portátil no debe ir dentro de su maletero siempre debe llevarse en su mano.
- Cuando vaya en su carro este debe ir en el baúl.
- No prestar el computador portátil a familiares y/o amigos

9. ACTUALIZACIÓN, MANTENIMIENTO Y DIVULGACIONDE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Éste documento se debe revisar a intervalos planificados o cuando se produzcan cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.
El Jefe de Riesgos o la persona designada por la presidencia debe aprobar el documento, es responsable por su publicación y comunicación a todos los empleados y partes externas pertinentes. El mecanismo de notificación y divulgación de los cambios realizados a la política de seguridad de la información será mediante correo electrónico.

10. COMITÉ DE SEGURIDAD

El Comité de Seguridad de la información está conformado por un equipo de trabajo interdisciplinario encargado de garantizar una dirección clara y brindar apoyo visible a la Presidencia Ejecutiva con respecto al programa de seguridad de la información dentro de la organización.

El comité debe estar a cargo de promover la seguridad de la organización por medio de un compromiso apropiado y contar con los recursos adecuados.

Las siguientes son las principales responsabilidades a cargo del Comité de Seguridad De la información, dentro de la Entidad:

- Revisión y seguimiento al modelo de gobierno de seguridad de la información a implementar en la organización.
- Revisión y valoración de la Política de Seguridad de la Información.
- Alineación e integración de la seguridad a los objetivos del negocio
- Garantizar que la seguridad de la información forma parte integral del proceso de planeación estratégica de la organización.
- Establecer las funciones y responsabilidades específicas de seguridad de la información para toda la compañía.
- Reportar, a través de reuniones semestrales a la Presidencia Ejecutiva el estado de la seguridad y protección de la información en la compañía y la necesidad de nuevos proyectos en temas de seguridad de la información
- Establecer y respaldar los programas de concientización de la compañía en materia de seguridad y protección de la información
- Establecer, evaluar y aprobar el presupuesto designado para el tema de seguridad de la información
- Evaluar la adecuación, coordinación y la implementación de los controles de seguridad específicos para nuevos servicios o sistemas de información.
- Promover explícitamente el apoyo institucional a la seguridad de la información en toda la organización.
- Supervisar y controlar de los cambios significativos en la exposición de los activos de información a las principales amenazas.
- Revisar y seguir los incidentes de seguridad de la información
- Analizar y autorizar cualquier tipo de movimiento o traslado de equipos de misión crítica para la compañía.

Adicionalmente, el comité tiene la responsabilidad de tratar los siguientes temas (por demanda):

- Mejoras en las actividades inherentes a la Seguridad de La Cámara de Comercio y sus procesos.
- Seguimiento a la aplicación de las políticas, programas y planes adoptados para la protección de los sistemas, recursos informáticos y servidores de la Red Interna y Centro de Cómputo de La Cámara de Comercio.
- Decisiones de carácter preventivo y proactivo que apunten a la

optimización de la seguridad de los procesos y sus procedimientos. Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la presente política de La Cámara de Comercio El Presidente Ejecutivo Convoca al comité de seguridad con el propósito de evaluar los cambios a la presente política y autorizar su publicación. De este comité se deja Acta como constancia de su evaluación y aprobación.

Las decisiones del comité de seguridad son protocolizadas mediante un Acta de Comité de Seguridad firmada por todos sus miembros. Las Actas de comité de seguridad podrán ser Anuladas por el comité de Seguridad mediante el uso de un Acta que invalide el contenido siempre y cuando no se haya(n) ejecutado la(s) acción(es) relacionadas.

ANEXO C. RESUMEN RAE

Título de Documento	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
Autor	CARDONA CASTAÑEDA, José Nayid SALCEDO RUIZ, Willis Alberto
Palabras Claves	• EAR/PILAR • Inventario de Activos de Información • ISO 27001 • ISO 27002 • Magerit • Riesgos
Descripción El presente proyecto de grado es una monografía cuyo fin es estructurar un sistema de control de vulnerabilidades y amenazas para la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas, con el cual se logre disminuir los riesgos a los que están expuestos diariamente.	
Fuentes Bibliográficas	Pritesh Gupta.(2012). El portal de ISO 27001 en español. Serie 27000. Recuperado de http://www.iso27000.es Gaona Vásquez Karina del Rocio. (2013). Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la Empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala (Tesis de grado). Universidad Politécnica Salesiana Sede Cuenca. Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C. (2013). Decreto Reglamentario 1377 de 2013. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646 Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. (2016). Estructura Orgánica Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Calda. Recuperado de http://www.camaradorada.org.co/version2/wp-content/uploads/2016/02/ORGANIGRAMA-sin-cod.png Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. (2016). Funciones y Deberes.

	Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas. Recuperado de http://www.camaradorada.org.co/transparencia#1456754723032-586984d6-dc4b

Contenido:

a) Descripción del problema:

En la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas, se cuenta con personal idóneo en sus funciones, sin embargo, esta misma condición hace que los funcionarios intenten por su propia cuenta solucionar las incidencias que se presentan, sin reportarlas a los funcionarios que realmente son los indicados para realizar los procesos de solución, los cuales deberían ser documentados de forma correcta, para determinar a futuro cual es la razón por la cual se está presentando la incidencia y tomar los correctivos necesarios.

Dentro de los problemas presentados, se pueden destacar los siguientes:

- Intentos de accesos no autorizados a los servidores ya que el nivel de protección con que se cuenta, no brinda la suficiente protección.
- Continuos bloqueos de los enrutadores inalámbricos y ha sido necesario configurarlos nuevamente o al menos reiniciarlos.
- Falta de una política institucional para el manejo de contraseñas para redes inalámbricas, ya que estas permanecen sin cambio durante mucho tiempo o sea que cambian de acuerdo al parecer del personal encargado del área técnica.
- La gran mayoría de funcionarios tiene sus propias memorias USB y estas son conectadas sin ningún tipo de protección en los equipos de la institución.
- En general faltan políticas claras en cuanto al manejo de la infraestructura tecnológica de la Cámara de Comercio.

b) Objetivo General.

Disminuir las vulnerabilidades y amenazas de seguridad informática a través de un sistema de control que incluya políticas y procedimientos de acuerdo a los resultados del análisis y evaluación de riesgos en la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas.

c) Objetivos Específicos.

- Recopilar información para conocer la situación actual de la Cámara de

Comercio, para determinar los riesgos de seguridad.

- Determinar los activos informáticos con que cuenta la Cámara de Comercio y que son usados para el manejo de la información.
- Realizar el proceso de análisis y evaluación de los riesgos a que está expuesta la organización debido a las vulnerabilidades y amenazas existentes usando la metodología MAGERIT de gestión de riesgo informático.
- Presentar informe detallado de resultados obtenidos durante la aplicación de los instrumentos de análisis y determinar los controles para mitigar los riesgos a que está expuesta la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas.

d) Resumen de lo desarrollado en el proyecto.

La seguridad es un proceso de mejora continua y de constante adaptación a los cambios en las organizaciones, en especial la seguridad de la información que se desarrolla atendiendo a tres dimensiones principales, las cuales son, confidencialidad que hace referencia a garantizar el acceso a la información por parte de usuarios autorizados, integridad que es la preservación de la información de forma completa y exacta y por último la disponibilidad que hace referencia a la garantía de acceso a la información en el momento que los usuarios la requieran. El proyecto se encaminó en la estructuración de un sistema de control de vulnerabilidades y amenazas para la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas.

Debido a su crecimiento y la normatividad contemplada en la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013, Decreto 2042 de 2014 y al Código de Comercio, la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas, debe implementar sus Políticas de Seguridad Informática, y actualmente se carece de estas, se tienen un documento con algunas políticas, pero estas se quedan cortas ya que solo consideran aspectos muy básicos relativos a la seguridad de la información, el único inventario con que se cuenta es el que manejan en el área contable, el cual nada tiene que ver un inventario de activos de información.

El proyecto inició con la visita a las instalaciones de la Cámara de Comercio de La Dorada, en dicha visita se realizó un recorrido por las instalaciones para observar el funcionamiento de las diferentes áreas y sobre todo poder evidenciar en que espacios eran atendidos los clientes que buscan cualquier trámite o servicio en la Cámara de Comercio, en cada área que visitamos fueron presentados cada uno de los funcionarios encargados del área, posterior al recorrido se realizó una reunión con los directivos de la organización, donde se estableció el cronograma de trabajo y en el cual se estipuló espacios para entrevistar de forma individual a los empleados, de la misma forma se solicitó toda

la información disponible de la organización con el fin de evidenciar la situación actual de la Cámara de Comercio.

La información facilitada fue:

- Estructura organizacional de la Cámara de Comercio.
- La Misión.
- La Visión.
- Las funciones de la Cámara de Comercio.
- Políticas de seguridad.
- Manual de funciones y perfiles del personal de la Cámara de Comercio.
- Documento de manejo copias de seguridad.
- Formato hoja de vida de equipos.

En el desarrollo del proyecto, se logró apreciar las vulnerabilidades y amenazas que presenta la organización, producto de la aplicación de las diferentes etapas de la metodología para el análisis de riesgos Magerit.

Se realizó un inventario de activos de información, se determinan las amenazas y vulnerabilidades a que está expuesta la organización, aplicando Magerit V3, luego se realiza el análisis y evaluación de los riesgos, se verifica también la existencia de controles de acuerdo a las normas ISO 27001:2013 e ISO 27002:2013 y de acuerdo a los resultados obtenidos se realiza el documento entregable con los hallazgos y controles a implementar.

Metodología

El tipo de investigación a realizar es cuantitativo, ya que mediante ella se pretende realizar un análisis de riesgos y así detectar las vulnerabilidades y amenazas a los cuales está expuesta la infraestructura tecnológica de la Cámara de Comercio.

La investigación es fáctica ya que para cumplir con los objetivos propuestos se basa en la experiencia propia para la recolección y análisis de información, así como los criterios adquiridos previamente en el desarrollo de la Especialización en Seguridad Informática.

Conclusiones

El proyecto se desarrolló con el fin de realizar 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.

Aunque la Cámara de Comercio tiene algunos instrumentos como Política de Seguridad Informática y Política para Manejo de Copias de Seguridad, estos se deben ajustar a las normas técnicas existentes.

Una vez se cuente con los anteriores instrumentos y que estén debidamente aprobados por la Presidencia Ejecutiva, estos deben ser dados a conocer al interior de la organización.

Se deben solucionar en el menor tiempo posible las fallas de seguridad detectadas como resultado del análisis y evaluación de las mismas.

Recomendaciones.

- Ajustar a la normatividad vigente la Política de Seguridad Informática y la Política para Manejo de Copias de Seguridad.
- Cuando se ajuste y aprueben los diferentes documentos de políticas internas, se debe realizar suficiente divulgación y promoción.
- Dar solución inmediata a las fallas de seguridad encontradas luego de realizado el análisis.