RESUMEN - TESIS DE GRADO

AUTORES	**ALEXANDER MENESES MARTINEZ** **ERNEY ALBERTO RAMIREZ CAMARGO** **MARIA ALEJANDRA MERCHAN VILLALBA** **YADITZA SUAREZ DE LA CRUZ**
FACULTAD	**DE INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION EN AUDITORIA DE SISTEMAS**
DIRECTOR	**Especialista YESICA MARIA PEREZ PEREZ**
TÍTULO DE LA TESIS	**DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI BASADO EN EL ESTÁNDAR ISO 27001, PARA LOS PROCESOS SOPORTADOS POR EL AREA DE SISTEMAS EN LA CÁMARA DE COMERCIO DE AGUACHICA, CESAR.**

RESUMEN
(70 palabras aproximadamente)

EL OBJETIVO PRINCIPAL DE ESTE PROYECTO CONSISTE EN LA ELABORACIÓN DEL DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS QUE SON SOPORTADOS POR EL ÁREA DE SISTEMAS DE LA CÁMARA DE COMERCIO DE AGUACHICA, CESAR, BASADO EN LA NORMA INTERNACIONAL ISO/IEC 27001: 2013, EN DONDE SEGUIMOS EL CICLO PHVA, LLEGANDO SOLO A LA FASE DEL PLAN, EN DONDE IDENTIFICAMOS LOS ACTIVOS, SALVAGUARDAS Y PLANTEAMOS LAS POLÍTICAS DE SEGURIDAD PERTINENTES PARA LA ENTIDAD

CARACTERÍSTICAS

PÁGINAS: 299	PLANOS:	ILUSTRACIONES: 4	CD-ROM: 1

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI BASADO EN EL ESTÁNDAR ISO 27001, PARA LOS PROCESOS SOPORTADOS POR EL AREA DE SISTEMAS EN LA CÁMARA DE COMERCIO DE AGUACHICA, CESAR.

ALEXANDER MENESES MARTINEZ

ERNEY ALBERTO RAMIREZ CAMARGO

MARIA ALEJANDRA MERCHAN VILLALBA

YADITZA SUAREZ DE LA CRUZ

Proyecto final presentado como requisito para optar el título de especialista en auditoría de sistemas.

Director

Especialista YESICA MARIA PEREZ PEREZ

Ingeniera de sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

ESPECIALIZACION EN AUDITORIA DE SISTEMAS

Ocaña, Colombia **Octubre 2016**

Índice

Lista de tablas

Lista de figuras

Lista de apéndices

Resumen

El objetivo principal de este proyecto consiste en la elaboración del Diseño del Sistema de Gestión de Seguridad de la Información para los procesos que son soportados por el Área de Sistemas de la Cámara de Comercio de Aguachica, Cesar, basado en la norma internacional ISO/IEC 27001: 2013, en donde seguimos el ciclo PHVA, llegando solo a la fase del Plan, en donde identificamos los activos, salvaguardas y planteamos las políticas de seguridad pertinentes para la entidad, el motivo que inspiro el mismo es determinado por el valor que representa la información para la cámara de comercio, y el análisis de resultados determinando las deficiencias en las buenas practicas por parte del personal encargado de la seguridad de la información y demás funcionarios.

Partiendo del análisis realizado a la información que se recolecto, aplicado a los funcionarios, se determinó que existen falencias; se ha determinado que no existen políticas actualizadas, que los empleados desconocen de buenas prácticas y que a la información no se le están garantizando las características básicas de la seguridad como son Disponibilidad, Confidencialidad e Integridad. Seguido de lo descrito anteriormente se realizó el análisis de riesgos, basados en la metodología Magerit V3, en donde se identificaron los activos de acuerdo a la clasificación sugerida por la misma, se realizó caracterización de amenazas y salvaguardas y finalmente se estimó el impacto potencial y riesgo potencial que cada amenaza conlleva al sistema.

Como fase final y pilar de este proyecto se realiza las Políticas de Seguridad de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los

recursos tecnológicos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

Introducción

La información es el activo más importante dentro de una organización, la seguridad de la información está compuesta por un conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar las características principales de la misma como lo son: la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y no repudio, en un sistema de información; implementar políticas de seguridad de los datos se ha convertido en una necesidad para que las organizaciones salvaguarden su información de cualquier tipo de ataque, daño o perdida de la misma.

En la actualidad existen normas que garantizan el uso adecuado que se le debe dar a la información, los cuales acreditan a las Organizaciones en cuanto al manejo de la misma, ISO 27001 es un estándar en el que se encuentran enmarcados una serie de procedimientos, que establece las pautas para la implementación de los Sistemas de Gestión de Seguridad de la Información SGSI) dentro una Organización y para el tratamiento del riesgo existe metodologías para gestionarlo entre ellos cabe mencionar MAGERIT.

Para diseñar el SGSI, ISO 27001, en su versión más reciente lanzada en el año 2013, enmarca 14 dominios y 113 controles, los cuales se deben de tener en cuenta para el Sistema de Gestión; utilizando como metodología el ciclo PHVA (Planear, Hacer, Verificar y Actuar). Para la Cámara de Comercio de Aguachica Cesar, se realizó el diseño del Sistema de Gestión de Seguridad de la Información, en el cual se estableció; el diagnostico de vulnerabilidades de la institución mediante una metodología de análisis de riesgo en donde se evidencio las

vulnerabilidades a las que está expuesta actualmente, que dio paso al diseño de la Política de seguridad de la información, en donde se enmarcan los controles y requerimiento para el desarrollo del sistema de gestión de seguridad de la información.

Lo que le permite a la Cámara de Comercio de Aguachica Cesar, identificar claramente sus activos, amenazas y salvaguardar para poder en un mediano plazo aspirar a la implementación del SGSI, en mirar de poder lograr la certificación por calidad en procesos de seguridad de la información, la cual expide la Organización Internacional de Estandarización ISO.

Capítulo 1. Diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, para los procesos soportados por el área de sistemas en la cámara de comercio de Aguachica, Cesar.

1.1 Planteamiento del problema

Hoy por hoy, las organizaciones sin importar su razón social están en manos de sus sistemas de información, infraestructuras tecnológicas y procesos automatizados, esto debido al incremento procedente de la utilización de nuevas tecnologías, que proporcionan y facilitan una adecuada gestión de la información producida por dichas organizaciones, esto les permite ser competentes en un mercado creciente y evolutivo tecnológicamente hablando.

Al interior de la Cámara de comercio de la ciudad de Aguachica, cesar se analiza que los procesos ejecutados podrían realizarse fundamentados en una norma o estándar de calidad nacional e internacional que los acredite en materia de políticas y controles de seguridad de la información. Los procedimientos efectuados en las diferentes estancias de la institución deberían ser contextualizados bajo el rigor de un esquema específico que supla las parquedades presentes en el tópico seguridad de la información. Lo que origina que la entidad y sus sistemas de información sean vulnerables a una serie de amenazas que pueden someter los activos críticos de información a muchas formas de delitos comunes e informáticos, lo que se cristianiza como un riesgo potencial inminente para este activo imprescindible, así como para la eficiente labor de la empresa.

1.2 Formulación del problema

¿Con el diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, para los Procesos Soportados por el Área de Sistemas en la Cámara de Comercio de Aguachica, Cesar, se planteará un SGSI y así mismo los principios fundamentales de la seguridad de la información?

1.3 Objetivos

General. Diseñar el Sistema de Gestión de Seguridad de la Información basado en el estándar ISO 27001, para los Procesos Soportados por el Área de Sistemas en la Cámara de Comercio de Aguachica, Cesar.

Específicos. Identificar cuál es el estado actual de la seguridad de la información para los Procesos Soportados por el Área de Sistemas en la Cámara de Comercio de Aguachica, Cesar.

Analizar los riesgos asociados al uso de las Tecnologías de la Información y la comunicación a partir de metodologías para la identificación, análisis y evaluación de amenazas, vulnerabilidades e impactos.

Definir el alcance y las Políticas del Sistema de Gestión de Seguridad de la información (SGSI) para los Procesos Soportados por el Área de Sistemas en la Cámara de Comercio de Aguachica, Cesar.

1.4 Justificación

El activo vital de toda empresa, sin importar su razón social, es la información; garantizar su integridad, disponibilidad, confidencialidad y autenticidad para el buen funcionamiento de la misma es de vital importancia; en la actualidad esto se ha convertido en una necesidad para que las organizaciones cada vez sean más competitivas puedan lograr el éxito y mantenerse en el mercado.

Debido a la proyección de crecimiento que tiene la Cámara de comercio de Aguachica y teniendo en cuenta todos los procesos que se manejan allí relacionados con información y de manera particular el proceso de apoyo (Sistemas, Compras Infraestructura), en donde el Área de Sistemas soporta todos los procesos misionales, se hace necesario realizar el diseño del sistema de gestión de seguridad de la información (SGSI) basado en el estándar ISO 27001 enmarcando una política de seguridad de la información e identificando, analizando y evaluando riesgos potenciales a los que está expuesta actualmente la información tales como pérdida total o parcial de los datos; alteración de dichos datos, sabotaje a los sistemas de información que actualmente posee el Área de Sistemas de la Cámara de comercio Aguachica.

La superintendencia de Industria y Comercio ejerce control sobre todas las Cámaras de Comercio en Colombia, en cualquier momento pueden hacer observaciones pertinentes referente a varios aspectos entre ellos, del manejo que se le da a los datos personales de los usuarios, para ello la superintendencia debe garantizar el pleno y efectivo ejercicio de los derechos del el hábeas data (ley 1266 de 2008) y la ley 1581 de 2012, con respecto a los datos personales. Dentro de las exigencias esta:

- Literal a) del artículo 5 de la ley 1266 de 2008 "Entidades que administren bases de datos deben tomar todas las medidas de seguridad razonables para garantizar que la información personal contenida en ellas, sea suministrada, únicamente, a los titulares, a las personas debidamente autorizadas por éstos o a sus causahabientes."

- numeral 4 del artículo 7 de la Ley 1266 de 2008 "los operadores de información deben remitir a la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio una copia del Manual de políticas y procedimientos que hayan adoptado"

- Literal g) del artículo 4 de la ley 1581 de 2012 "La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"

Por lo anterior expuesto la Cámara de Comercio de Aguachica no puede ser ajena a las exigencias que demanda el ente de control, debe estar a la vanguardia y garantizar las características de la seguridad de la información por ley. (PERSONALES).

Es de ahí donde surge la necesidad de diseñar el Sistema de Gestión de seguridad de la información (SGSI) para esta esta organización, que le garantizara en gran medida poder mejorar el proceso de Sistemas y por ende todos los procesos concernientes con la información debido a que esta área soporta los procesos misionales tales como: Registro Públicos, Promoción y Desarrollo Empresarial y Arbitraje y Conciliación; los cuales manejan información de carácter público y privado que debe ser salvaguardada

Permitiéndole así darle un óptimo tratamiento a la información que se maneja dentro de esta entidad, este propósito se llevara a cabo basándose en este estándar internacional (ISO 27001) el cual está regido por principios acreditados de calidad a nivel mundial, con el objetivo de proporcionar un marco de referencia para Gestionar la Seguridad de la Información.

El estudio se realizará con el objetivo de que los Procesos Soportados por el Área de Sistemas en la Cámara de Comercio de Aguachica, tenga estandarizado el manejo de la seguridad de la información y por ende los procesos propios que ahí se manejan, para que dichas actividades se realicen de forma apropiada proporcionando organización, confiabilidad e información veraz y oportuna.

1.5 Delimitación

1.5.1 Conceptual. La presente investigación tendrá en cuenta los siguientes términos: acción correctiva, acción preventiva, activo, alcance, amenaza, análisis de riesgos, autenticación, confidencialidad, control, disponibilidad, evaluación de riesgos, gestión de riesgos, incidente, integridad, ISO, ISO 27001, ISO 27002, PDCA, política de seguridad, riesgo, riesgo residual, seguridad de la información, selección de controles, SGSI, tratamiento de riesgos, vulnerabilidad.

1.5.2 Temporal. El desarrollo del proyecto de investigación tendrá una duración de 6 meses una vez sea aprobado el anteproyecto.

1.5.3 Espacial. El proyecto se llevará a cabo en la Cámara de comercio de Aguachica, ubicada en la Carrera 14 Numero 6-74 en la Cuidad de Aguachica en el sur del departamento del Cesar.

1.5.4 Geográfica. Aguachica está ubicada al sur del departamento del Cesar, a los 8º 18’ 45” de latitud norte y 73º 37´37” de longitud oeste del meridiano de Greenwich, entre la cordillera oriental y el valle del río Magdalena, a una distancia de 301 kilómetro de Valledupar, la capital del Cesar. Su extensión territorial es de 876.26 kilómetros cuadrados que ocupa el 3,8% de la superficie del departamento. Limita por el norte con el municipio de La Gloria (Cesar), El Carmen (Norte Santander), por el este con Rio de Oro (Cesar), por el sur con San Martín (Cesar) y Puerto Wilches (Santander), por el oeste con Gamarra (Cesar) y Morales

(Bolívar).

El territorio de Aguachica tiene una zona montañosa al norte, representadas por las estibaciones noroccidentales de la cordillera oriental con elevaciones entre los 200 y 2.150 metros sobre el nivel del mar (msnm); al sur una zona de planicie o llanura regada por los ríos Lebrija y Magdalena y sus numerosas quebradas y arroyos hoy disminuidos drásticamente por la deforestación, su fisiografía oscila entre los 50 y los 200 msnm. Presenta un clima con temperatura promedio de 28 ºC y precipitación media anual de 1.835 mm, con dos periodos de lluvias al año.

Capítulo 2. Marco referencial

2.1 Marco histórico

Desde la antigüedad, la información ha estado siempre presente. El ser humano ha llevado datos importantes como bienes y propiedades por medio de registros escritos, logrando así mantener de una u otra forma el control de sus pertenencias y tomar decisiones de acuerdo a dicha información para obtener beneficios.

Si se compara lo anterior con el mundo actual aún se mantiene esa idea pero la cantidad de información que se genera en el mundo contemporáneo es extremadamente grande, en donde nace la necesidad de administrar de forma segura y eficiente la información.

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (Britih Standards Institution) es responsable de la publicación de importantes normas como:

- 1979 Publicación BS 5750 - ahora ISO 9001
- 1992 Publicación BS 7750 - ahora ISO 14001
- 1996Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se Publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

A continuación se hace referencia a los trabajos de investigación que son afines a la investigación tratada, aquí se realizan comparativos para analizar similitudes y diferencias que existan entre las investigaciones con el fin de estudiar los contenidos que tratan cada una de ellas.

Internacional. Título: PROYECTO AMPARO (FORTALECIMIENTO DE LA CAPACIDAD REGIONAL DE ATENCIÓN DE INCIDENTES DE SEGURIDAD EN

AMÉRICA LATINA Y EL CARIBE).

Autor (es): LACNIC con el apoyo de IDRC (centro de investigaciones para el desarrollo internacional) de Canadá

Autores del "Manual de Gestión de Incidentes de Seguridad Informática"

Ing. Rubén Aquino Luna, MEXICO

Ing. José Luis Chávez Cortez, GUATEMALA

Ing. Leonardo Vidal, URUGUAY

Ing. Lorena Ferreyro, ARGENTINA

Ec. Araí Alvez Bou, URUGUAY

Msc. Ing. Eduardo Carozo, URUGUAY

Autores de los "Talleres de Gestión de Incidentes"

Ing. Gastón Franco, ARGENTINA

Ing. Carlos Martínez, URUGUAY

Ing. Alejandro Hevia, CHILE

Ing. Felipe Troncoso, CHILE

Dr. Jeimy Cano, COLOMBIA

Ing. Andres Almanza, COLOMBIA

Integrantes del Steering Committe del Proyecto AMPARO

Dr. Ing. Cristine Hoeppers, BRASIL

Ing. Patricia Prandini, ARGENTINA

Ing. Indira Moreno, MEXICO

Ing. José Luis Chávez Cortez, GUATEMALA

Dr. Ing. Alejandro Hevia, CHILE

Ing. Pablo Carretino, ARGENTINA

Dr. Jeimy Cano, COLOMBIA

Institución: LACNIC (Registros de direcciones de internet para américa latina y caribe).

Fecha: 2009 – 2010

Institución: LACNIC (Registros de direcciones de internet para américa latina y caribe).

Fecha: 2009 – 2010

Resumen: éste manual ha sido desarrollado en el marco de las actividades del Proyecto AMPARO, una iniciativa de LACNIC con el apoyo de IDRC de Canadá. El proceso de creación del mismo ha implicado un gran esfuerzo por parte de un equipo de expertos en el manejo de incidentes de seguridad, académicos de diversos países de la región, de alto reconocimiento nacional e internacional y personal de LACNIC, e IDRC. (AMPARO)

Este es un proyecto donde se analizan todos los incidentes que ocurren en cuanto a seguridad de la información se refiere, el estudio está realizado a América latina la cual tiene un gran índice de incidentes en cuanto a violación de la seguridad de la información se refiere. Este proyecto trata todos estos factores que inciden a que la información se vea expuesta a una serie de amenazas y como tomar acciones preventivas para mitigar estos riesgos.

Título: TENDENCIAS EN LA SEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA Y EL CARIBE Y RESPUESTAS DE LOS GOBIERNOS.

Autor (es): ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

Institución: ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

Fecha: 07/04/2013

Resumen. En un mundo interconectado, es necesario buscar un equilibrio entre disfrutar la comodidad que ofrecen las tecnologías de la información y minimizar las oportunidades que su uso les ofrece a los delincuentes cibernéticos, quienes pueden, por ejemplo, difundir amenazas complejas explotando los populares dispositivos móviles y las aplicaciones en la nube para infiltrarse en blancos de alto valor y han convertido el espacio cibernético en un medio para victimizar al público. (AMERICANOS, 2013)

Nacional:

Título: GUÍA DE BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN EN CONTEXTOS DE MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS DE LA REGIÓN.

Autor (es): GERARDO AYALA GONZÁLEZ, JULIÁN ALBERTO GÓMEZ ISAZA.

Institución: UNIVERSIDAD TECNOLÓGICA DE PEREIRA.

Fecha: 03/02/2011.

Resumen: Este documento se centra en la aplicación de la norma ISO/IEC 27001 en atención a los numerales 4.2.2 Implementación y Operación de un Sistema de Gestión de la Seguridad de la Información (por sus siglas, SGSI), identificando las acciones de: la gestión apropiada, prioridades y responsabilidades de la gerencia en la creación de políticas que garanticen el cumplimiento de los objetivos del SGSI, además se hace referencia a la creación

de planes de acción para el tratamiento, análisis y gestión de los riesgos implementando procedimientos que brindan una atención oportuna a los incidentes de seguridad de la información, acompañados de estrategias de capacitación y formación para los integrantes de la organización. (SEGURIDAD)

En el trabajo anterior se basa en establecer un sistema de gestión de seguridad de la información el cual está basado en el estándar ISO 27001 con el objetivo de establecer políticas de seguridad aplicando controles que permitan cumplir los objetivos de la misma.

Título: IMPLEMENTACION DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA COMUNIDAD NUESTRA SEÑORA DE GRACIA, ALINEADO TECNOLÓGICAMENTE CON LA NORMA ISO 27001.

Autor (es): FABIÁN DÍAZ ANDRÉS, COLLAZOS GLORIA ISABEL, HERMES CORTEZ LOZANO

Institución: NUESTRA SEÑORA DE GRACIA (Bogotá D.C)

Fecha: 05/08/2011

Resumen: Éste artículo es el resultado de un proyecto de investigación, adelantado por un grupo de estudiantes de ingeniería de sistemas con el fin de implementar un SGSI en la Comunidad Nuestra Señora de Gracia. Este sistema se basa en las directrices indicadas en la

norma ISO/IEC 27001, y en el marco del mismo se generó un análisis de *gap*3, que permitió evidenciar un nivel de brechas significativo en la mencionada Comunidad, con base en el cual se establecieron políticas y controles de mejoramiento de los procesos de seguridad de la información y se definieron las declaraciones de aplicabilidad que fortalecieron todo el análisis de riesgos efectuado. (FABIÁN DÍAZ ANDRÉS, 2011)

Este artículo surge como resultado de una investigación de un grupo de estudiantes el cual analiza a viabilidad de la implementación de un sistema de gestión de seguridad de la información en cual estará alienado con la norma ISO 2700.

Título: DEFINICIÓN DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA COMPUTACIÓN EN NUBES PRIVADAS Y COMUNITARIAS.

Autor (es): ANDRES FELIPE CHACÓN HURTADO JUAN FEDERICO MAYA SUDUPE

Institución: UNIVERSIDAD ICESI (Santiago de Cali - Colombia)

Fecha: Junio 21 de 2012

Resumen: En los últimos años, la computación en la nube ha tenido un incremento en su utilización. Se espera que dentro de los próximos 5 a 10 años este modelo de despliegue de servicios esté en una fase de producción, y que no sea de uso exclusivo de expertos en

tecnologías de información y comunicaciones, sino también de académicos, empresarios y personas comunes que se vean atraídos por las ventajas ofrecidas por este modelo. La seguridad de la información es uno de los aspectos que más preocupan a los directivos de TI para migrar sus aplicaciones e información a la nube, debido a que están confiando sus datos privados a un tercero. Por este motivo, las organizaciones toman medidas que garanticen el control de su información y que minimicen los riesgos que la pueden impactar, basándose en estándares de seguridad pensados para la computación tradicional. Existen iniciativas y marcos de trabajo, tales como PCI o CSA, que pueden aportar información, pero al no haber un modelo completo de seguridad para la computación en la nube, existe la posibilidad de no hacer consciencia de los diferentes riesgos, o tratarlos de forma inadecuada. (CHACÓN HURTADO ANDRES FELIPE, 2012)

Esta investigación busca darle un tratamiento diferente a la información en cual está basado en que la información este alojada en la nube, es decir, que estén situada o almacenadas en servidores distintos pero con accesos comunitarios.

Local:

Título: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE CONTABILIDAD DE LA E.S.E. HOSPITAL LOCAL DE RIO DE ORO CESAR.

Autor (es): CASADIEGOS SANTANA, AURA LUCIA QUINTERO JIMÉNEZ, MARCELA TORO RUEDA, MILEIDY

Institución: Universidad Francisco de Paula Santander Ocaña.

Fecha: 28-jul-2014

Resumen: Mediante un SGSI – sistema de gestión de seguridad de la información, el área de contabilidad de la E.S.E hospital local de rio de oro cesar conseguirá minimizar considerablemente el riesgo de que su productividad se vea afectada debido a la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad de la información o de alguno de los sistemas informáticos. Este sistema permite identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información, de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (CASADIEGOS SANTANA, 2014)

Esta investigación busca darle un tratamiento diferente a la información en la cual se basa en centralizar el diseño del SGSI, solo en los procesos contables que maneja el hospital de rio de oro, recomendando pautas para el mejoramiento de los procesos contables.

Título: ELABORACIÓN DE POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL BASADOS EN EL ESTÁNDAR INTERNACIONAL ISO/IEC 27002:2013 EN EL HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE ESE. DE LA CIUDAD DE AGUACHICA-CESAR.

Autor (es): MOSQUERA QUINTERO, GERARDO CESAR PACHECO PÉREZ, JOSÉ JULIÁN SARAVIA ALVERNIA, JORGE ARMANDO.

Institución: Universidad Francisco de Paula Santander Ocaña.

Fecha: 2-dic-2015

Resumen: el presente trabajo tiene por objetivo la creación de las políticas de seguridad física y ambiental que brinde apoyo para poder proteger la información en el hospital José David padilla Villafañe de Aguachica, para las mejores prácticas en el uso adecuado según los lineamientos del estándar internacional ISO/IEC 27002:2013, y a su vez proporcionar un plan de mejora para la optimización, brindando recomendaciones en forma sencilla y entendible, acerca de cómo mejorar los procesos par a proteger la in formación. (MOSQUERA QUINTERO, 2015)

En la presente investigación tiene como objetivo la creación de políticas físicas y ambientales, para el hospital de Aguachica José David Padilla Villafañe, en donde les pueda garantizar la conservación de la información aplicando el manual de buenas prácticas que brinda la ISO 27002 en su versión de 2013.

2.2 Marco teórico

Al abarcar contenidos teóricos a la investigación cabe resaltar las teorías en las cuales se ha enfocado a través de los años para realizar un sistema de gestión de seguridad de la

información, que se apropiado para alcanzar el éxito deseado y se adapte a las necesidades presentes en la organización que desee implantarlo.

Teoría de la información. La Teoría de la Información nos muestra, entre otras cosas, el camino a seguir para determinar la cantidad de información útil a partir de unos datos. Y para comprimir la información de manera que los datos se representen de una manera eficiente. Nace de la necesidad de optimizar los contenidos de las informaciones, en una época histórica en la que la comunicación alcanzaba un destacado papel (Shannon, 1948), esto después del nacimiento del código binario (Hartley, 1927) y los primeros pasos de encriptación (Turing, 1936). En consecuencia, se debía encontrar una forma en la cual determinar "la cantidad de información" que entregaba un mensaje.

El mayor investigador de este tema fue Claude Shannon quién aportó el concepto de que la información debe dejar de verse como inmaterial y subjetiva, sino que como perfectamente material y cuantificable. Así pasó a considerarse de una manera independiente un dispositivo de representación y se dio la posibilidad de hablar de procesos de representación y manipulación de la información sin hacer énfasis si era el cerebro o un ordenador quien realizaba dichos procesos. Esto permitió, dar el primer paso para la cibernética: el control de las máquinas para realizar tareas humanas. (TOMAS, 2014)

Definición de información: - Es el conjunto de datos o mensajes inteligibles creados con un lenguaje de representación y que debemos proteger ante las amenazas del entorno, durante su transmisión o almacenamiento, usando técnicas criptográficas entre otras herramientas. - La

teoría de la información (JORGE, 2006) mide la cantidad de información que contiene un mensaje a través del número medio de bits necesario para codificar todos los posibles mensajes con un codificador óptimo.

Seguridad de la información desde la Teoría de las Limitaciones

El eslabón más débil de la cadena. A cualquier profesional le suena: "La seguridad es como una cadena, es tan fuerte como el eslabón más débil". Esto se dice por varios motivos: Para enfatizar la naturaleza de seguridad como proceso, como sistema, pero también para entender que se trata de una posición de defensa débil, es decir, el defensor tiene que defender todos los puntos, mientras que al atacante le basta con encontrar un punto vulnerable para tener éxito en su ataque.

Sin embargo, aunque se está convencido de que esto es así, muy pocos (por no decir, ninguno) realiza la gestión de este proceso conforme a esta máxima. Porque si se gestionará la seguridad teniendo este paradigma en mente, lo mejor sería emplear la misma estrategia que cualquier otro sistema cuya producción esté gobernada por su factor limitante. Me explico, después de identificarlo, habría que hacer que este factor limitante produjese al máximo nivel.

Esta forma de gestionar la seguridad cambiaría sobremanera el enfoque actual del proceso de gestión. Si se sigue lo establecido en los estándares, por ejemplo, el estándar ISO/IEC 27001 que establece las pautas para montar un Sistema de Gestión de la Seguridad de la Información (SGSI) "certificable", tenemos que (como ya hemos comentado aquí anteriormente) llevar a cabo

un análisis de riesgos que nos permita identificar el nivel de riesgo por cada área o dominio del alcance establecido y pasar a gestionar el riesgo en función de la estrategia definida.

Si se plantea la seguridad como un sistema en el que el output fuera el nivel de seguridad de la organización (parece obvio, ¿no?), el máximo nivel estaría marcado por el máximo caudal que pudiera gestionar el cuello de botella del sistema, es decir, el nivel de seguridad de la organización sería el del eslabón más débil de la cadena.

¿Cuál es la diferencia entre estas dos maneras de gestionar la seguridad? la diferencia es que no tendría tanto interés realizar un análisis de riesgos como el hecho de encontrar cuál es el factor limitante, cuál es el eslabón más débil, puesto que sería el que marcaría el nivel de seguridad de nuestra organización. A partir de ahí, si se quiere elevar el nivel de seguridad de nuestra organización, se debería gestionar esa limitación y eso, ya se sabe, hay que preguntarle a Goldratt el cómo. (RAMOS)

Teoría de la seguridad por oscuridad Gaming. Shannon buscó la seguridad contra el atacante con poderes computacionales ilimitados: si la información transmite cierta información, a continuación, el atacante de Shannon seguramente va a extraer esa información. Diffie y Hellman refinaron el modelo atacantes de Shannon al tener en cuenta el hecho de que los atacantes reales son computacionalmente limitados. Esta idea se convirtió en uno de los grandes nuevos paradigmas en ciencias de la computación, y condujo a la criptografía moderna.

Shannon también buscó la seguridad contra el atacante con poderes lógicos y observacionales ilimitadas, expresada a través de la máxima de que "el enemigo conoce el sistema". Este punto de vista todavía es refrendado de la criptografía. La formulación popular, que se remonta a Kerckhoffs, es que "no hay seguridad por oscuridad", lo que significa que los algoritmos no se pueden mantener ocultos al atacante, y que la seguridad sólo deben confiar en las claves secretas. De hecho, la criptografía moderna va más allá de Shannon o Kerckhoffs en asumir tácitamente que si hay un algoritmo que puede romper el sistema, entonces el atacante seguramente encontrará ese algoritmo. El atacante no es visto como un equipo omnipotente más, pero él todavía se interpreta como un programador omnipotente.

Así que el paso de Diffie-Hellman de ilimitado a potencias computacionales limitados no se ha extendido a un paso de la ilimitada a los limitados poderes lógicos o de programación. Es la hipótesis de que todos los algoritmos factibles finalmente serán descubiertos y aplican realmente diferente de la suposición de que todo lo que es computable el tiempo se puede calcular. Aquí se exploran algunas maneras para refinar los modelos actuales del atacante y del defensor, teniendo en cuenta lo limitado de sus facultades lógicas y programación. Si el atacante adaptativo consulta activo el sistema para buscar a sus vulnerabilidades, el sistema puede ganar un poco de seguridad al aprender activamente los métodos del atacante, y la adaptación a ellos. (PAVLOVIC)

2.3 Marco legal

Siempre que se desea implementar un Sistema de Gestión, toda organización debe obligatoriamente cumplir con todas las leyes, normas, decretos, etc. que sean aplicables en el

desarrollo de sus actividades. De manera general se puede mencionar el tema de seguridad social, cumplir con la Cámara de Comercio, permisos, licencias de construcción, etc. pero en lo que se refiere específicamente a seguridad de la información, estas son las Leyes vigentes al día de hoy:

ISO 27001. La norma ISO 27001 fue publicada en octubre de 2005, esencialmente la sustitución de la antigua norma BS7799-2. Es la especificación para un SGSI, un Sistema de Gestión de Seguridad de la Información. Sí BS7799 era un estándar de larga data, publicado por primera vez en los años noventa como un código de prácticas. Como este maduró, una segunda parte surgió para cubrir los sistemas de gestión. Es esto en contra de la cual se concede la certificación. Hoy en día más de mil certificados están en su lugar, en todo el mundo.

En la publicación, la norma ISO 27001 mejora el contenido de la norma BS7799-2 y armonizada con otros estándares. Un esquema se ha presentado por varios organismos de certificación para la conversión de la certificación BS7799 con la certificación ISO27001.

El objetivo de la norma en sí misma es "proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI)". En cuanto a su adopción, esto debería ser una decisión estratégica. Además, "El diseño y la aplicación de la información del sistema de gestión de seguridad de una organización están influenciados por las necesidades de la organización y objetivos, requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización."

La versión 2005 de la norma en gran medida empleada del PDCA, Plan-Do-Check-Act modelo para estructurar los procesos, y reflejen los principios establecidos en las directrices OECG (ver oecd.org). Sin embargo, la versión más reciente, de 2013, pone más énfasis en la medición y evaluación de lo bien SGSI de una organización está realizando. Una sección sobre la contratación externa también se añadió con esta versión, y se prestó mayor atención al contexto de la organización de seguridad de la información. (ISO)

Certificación del Sistema de Gestión de Seguridad de la Información con ISO/IEC 27001 – ICONTEC. El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), es el Organismo Nacional de Normalización de Colombia. Entre sus labores se destaca la creación de normas técnicas y la certificación de normas de calidad para empresas y actividades profesionales. ICONTEC es el representante de la Organización Internacional para la Estandarización (ISO), en Colombia.

El estándar para la seguridad de la información ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Abarca:

- Organización de la seguridad de la información.
- Política de seguridad.
- Gestión de activos.

- Control de acceso.
- Seguridad de los recursos humanos.
- Cumplimiento.
- Seguridad física y del entorno.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Gestión de las comunicaciones y operaciones.
- Gestión de la continuidad del negocio.
- Gestión de incidentes de seguridad de la información. (ICONTEC, 2014)

Ley 23 De 1982 Sobre derechos de autor. Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y en cuanto fuere compatible con ella, por el derecho común. También protege esta Ley a los intérpretes o ejecutantes, a los productores de programas y a los organismos de radiodifusión, en sus derechos conexos a los del autor. (Ley 23 de 1982, 2014)

Ley 44 de 1993. Por la cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal.

Ley N° 44 de 1993 (5 de febrero) modifica y adiciona la Ley N° 23 de 1982 y se modifica la Ley N° 29 de 1944. Mediante la adición de disposiciones y medidas especiales para el Registro Nacional del Derecho de Autor, las sociedades de gestión colectiva de derechos de autor y derechos conexos, sanciones y otros derechos. (Ley 44 de 1993 , 2014)

El Registro Nacional del Derecho de Autor es competencia de la Unidad Administrativa Especial - Dirección Nacional del Derecho de Autor, con carácter único para todo el territorio nacional.

Ley 719 de 2001. DECRETO 1721 DE 2002 (Agosto 6) "Por el cual se reglamenta la Ley 719 de 2001, que modificó las Leyes 23 de 1982 y 44 de 1993". EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA, en ejercicio de sus facultades constitucionales, en especial las conferidas por el Artículo 189 numeral 11 de la Constitución Política de Colombia, DECRETA: Derecho exclusivo. El autor de una obra musical, o su derechohabiente, tiene el derecho exclusivo de realizar, autorizar o prohibir cualquier comunicación al público de su obra por medios alámbricos o inalámbricos, comprendida su puesta a disposición del público, de tal forma que los miembros del público puedan acceder a éstas desde el lugar y en el momento que cada uno de ellos elija. (Ley 719 de 2001, 2014)

Ley 527 De 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ambito de aplicación. La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;

b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo. (Ley 527 De 1999 , 2014)

Ley Estatutaria 1266 Del 31 De Diciembre De 2008. Decreto N° 2952 de 2010 por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008, EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. En ejercicio de sus facultades constitucionales y legales, en especial, las conferidas por el numeral 11 del artículo 189 de la Constitución Política y en desarrollo de lo previsto en los artículos 12 y 13 de la Ley 1266 de 2008.

Que el 31 de diciembre de 2008 se expidió la Ley Estatutaria N° 1266 por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. (LEY ESTATUTARIA 1266 DE 2008, 2014).

Ley 1273 Del 5 De Enero De 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". (Ley 1273 5 de enero de 2009)

El 5 de Enero de 2009 se decretó la Ley 1273 de 2009, la cual añade dos nuevos capítulos al Código Penal Colombiano: Capitulo Primero: De los atentados contra la confidencialidad, la

integridad y la disponibilidad de los datos y de los sistemas informáticos; Capitulo Segundo: De los atentados informáticos y otras infracciones.

Como se puede ver en el primer capítulo, esta Ley está muy ligada a la ISO 27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.

Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (LEY ESTATUTARIA 1581 DE 2012.)

2.4 Marco conceptual

La información hoy en día, es uno de los más importantes activos no solo para las empresas y organizaciones, si no para cada individuo. Por este motivo la misma requiere ser asegurada y protegida en forma apropiada. La Seguridad de la Información es el conjunto de metodologías, prácticas y procedimientos que buscan proteger la información como activo valioso, con el fin de minimizar las amenazas y riesgos continuos a los que está expuesta, a efectos de asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de

inversiones y las oportunidades del negocio. Y en el caso de cada individuo de proteger la identidad y la privacidad

Acción correctiva: medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

Acción preventiva: medida de tipo pro-activo orientada a prevenir potenciales no-conformidades asociadas a la implementación y operación del SGSI.

Activo: cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

Alcance: ámbito de la organización que queda sometido al SGSI. Este debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno.

Amenaza: Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o la organización.

Análisis De Riesgos: uso sistemático de la información para identificar fuentes y estimar el riesgo.

Autenticación: proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Confidencialidad: acceso a la información por parte únicamente de quienes estén autorizados. Característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: control es también utilizado como sinónimo de salvaguarda o contramedida.

Disponibilidad: acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación De Riesgos: según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Gestión De Riesgos: es un proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la

valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Incidente: según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: es el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 27001: es un estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005.

ISO 27002: es un código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio de oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007.

PDCA: Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Política De Seguridad: documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual: según [ISO/IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

Seguridad De La Información: según [ISO/IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Selección De Controles: proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información.

Tratamiento de riesgos: según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Vulnerabilidad: debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza

Capitulo 3. Diseño metodologico

3.1 Tipo de investigacion

Para el desarrollo de la investigación se acudirá a la investigación Descriptiva porque ésta busca especificar las propiedades, características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Describe tendencias de un grupo o población. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar como se relacionan éstas. (HERNANDEZ SAMPIERI, 2010)

Teniendo en cuenta que el objeto del estudio inicialmente es establecer el Diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, para los Procesos Soportados por el Área de Sistemas en la Cámara de Comercio de Aguachica, Cesar, para lograr este fin se necesita caracterizar el objeto de estudio, identificar los objetos que tienen dicha característica, describir el contexto en el cual se está desarrollando el objeto de estudio, cuantificar que tan grande es la problemática.

3.2 Población y muestra

La población está definida por los procesos que maneja el personal administrativo de la cámara de comercio de Aguachica cesar.

Considerando que la población objeto de la investigación, cuantitativamente es reducida, se trabajará con el total de la población.

3.3 Técnicas e instrumentos de recolección de datos

Para la Auditoria de Cumplimiento la recolección de la información será recopilada por medio de encuestas, observación directa, listas de chequeo, y entrevistas no estructuradas, realizadas al personal administrativo, entre los que cabe resaltar la coordinadora de sistemas y a los funcionarios de la Cámara de Comercio de Aguachica.

La encuesta la define el Prof. García Ferrado como "una investigación realizada sobre una muestra de sujetos representativa de un colectivo más amplio, utilizando procedimientos estandarizados de interrogación con intención de obtener mediciones cuantitativas de una gran variedad de características objetivas y subjetivas de la población" (ESTADISTICA, 2013).

La entrevista no estructurada siendo esta terminología definida por Natalia Jimeno Molins, donde explica el tipo de entrevista utilizada por el proyecto, en la que abre el grado de libertad de preguntas y respuestas, las preguntas no son realizadas a través de un formato rígido o específico, sino que ocurren con cierto grado de espontaneidad. (NATALIA)

Según (PUENTE, 2009) la observación directa es una técnica que consiste en observar atentamente el fenómeno, hecho o caso, sin intervención, con el fin de tomar información y registrarla para su posterior análisis. La observación es un elemento fundamental de todo proceso

investigativo; en ella se apoya el investigador para obtener el mayor número de datos. Gran parte del acervo de conocimientos que constituye la ciencia ha sido lograda mediante la observación. Observar científicamente significa observar con un objetivo claro, definido y preciso: el investigador sabe qué es lo que desea observar y para qué quiere hacerlo, lo cual implica que debe preparar cuidadosamente la observación.

La lista de chequeo, como herramienta metodológica está compuesta por una serie de ítems, factores, propiedades, aspectos, componentes, criterios, dimensiones o comportamientos, necesarios de tomarse en cuenta, para realizar una tarea, controlar y evaluar detalladamente el desarrollo de un proyecto, evento, producto o actividad. Dichos componentes se organizan de manera coherente para permitir que se evalúe de manera efectiva, la presencia o ausencia de los elementos individuales enumerados o por porcentaje de cumplimiento u ocurrencia. (Oliva, 2009)

3.4 Informe de auditoria

Se tabulará de acuerdo a las técnicas recomendadas para obtener el mejor efecto posible, donde se tomaran resultados para análisis de los datos y determinar el estado en el que se encuentra la seguridad de información en los Procesos Soportados por el Área de Sistemas en la Cámara de Comercio de Aguachica, Cesar

Capítulo 4. Resultados

4.1. El estado actual de la seguridad de la información para los procesos soportados por el área de sistemas en la cámara de comercio de Aguachica, Cesar.

4.1.1. Archivos permanentes

Tabla 1. Archivos permanentes.

ARCHIVOS PERMANENTES	
Secciones	**Nomenclatura**
Organigrama de la empresa	AP1 - 1/n
Manuales de funciones y Procedimientos.	AP2 – 1/n
Plan estratégico	AP3 – 1/n
Esquema de distribución de los equipos de cómputo.	AP4 – 1/n
Inventario de Recursos Tecnologías de la información	AP5 – 1/n
Mantenimiento a Recursos Informáticos	AP6 – 1/n
Plan de Contingencia	AP7 – 1/n

Fuente: Autores del proyecto.

4.1.2 Plan de auditoria

MODELO DE PROGRAMA GENERAL DE TRABAJO DE AUDITORIA

Descripción de la entidad auditada

Objetivos. La Cámara de Comercio de Aguachica - Cesar es una entidad privada de carácter gremial que representa los intereses de los empresarios y la comunidad en general del Sur del Cesar y de Bolívar, y cumple funciones delegadas por el Estado.

Objetivos corporativos

- Organizar y prestar de forma eficiente y eficaz los servicios de registros públicos a los empresarios y comunidad en general del Sur del Cesar y Sur de Bolívar.
- Promover el desarrollo empresarial del Sur del Cesar y Sur de Bolívar
- Mantener la sostenibilidad económica y social de la Cámara, para garantizar la prestación eficiente de los registros públicos
- Implantar una cultura orientada al cliente, soportada en procesos organizacionales efectivos que respondan a las necesidades y requerimientos legales.

Objetivos estratégicos:

PERSPECTIVA FINANCIERA

Generar nuevas fuentes de recursos para la entidad y administrarlos adecuadamente.

PERSPECTIVA ORGANIZACIONAL

Lograr una cultura de mejoramiento permanente.

Mejorar la estructura física y tecnológica.

PERSPECTIVA PROCESOS

Diversificar y Generar nuevos servicios para el empresariado y la comunidad.

Generar sentido de pertenencia en la comunidad empresarial.

Generar procesos de desarrollo empresarial y regional.

Perspectiva Clientes

Satisfacer los requerimientos de servicio formulados por nuestros usuarios.

Estructura

Misión. La Cámara de Comercio de Aguachica. Es una entidad privada, sin ánimo de lucro, con el propósito de prestar los servicios de registros, conciliación y desarrollo socioeconómico de la región, llevando la representación y vocería de los empresarios ante el gobierno nacional, regional y municipal, para fortalecer el Bienestar de la comunidad, basada en una cultura del conocimiento.

Visión. Liderar el desarrollo integral de la región y promover estrategias que permitan fortalecer la cultura empresarial de las comunidades de la jurisdicción, en respuesta a los cambios globales.

Organigrama general

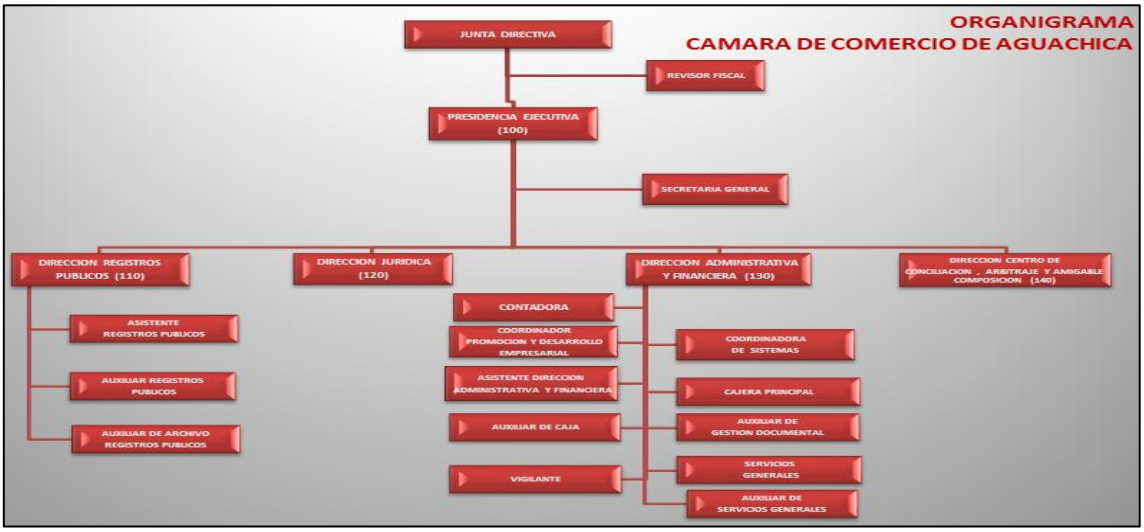

Figura 1. Organigrama de la cámara de comercio de Aguachica, Cesar.

Fuente: Cámara de Comercio de Aguachica.

Mapa de Procesos

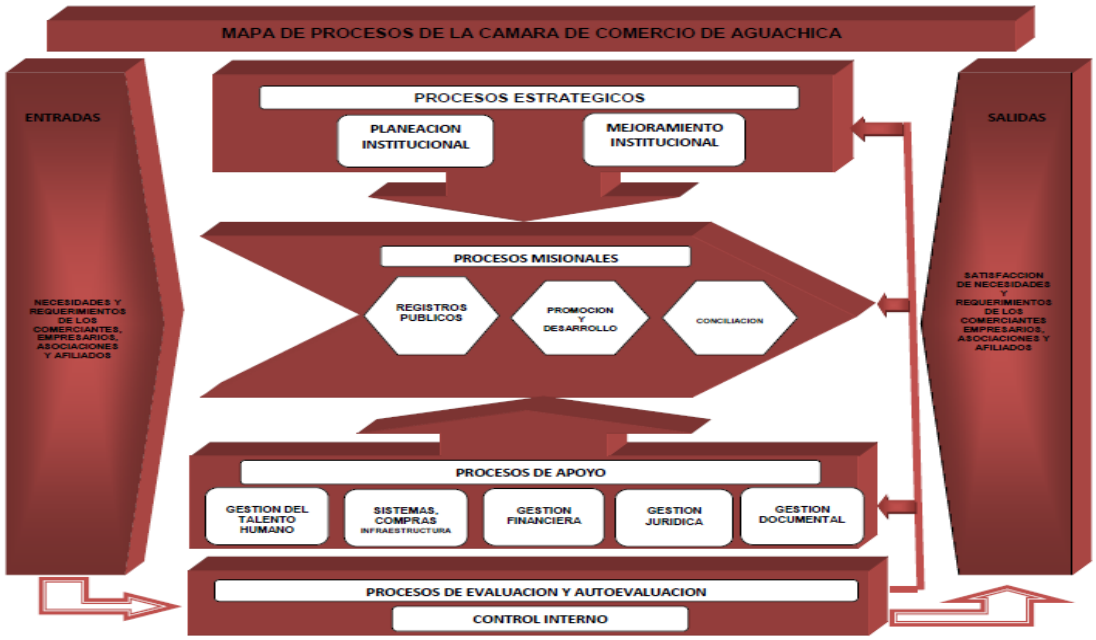

Figura 2. Mapa de procesos de la cámara de comercio de Aguachica, Cesar.

Fuente: Cámara de Comercio de Aguachica.

Sistemas. La Cámara de Comercio de Aguachica es una entidad que soporta sus procesos misionales y de apoyo a través de sistemas de información las cuales les permiten diligenciar cada uno de los trámites necesarios para dar cumplimiento a todas sus funciones.

La Cámara de Comercio cuenta con 21 empleados de los cuales 16 utilizan un computador y solo 5 empleados no utilizan (2 trabajan en la calle, 3 servicios generales), esto quiere decir que los principales procesos requieren de las labores realizadas a través de equipos de cómputo.

Los sistemas de información que utilizan la Cámara de Comercio son:

Tabla 2. Sistemas de información utilizados en la cámara de comercio de Aguachica, cesar.

Software	**Descripción**
JSP7	Software Contable
Sistema Integrado de Información **SII**	Utilizado para soportar todos los servicios camerales como: matriculas, cancelaciones, inscripción de actos, embargos, desembargos y demás procesos.
DocuWare	Utilizado para digitalizar todos los documentos que ingresan a la Cámara de Comercio los cuales son: registros Públicos (Mercantil, Esal, Proponentes), correspondencia, documentos administrativos, contables y de conciliación.

Fuente: Autores del proyecto.

Las características de la infraestructura física son las siguientes:

Tabla 3. Características de la infraestructura física

	Características
Topología de red física	Estrella extendida
Canal dedicado de UNE	10 Megas
Canal Banda Ancha de Movistar	2 Megas
Canal Banda Ancha de Movistar	4 Megas
Router	Cisco 1700
Switch	3com 3C17300A SuperStack 4200 26 puertos
Switch	Planet 10/100 Mbps Ethernet Switch 24 Puertos
Switch	HP V1910 246 Switch JE006A 24 Puertos

Fuente: Autores del proyecto.

Servidores

Tabla 4. Servidores

Nombre	Función	Computador	Sistema Operativo	Base de datos
SIREP	Base de datos de los Procesos Camerales	Hp Provilan ML110	Suse Linux 10	Adabas
Sega	Contable	Hp Proliant ML110	Suse Linux 10	SQL server
Docuware	Digitalización	Hp Proliant ML3 10e Gen 8 V2	Windows server 2012	SQL Server
SII (Sistema Integrado de Gestión)	Trámites de los procesos Camerales	En la nube	Ubunto 4.14	

Fuente: Autores del proyecto.

Esquema Lógico de Red

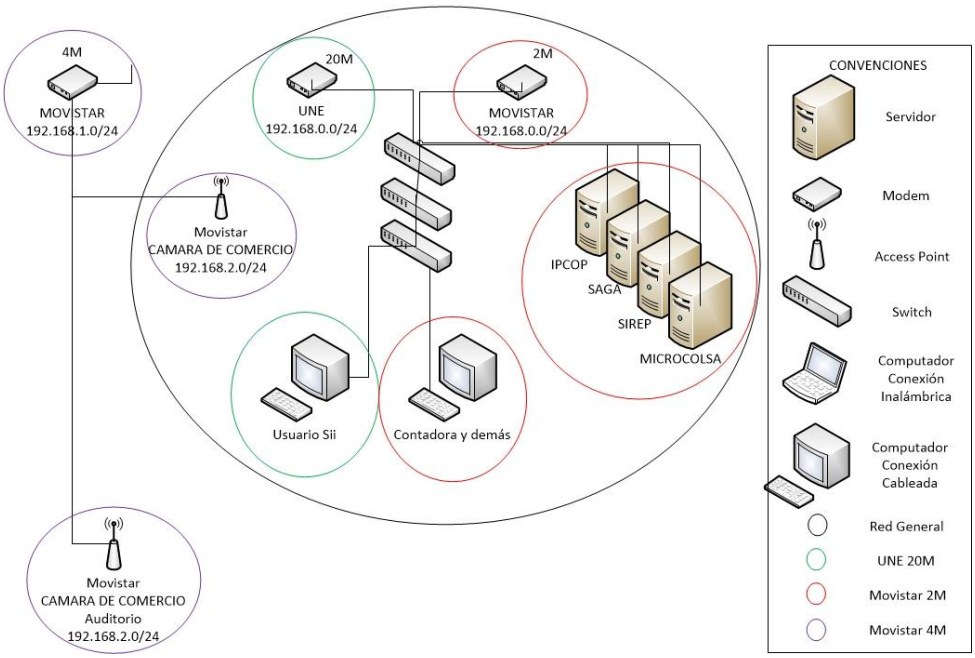

Figura 3. Esquema lógico de red
Fuente: Autores del proyecto.

Objetivos de la Auditoria

Objetivos

General. Evaluar el estado actual de la seguridad de la información en la Cámara de Comercio de Aguachica

Alcance del Trabajo. La Auditoría se desarrollara en la Cámara de Comercio de Aguachica, en donde se realizara la revisión de todas las áreas de acuerdo a la norma ISO 27002:2013.

Tabla 5. Alcance del trabajo

FASE	DESCRIPCION	ACTIVIDAD	NUM. DEL PERSONAL PARTICIPANTE	PERIODO ESTIMADO	
				INICIO	TERMINO
1	Identificar la naturaleza operativa de la organización, ubicación de sus instalaciones, servicios prestados, su estructura y otros asuntos que sean significativos en la auditoria.	Visita preliminar al área auditada Solicitar manual de funciones y organigrama Determinar el objetivo y alcance Establecer los puntos que serán evaluados Seleccionar métodos, instrumentos y técnicas de recolección de información, de acuerdo a los requerimientos Entrega de acta de iniciación de auditoria	ALEXANDER MENESES MARTINEZ ERNEY ALBERTO RAMIREZ CAMARGO MARIA ALEJANDRA MERCHAN VILLALBA YADITZA SUAREZ DE LA CRUZ	25/05/16	01/06/16
2	Se aplicaran cada uno de los instrumentos de recolección y pruebas	Aplicar las entrevistas Efectuar las encuestas Aplicar las listas de chequeo Realizar las pruebas pertinentes	ALEXANDER MENESES MARTINEZ ERNEY ALBERTO RAMIREZ CAMARGO MARIA ALEJANDRA MERCHAN VILLALBA YADITZA SUAREZ DE LA CRUZ	01/05/16	04/06/16
		Identificar y documentar las situaciones encontradas	ALEXANDER MENESES MARTINEZ	05/06/16	07/06/16

3	En esta fase analizaremos la información recolectada en donde se identificaran y documentaran las situaciones encontraras y relevantes dando como resultado el dictamen final y sus respectivas recomendaciones	Poner en discusión los hallazgos con el personal auditado y el equipo auditor Identificar las situaciones relevantes Desarrollar el borrador del informe Elaborar el dictamen final Presentar el informe de Auditoría Presentar el informe al Director Ejecutivo de la Cámara de Comercio y a la Directora Administrativa y Financiera	ERNEY ALBERTO RAMIREZ CAMARGO MARIA ALEJANDRA MERCHAN VILLALBA YADITZA SUAREZ DE LA CRUZ		

Fuente: Autores del proyecto.

4.1.3 Guía de auditoria

GUIA DE AUDITORIA PARA LA FASE **INVESTIGACIÓN PRELIMINAR**

Tabla 6. Guía de auditoria para la fase investigación preliminar.

CÁMARA DE COMERCIO DE AGUACHICA			Fecha Inicial			Fecha Final		
			DD	MM	AA	DD	MM	AA
			25	05	16	01	06	16
Referencia	Actividad o función a evaluar.	Técnica de evaluación.	Calificación.			Observación.		
P-001	Visita preliminar al área auditada	Observación directa.						
P-002	Identificar la estructura organizacional de la Cámara de Comercio de Aguachica y sus	Revisión documental del manual de funciones y organigrama, plan de contingencia, inventario de software, hardware						

	funciones.	Entrevista dirigida a la Directora Administrativa y Financiera de la Cámara de Comercio de Aguachica.		
P-003	Documentar el objetivo y alcance de la Auditoria	Documento.		
P-004	Establecer los puntos que serán evaluados	Observación Directa Documentos		
P-005	Diseñar los instrumentos de recolección de información	Documentos.		
P-006	Entrega de acta de iniciación de auditoria	Documento		

Fuente: Autores del proyecto.

GUIA DE AUDITORIA PARA LA FASE **EJECUTAR LA AUDITORIA**

Tabla 7. Guía de auditoria para la fase ejecutar la auditoria.

CÁMARA DE COMERCIO DE AGUACHICA			Fecha Inicial			Fecha Final		
			DD	MM	AA	DD	MM	AA
			01	06	16	04	06	16
Referencia	Actividad o función a evaluar.	Técnica de evaluación	Calificación.			Observación.		
E-001	Identificar el conocimiento básico referente a seguridad de la información por parte de los empleados de la Cámara de Comercio de Aguachica	Encuesta						
E-002	Políticas de Seguridad.	Lista de Chequeo						
E-003	Aspectos Organizativos de La Seguridad de La Información	Entrevista						
E-004	Seguridad Ligada a los Recursos Humanos	Entrevista						

E-005	Gestión de Activos	Lista de Chequeo		
E-006	Control de Accesos	Entrevista		
E-007	Seguridad Física y Ambiental	Entrevista		
E-008	Seguridad en la Operativa	Lista de Chequeo		
E-009	Seguridad en las Telecomunicaciones	Lista de Chequeo		
E-010	Adquisición, Desarrollo y Mantenimiento de Los Sistemas de Información	Lista de Chequeo		
E-011	Relaciones con Suministradores.	Lista de Chequeo		
E-012	Gestión de Incidentes en la Seguridad de la Información	Lista de Chequeo		
E-013	Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	Lista de Chequeo		
E-014	Cumplimiento	Lista de chequeo		

Fuente: Autores del proyecto.

GUIA DE AUDITORIA PARA LA FASE **DICTAMEN DE LA AUDITORIA**

Tabla 8. Guía de auditoria para la fase dictamen de la auditoria.

CÁMARA DE COMERCIO DE AGUACHICA			Fecha Inicial			Fecha Final		
			DD	MM	AA	DD	MM	AA
			05	06	16	07	06	16
Referencia	Actividad o función a evaluar.	Técnica de evaluación.	Calificación.			Observación.		
D-001	Analizar la información recolectada y Recopilar las situaciones encontradas	Formularios (situaciones encontradas)						

D-002	Comentar con el equipo de auditoria y el persona auditado situaciones encontradas, determinar las causas y soluciones, para definir las situaciones relevantes	Formularios (situaciones encontradas)		
D-003	Desarrollar el borrador del informe	Documento		
D-004	Elaborar el informe final	Documento		
D-005	Presentar el informe final al Director Ejecutivo de la Cámara de Comercio de Aguachica	Reunión		

Fuente: Autores del proyecto.

Carta de inicio de auditoria, **apéndice A**

4.1.4 Instrumentos de Recolección de Información

Ver apéndice s B y C

4.1.5 Dictamen

Situaciones Encontradas

Tabla 9. Situaciones encontradas

Empresa	**Área auditada**	**Día**	**Mes**	**Año**
Cámara de Comercio de Aguachica	Departamento de Sistemas	05	06	16

Ref.	**Situaciones**	**Causas**	**Solución**	**Fecha de Solución**	**Responsable**
001	Faltan buenas prácticas	Falta de	Capacitación al	10/10/2016	Coordinadora

	en la utilización de contraseñas de accesos a los equipos.	conocimientos de buenas prácticas en seguridad de la información.	personal administrativo.		de Sistemas
002	Instalación de Software sin certificado de seguridad reconocido.	Ausencia de políticas de seguridad de la información en donde se reglamente la instalación del Software.	Diseño e implementación de una política adecuada donde se contemple todo lo relacionado con el Software.	22/09/2016	Coordinadora de Sistemas
003	Ausencia parcial de cultura de copias de seguridad y restauración (Backup) de la información sensible de la empresa.	Desconociendo de buenas prácticas de seguridad de la información	Capacitación al personal de organización. Creación de procedimientos para el crear Backup.	10/10/2016	Coordinadora de Sistemas
004	Inclusión de datos personales en las contraseñas de acceso y poca frecuencia en el cambio de las mismas.	Falta de implementación de las políticas de seguridad de la información y de buenas prácticas.	Reestructuración de la política existente y la capacitación al personal en buenas partes.	22/09/2016 Reestructuración del manual de seguridad de la información 10/10/2016 Capacitación al personal.	Directora Administrativa y Financiera. Coordinadora de Sistemas.
005	Malos manejos en los almacenamientos de la información en medios magnéticos.	Falta de políticas de seguridad de la información y de buenas prácticas.	Reestructuración de la política existente y la capacitación al personal en buenas partes.	22/09/2016 Reestructuración del manual de seguridad de la información 10/10/2016 Capacitación al personal.	Coordinadora de Sistemas.
006	Malos manejos en las cuentas de correo electrónico institucionales.	Falta de políticas de seguridad de la información y de buenas prácticas de seguridad de la información.	Reestructuración de la política existente y la capacitación al personal en buenas partes.	22/09/2016 Reestructuración del manual de seguridad de la información 10/10/2016 Capacitación al personal.	Coordinadora de Sistemas.
007	Incumplimiento en los objetivos misionales Plantados.	Falta de un modelado de procesos adecuados.	Reestructuración del mapa y el modelado procesos misionales de la empresa.	10/02/2017	Director Ejecutivo Directora Administrativa y Financiera.
008	Incumplimiento en algunas funciones de los empleados.	Inconsistencia en el manual de procesos y procedimientos.	Adecuación del manual de procesos y procedimientos.	17/04/2017	Director Ejecutivo Directora Administrativa

					y Financiera.
009	Malos manejos en la adquisición y la implementación de TI.	Desconocimientos en adquisición de TI	Estructuración de un Plan de Estratégico de TI	10/04/2017	Directora Administrativa y Financiera. Coordinadora de Sistemas.
010	Desconocimientos de la seguridad de la información por parte de la alta gerencia.	Falta de políticas de seguridad de la información y de buenas prácticas.	Implementación de políticas de seguridad de la Información y capacitación al personal administrativo.	2017	Coordinadora de Sistemas.
011	Se observó que el proceso de selección de personal debe ser más riguroso	Inexistencia de criterios de selección, dentro de una política establecida.	Estructuración de las políticas, en donde se estipula criterios de antes y después de la contratación.	22/09/2016	Director Ejecutivo Directora Administrativa y Financiera.
012	Inconsistencia en la entrega de cargos, o empalmes pertinentes.	Inexistencia de criterios dentro de la política que establece la terminación de contrato.	Estructurar en la política institucional, los respectivos empalmes a la hora de finalización de contratos.	19/09/2016	Director Ejecutivo Directora Administrativa y Financiera.
013	No se contempla la entrega de las políticas de seguridad de la información a funcionarios	Desconocimiento de la importancia de la política de seguridad de la información para la organización.	Directrices de las alta gerencia para la implantación la políticas de seguridad de la información.	2017	Directora Administrativa y Financiera. Coordinadora de Sistemas.
014	Inconsistencias en el tratamiento de la seguridad de la información.	Desconocimiento de la importancia de salvaguardar la confidencialidad, integridad y disponibilidad	Contratación y capacitación del personal y Tecnología adecuada que permita salvaguardad la información	2017	Coordinadora de Sistemas.
015	Ausencia de las penalidades contempladas para quienes infrinjan las normas.	Inexistencia de una política de seguridad de la información que contemple dichas sanciones	Elaboración de una política de seguridad de la información que contemple dichas restricciones.	2017	Directora Administrativa y Financiera. Coordinadora de Sistemas.
017	La Cámara de Comercio de Aguachica cuenta con un Manual de Seguridad de la Información, el cual no ha sido	Desconocimiento de la importancia de implementar políticas de seguridad de la información, para	Implementar las políticas de seguridad de la información.	2017	Director Ejecutivo Directora Administrativa y Financiera.

	Aprobado ni implementado.	tener buenas prácticas en el buen uso seguro de la información.			Coordinadora de Sistemas.
018	El manual de seguridad de la información no incluye los criterios para la implementación de un SGSI.	Desconocimiento de la Norma ISO 27001.	Actualización del manual de seguridad de la información o políticas, que contenga los criterios necesarios para la implementación de un SGSI.	22/09/2016	Director Ejecutivo Directora Administrativa y Financiera. Coordinadora de Sistemas
019	El manual de seguridad de la información no ha sido socializado ante los funcionarios y mucho menos aprobada.	Falta de compromiso con la seguridad de la información de la empresa.	Actualizar e implementar el manual o políticas de seguridad de la información.	20/09/2016 actualización de las políticas de seguridad de la información 2017 Implementación de las políticas de la seguridad de la información.	Director Ejecutivo Directora Administrativa y Financiera. Coordinadora de Sistemas.
020	No se realizan revisiones periódicas a las políticas de seguridad de la información.	No cuenta con comité de seguridad de la información que esté al tanto de los cambios en cuanto a seguridad de la Información.	Crear un Comité de Seguridad de la Información.	2017	Director Ejecutivo Directora Administrativa y Financiera. Coordinadora de Sistemas.
021	El inventario de los activos es llevado en un aplicativo contable y este activo es asignado a cada empleado, pero este desconoce que activo le es asignado debido a que no le hacen firmar ningún documento que así lo diga.	Falta de formalismo en el proceso y falta de comunicación entre la parte directiva y el empleado.	Comunicarle de manera formal que activos le son asignados al empleado, debido a que en la Cámara de Comercio existes activos que se comparten entre más de una persona pero no se sabe quién es el responsable de ese activo.	02/11/2016	Directora Administrativa y Financiera.
022	No están documentadas, ni implementadas las reglas de uso aceptable de la información y activos de información.	Falta de implementación de Políticas de seguridad de la información, que especifiquen la	Incluir dentro de las Políticas de Seguridad de la Información este punto, que el empleado sepa	27/02/2016	Coordinadora de Sistemas.

	Existe un Manual de políticas de seguridad de la información y un manual de protección de datos personales, pero no se cumple, no se ha implementado.	manera como se debe usar la Información.	cuál es el uso aceptable de la información y de los activos; además implementar dicha política.		
023	No existe control de las devoluciones de activos, por parte del usuario al momento de finalizar el contrato o empleo.	Falta de control de los activos de la empresa. No existe ni siquiera el acta por el cual el empleado se hace responsable de los activos que utiliza mientras tiene alguna vinculación con la Cámara de Comercio de Aguachica.	Formalizar el proceso, llenar las actas de entrega de activos al momento de emplear y actas de entrega al momento que se desvincula el funcionario o contratista.	02/11/2016	Directora Administrativa y Financiera.
024	Solo la información del área de registro está clasificada en función de los requisitos legales, criticidad y susceptibilidad	No se tiene conciencia de la importancia de clasificar toda la información de la empresa, tanto privada como publica	Al igual que está clasificada la información de registros públicos, realizar el proceso para clasificar la información de las demás dependencias de la Cámara de Comercio de Aguachica.	27/02/2017	Directora Administrativa y Financiera. Y Coordinadora de Sistemas.
025	La información no se encuentra etiquetada de acuerdo a los esquemas de clasificación de la Cámara de Comercio de Aguachica	Falta de conocimiento de la importancia de tener identificada la información.	De acuerdo a la clasificación de la información comenzar a etiquetarla para poder identificarla con claridad	03/03/2017	Directora Administrativa y Financiera.
026	No existen procedimientos para el manejo de activos de acuerdo al esquema de clasificación de la organización.	No se tiene conciencia de la importancia de clasificar los activos de acuerdo al esquema de clasificación de la información. El esquema de clasificación de la información es	Realizar la clasificación para toda la entidad y definir los procedimientos adecuados para el manejo de los activos de acuerdo a dicha información.	03/03/2017	Directora Administrativa y Financiera.

		solo de registros públicos más no de toda la información de la entidad.			
027	No existen políticas para gestionar los medios removibles, para proteger la información contenida en las diferentes formas almacenamiento.	No se tiene conciencia de la importancia de proteger los diferentes sitios donde se almacena la información.	Definir dentro de las políticas de seguridad la gestión de los medios removibles dentro de la entidad.	15/09/2016	Directora Administrativa y Financiera. Y Coordinadora de Sistemas.
028	No existe un procedimiento para disponer en forma segura de los medios cuando ya no se requieran.	La Cámara de Comercio no cuenta con un comité de seguridad de la información ni de calidad para definir este tipo de políticas y procedimientos.	Realizar un comité de calidad y de seguridad de la información para definir estos procedimientos.	03/04/2017	Directora Administrativa y Financiera. Y Coordinadora de Sistemas.
029	No se encuentran protegidos los medios que contienen información contra acceso no autorizado, uso indebido o corrupción durante el transporte, como el dispositivo con interfaz USB para firmado digital.	No existe conciencia sobre la protección que se le debe dar a estos medios.	Especificar dentro de las políticas de seguridad de la información la forma como se deben proteger estos medios.	03/04/2017	Coordinadora de Sistemas.
030	No está oficializada la asignación de la función de administrador de la seguridad a la ingeniera de sistemas.	No está actualizado el manual de funciones de cada cargo de la Cámara de Comercio de Aguachica	Actualizar el Manual de funciones de acuerdo a las nuevas funciones de cada empleado.	05/05/2017	Directora Administrativa y Financiera. Y Coordinadora de Sistemas.
031	No existen controles para evitar la instalación de programas per to per o mensajería instantánea.	No utilizar controles que impidan la instalación de este tipo de programas.	Agregar en la política de seguridad de la información los controles necesarios para evitar la instalación de estos programas.	20/09/2016	Coordinadora de Sistemas.
032	La coordinadora de sistemas y La Ingeniera de sistemas tienen acceso como administradores de los	Falta de definir en el manual de funciones que le corresponde hacer a cada funcionario,	Reestructuración del manual de funcionalidades de los empleados.	05/04/2017	Directora Administrativa y Financiera.

	sistemas de información SII y DocuWare, lo recomendable es que solo un usuario pueda realizar los cambios como administrador. Esto puede generar inconsistencias a la hora de presentar desfiguración del sistema, al no saber con certeza quien es el culpable.	para que no se mezclen las funciones.			
033	No existe ninguna medida para controlar el uso de quemadoras de CD, unidades ZIP y memorias USB, exponiendo la información de la cámara de comercio.	No existen políticas implementadas que indiquen como se deben controlar estas situaciones.	Agregar a la política de seguridad de la información un ítem que controle el uso de Quemadoras de CD, Unidades ZIP y USB.	20/09/2016	Coordinadora de Sistemas.
034	No existe ningún procedimiento para otorgar y/o revocar el acceso y privilegios a los sistemas informáticos.	No está establecido un comité de calidad, no existen procedimientos formales.	Establecer un procedimiento formal para este caso.	06/04/2017	Directora Administrativa y Financiera.
035	Solo cuentan con antivirus para la protección de los equipos de cómputo, no tienen instalados otra medida de seguridad como IDS, FIREWALLS, entre otros. La manera como protegen sus servidores físicamente es aislándolos del personal no autorizado y de manera lógica con contraseñas de acceso.	Confianza en el equipo de trabajo, y falta de inversión en el aspecto de seguridad.	Tomar conciencia de la importancia de establecer medidas de seguridad tanto físicas como lógicas para salvaguardar el activo más importante de la empresa como lo es la información.	20/02/2016	Directora Administrativa y Financiera. Y Coordinadora de Sistemas.
036	No existen controles por medio de pruebas de auditorías (Audit trails).	Nunca se ha realizado auditoria de sistemas. La base de datos no permite ver el registro de auditorías.	Establecer procedimientos para que el DBMS, ejecute auditorías a la base de datos y que constantemente se realicen auditorias	2017	Director Ejecutivo Directora Administrativa y Financiera. Coordinadora de Sistemas.

			de sistemas a todas las áreas de la Cámara de Comercio.		
037	No existe procedimiento documentado para habilitar a la Alta Dirección de la Cámara de Comercio que verifiquen y revisen las autorizaciones por periodos a los sistemas de información.	Falta de procedimientos formales.	Establecer procedimientos formales para ese tipo de procesos	2017	Directora Administrativa y Financiera.
038	Disponen de un manual de Seguridad de la Información que establece los criterios para la creación de contraseñas robustas, pero este manual no está implementado y nunca se ha actualizado.	No cuentas con un comité de seguridad que lidere estos procesos, como la implementación del manual de seguridad de la información y que además constantemente lo actualicen de acuerdo a los cambios.	Crear el comité de seguridad de la información, crear nuevamente el manual o políticas de seguridad de la Información con base a los cambios efectuados en los sistemas de información e implementarlo.	10/09/2016 creación de las Políticas de seguridad de la Información 2017 Implementación de estas políticas.	Director Ejecutivo Directora Administrativa y Financiera. Coordinadora de Sistemas.
039	No cuentas con herramientas para la administración de los sistemas.	Consideran que la Cámara de Comercio es muy pequeña y aun no requieren de herramientas para administrar los sistemas. Cada Sistema de Información dispone de privilegios de administrador para controlar las funciones de cada usuario.	Adquisición de herramientas necesarias para administrar los sistemas y poder controlarlos mejor.	2017	Director Ejecutivo Directora Administrativa y Financiera. Coordinadora de Sistemas.
040	No existe una bitácora que recopile las veces que se le realizan revisiones a las instalaciones físicas, verbalmente indican que se realizan con mucha frecuencia pero no existe la evidencia.	Le restan importancia a la formalidad que deben tener estos procesos, de documentar cada vez que se realicen revisiones.	Llevar un registro cada vez que se realicen revisiones físicas y reportan los inconsistencias detectadas.	10/11/2016	Directora Administrativa y Financiera.

041	No existe ningún control para los visitantes, y ellos no son acompañados para visitar las áreas de la cámara de comercio, excepto el área de sistemas.	Falta de políticas de establezcan el ingreso controlado a las instalaciones de la Cámara de Comercio.	Establecer dentro de las Políticas de Seguridad de la información el control de acceso físico a las instalaciones.	20/09/2016	Director Ejecutivo Directora Administrativa y Financiera.
042	Sobre el cuarto donde está alojado el Data Center, existe un baño, lo que genera riesgo de daño de los dispositivos electrónicos por la humedad en el data Center.	Mal planificación y diseño de la Cámara de Comercio de Aguachica.	Reubiquen el baño que está ubicado en el segundo piso, sobre el Data Center.	2017	Director Ejecutivo Directora Administrativa y Financiera.
043	Cualquier persona puede ingresar a donde así lo desee, generando un problema de seguridad. El personal pregunta en recepción hacia donde desea ir, la funcionaria indica la ubicación y la persona se dirige a las instalaciones sin ningún problema, excepto al cuarto donde está el Data center, que siempre está bajo llave.	Exceso de confianza y falta de políticas que controlen estos aspectos de acceso a las instalaciones de la Cámara de Comercio.	Actualizar las Políticas de Seguridad de la información para incluir el acceso a las Instalaciones de la Cámara de Comercio.	20/09/2016	Director Ejecutivo Directora Administrativa y Financiera.
044	No existe ningún proceso para el control de llaves, solo la funcionaria encargada de servicios generales, la Directora Administrativa y Financiera, y en las noches el celador, manejan las llaves.	Falta de Políticas que controlen el manejo de las llaves y la realización de las respectivas copias.	Establecer una política para administrar que funcionarios administraran las llaves y el respectivo realizado de copias de las mismas.	24/09/2016	Director Ejecutivo Directora Administrativa y Financiera.
045	Si existe un sistema interno de grabación de circuito cerrado de tv, pero solo graba por siete días seguidos, después de ahí se reescribe la información.	El disco Duro del DVR no cuenta con el suficiente espacio para almacenar más de videos.	Adquirir un nuevo DVR o ampliar el disco duro para aumentar los días de grabado.	07/07/2017	Director Ejecutivo Directora Administrativa y Financiera. Coordinadora de Sistemas.
046	No se realizan cambios de las cerraduras con regularidad.	Exceso de confianza.	Establecer una política que regule la realización de cambios en la cerradura con	20/09/2016	Directora Administrativa y Financiera.

			frecuencia.		
047	La Cámara de comercio cuenta con alarmas, pero no están monitoreadas por alguna estación central.	Desconocimiento o exceso de confianza	Incluir en la Política, la obligatoriedad de tener monitoreada la alarma por un ente central.	20/09/2016	Director Ejecutivo Directora Administrativa y Financiera
048	No está documentada la ubicación de la alarma de detección de humo y tampoco está conectada a la central de bomberos	Inconsistencias en el diseño del plan de emergencias y evacuación.	Actualizar el plan de emergencias y evacuación.	2017	Director Ejecutivo Directora Administrativa y Financiera
049	El lugar donde está ubicado el Data Center, sólo cuenta con una puerta como control de acceso, no utiliza sistemas biométricos y tampoco cuenta con controles de temperatura y humedad.	Falta de políticas de seguridad de la información, de plan de contingencia y de inversión.	Implementar las políticas de seguridad de la información y plan de contingencia.	2017	Director Ejecutivo Directora Administrativa y Financiera
050	La Cámara de Comercio de Aguachica, no cuenta con fuentes de poder separadas para cada equipo de cómputo, tiene instalada una UPS de 1KW con capacidad de 15 min, que es utilizada para los dispositivos de red, servidores y tres equipos computo. A esta UPS, no se le realizan pruebas.	No existe plan de contingencia.	Desarrollar un plan de contingencia.	2017	Director Ejecutivo Directora Administrativa y Financiera
051	No existe medidas de seguridad que garanticen la continuidad del suministro eléctrico	No tienen plan de contingencia. No existe planta eléctrica en la Cámara de Comercio de Aguachica	Adquirir una Planta Eléctrica. Establecer mecanismos para poder continuar sin el fluido eléctrico.	06/06/2017	Director Ejecutivo Directora Administrativa y Financiera
052	No existen procedimientos para la eliminación de manera segura de información o dispositivos de cómputo.	Falta de procedimientos para controlar, la información y dispositivos que no son utilizados.	Desarrollar un comité de calidad y actualizar las políticas de seguridad de la información que	25/09/2016	Director Ejecutivo Directora Administrativa y Financiera.

	Cuando ya no es útil es alojada aun archivador físico o los dispositivos de cómputo se donan.		contemplen esta parte		
053	No existe un funcionario encargado de la verificar que todas las funciones de cada quien se realicen de manera correcta.	No existen comités de calidad ni de control interno.	Establecer un comité de Calidad y Control interno.	2017	Directora Administrativa y Financiera.
054	No existe control interno, o alguien que haga sus veces para verificar que se realizan los procedimientos como así están estipulados.	No existe control Interno	Establecer el control interno en la CC de Aguachica	2017	Director Ejecutivo Directora Administrativa y Financiera
055	No existe protección contra código malicioso	No cuentan con herramientas especializadas para este tipo de inconvenientes.	Adquirir nuevas herramientas de seguridad de la información e implementar las Políticas de Seguridad de la información.	2017	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas.
056	No existe un procedimiento que para realizar las copias de seguridad y tampoco que indique la manera de restauración. Actualmente se realizan copias pero sin seguir un procedimiento y sin saber cómo restaurar en caso de pérdida de información.	Falta de un comité de seguridad y de las Políticas de Seguridad de la información. Falta de plan de contingencia.	Desarrollar un procedimiento para poder saber con certeza como realizar las copias y restauración de la información.	2017	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas
057	No se lleva un registro de actividades y supervisión y nunca se han realizado auditorias de Sistemas.	Falta de personal Capacitado en el área de Auditoria, y no le dan importancia a los registros de supervisión y actividades.	Desarrollar un plan de auditorías y concienciar a los funcionarios encargados del área de la importancia de llevar registros de las actividades y supervisión.	2017	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas
058	La CC de Aguachica, no dispone de políticas de gestión y control de las redes para proteger la información en	Falta de políticas dentro de la CC que indiquen como se deben gestionar los procesos.	Implementación de las Políticas de Seguridad de la información.	2017	Director Ejecutivo Directora Administrativa

	sistemas y aplicaciones.				y Financiera Coordinadora de Sistemas
059	No existe ninguna documentación de los mecanismos de seguridad ni tampoco de los niveles de prestación y los requisitos de gestión de seguridad de los servicios de red.	Falta de Comité de sistemas de gestión. Falta de comité de seguridad de la información. Falta de control Interno	Nombrar los diferentes comités y exigir la creación de políticas internas para establecer los mecanismos de seguridad de la red y los requisitos de gestión de la misma y documentarlos.	2017	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas.
060	No existen políticas, ni procedimientos, para proteger la transferencia de información por cualquier medio.	Falta de políticas de seguridad de la información y del comité de calidad o control interno.	Definir las políticas de seguridad de la información e implementarlas.	20/09/2016 – diseño de políticas 2017 - implementación	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas.
061	No se documentan, ni revisan los requisitos para acuerdos de confidencialidad o no divulgación para la protección de la información.	Falta de control interno. Falta de Políticas de Seguridad de la información.	Definir las políticas de seguridad de la información e implementarlas.	20/09/2016 – diseño de políticas 2017 - implementación	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas.
062	La CC de Aguachica no dispone de ninguna herramienta para filtrar contenido web.	Falta de disposición económica para la adquisición de un sistema de protección, como Firewalls.	Incluir dentro del presupuesto, la necesidad de adquirir un sistema de filtrado web.	2017	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas.
063	Gestión de requerimientos para adquirir nuevos sistemas de información o mejorar los existentes.	Falta de planeación	Planear y gestionar los requerimientos que contribuyan a la toma de decisiones en el momento de adquirir nuevos sistemas de información o mejorar los	2017	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas.

			existentes		
064	No se garantizan las características fundamentales de la seguridad de la información en las aplicaciones.	No se estiman los riesgos inherentes a la información y el valor que ésta tiene para la organización	Tipificar, clasificar la información que se transmite hacia y desde la red y que opera bajo las plataformas organizacionales	20/09/2016	Coordinadora de Sistemas.
065	No existe un procedimiento de control formal para realizar cambios a los sistemas	Desconocimiento de la importancia de identificar los activos de la organización, sus funciones y su utilización	Documentar detalladamente todo el proceso de adquisición y mantenimiento y cambios en los sistemas	2017	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas.
066	No se realiza supervisión y seguimiento de sistemas contratados externamente	Falta de Gestión y pertinencia a las contrataciones	Mantener de manera organizada el proceso de seguimientos a las diferentes contrataciones.	2017	Director Ejecutivo Directora Administrativa y Financiera
067	En la política de seguridad de la información existente, no se contempla la relación con los suministradores ni gestión de riesgos presentes en este proceso	No se contempla el proceso de adquisición como factor importante de la seguridad de la información	Ampliar el alcance y contemplar factores estratégicos en la política de seguridad de la información	22/09/2016	Directora Administrativa y Financiera Coordinadora de Sistemas.
068	Falta documentación y control de servicios prestados por terceros	No se contempla como proceso importante tener seguimiento de los temas que tienen que ver con terceros	Plantear dentro de las políticas y gestión de riesgos la trazabilidad de procesos con terceros.	20/09/2016	Directora Administrativa y Financiera Coordinadora de Sistemas.
069	No se realiza gestión de incidentes de seguridad de la información	No se tiene en cuenta como factor de riesgo el control y reporte de los incidentes asociados a la seguridad de la información	Contemplar en la política de seguridad de la información los incidentes de seguridad y cómo actuar sobre estos.	21/09/2016	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas.
070	No se cuenta con un proceso de control para mantener las licencias de software actualizadas	No se contempla en las políticas de seguridad de la información el seguimiento y	Se debe plantear en la política de seguridad de la información la periódica	22/09/2016	Director Ejecutivo Directora Administrativa

		actualización de productos software	actualización de software que lo requiera		y Financiera Coordinadora de Sistemas.
071	La cámara de comercio de Aguachica no cuenta con un plan de contingencia y de manejo de accidentes, incidentes en caso de desastres naturales o cualquier otro fallo de seguridad y de operaciones	No existe plan de contingencia	Realizar el plan de contingencia y aplicar medidas de seguridad y continuidad del negocio	2017	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas.
072	No se realizan con frecuencia respaldos de información ni copias de seguridad de la configuración del servidor y de los equipos activos de red.	El jefe de sistema no tiene programada la realización de Backups mensual como lo indico en la entrevista	Realizar un plan para la realización de Backup	20/09/2016	Coordinadora de Sistemas.
073	No se contemplan procesos de cifrado de información sensible de la organización	Falta mayor incorporación de las políticas de seguridad de la información	Actualizar las Políticas de seguridad de la información mejoradas y gestión de riesgos.	22/09/2016	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas.
074	No se revisa ni se actualizan periódicamente elementos que puedan mejorarse en la política de seguridad de la información	Falta de concientización por parte del personal encargado y de valoración de la información como activo vital de la empresa	Revisar periódicamente de manera documentada y organizada las política de seguridad de la información	22/09/2016	Director Ejecutivo Directora Administrativa y Financiera Coordinadora de Sistemas.

Elaborado (Nombre y Firma)	**Aprobó (Nombre y Firma)**
Alex Meneses Martínez Erney Alberto Ramírez Camargo María Alejandra Merchán Villalba Yaditza Suarez de la Cruz	Alex Meneses Martínez Erney Alberto Ramírez Camargo María Alejandra Merchán Villalba Yaditza Suarez de la Cruz

Fuente: Autores del proyecto.

Tabla 10. Situaciones relevantes

Día	Mes	Año
05	06	16

Área auditada
Departamento de Sistemas

Empresa
CAMARA DE COMERCIO DE AGUACHICA

Ref.	Situaciones	Causas	Solución
001	Instalación de Software sin certificado de seguridad reconocido.	Ausencia de políticas de seguridad de la información en donde se reglamente la instalación del Software.	Diseño e implementación de una política adecuada donde s contemple todo lo relacionad con el Software.
002	Inclusión de datos personales en las contraseñas de acceso y poca frecuencia en el cambio de las mismas.	Falta de implementación de las políticas de seguridad de la información y de buenas prácticas.	Reestructuración de la políti existente y la capacitación a personal en buenas partes.
003	Malos manejos en los almacenamientos de la información en medios magnéticos.	Falta de políticas de seguridad de la información y de buenas prácticas.	Reestructuración de la políti existente y la capacitación a personal en buenas partes.
004	Incumplimiento en los objetivos misionales Plantados.	Falta de un modelado de procesos adecuados.	Reestructuración del mapa y modelado procesos misionale de la empresa.
005	Incumplimiento en algunas funciones de los empleados.	Inconsistencia en el manual de procesos y procedimientos.	Adecuación del manual de procesos y procedimientos.
006	Malos manejos en la adquisición y la implementación de TI.	Desconocimientos en adquisición de TI	Estructuración de un Plan de Estratégico de TI
007	Desconocimientos de la seguridad de la información por parte de la alta gerencia.	Falta de políticas de seguridad de la información y de buenas prácticas.	Implementación de políticas d seguridad de la Información y capacitación al personal administrativo.
008	Se observó que el proceso de selección de personal debe ser más riguroso	Inexistencia de criterios de selección, dentro de una política establecida.	Estructuración de las políticas en donde se estipula criterios d antes y después de la contratación.
009	Inconsistencia en la entrega de cargos, o empalmes pertinentes.	Inexistencia de criterios dentro de la política que establece la terminación de contrato.	Estructurar en la política institucional, los respectivos empalmes a la hora de finalización de contratos.
010	No se contempla la entrega de las políticas de seguridad de la información a funcionarios	Desconocimiento de la importancia de la política de seguridad de la información para la organización.	Directrices de las alta gerenci para la implantación la políti de seguridad de la informació
011	Ausencia de las penalidades contempladas para quienes infrinjan las normas.	Inexistencia de una política de seguridad de la información que contemple dichas sanciones	Elaboración de una política d seguridad de la información qu contemple dichas restriccione
012	La Cámara de Comercio de Aguachica cuenta con un Manual de Seguridad de la Información, el cual no ha sido	Desconocimiento de la importancia de implementar políticas de seguridad de la información, para tener buenas	Implementar las políticas de seguridad de la información.

	Aprobado ni implementado.	prácticas en el buen uso seguro de la información.	
013	El manual de seguridad de la información no incluye los criterios para la implementación de un SGSI.	Desconocimiento de la Norma ISO 27001.	Actualización del manual de seguridad de la información o políticas, que contenga los criterios necesarios para la implementación de un SGSI.
014	El manual de seguridad de la información no ha sido socializado ante los funcionarios y mucho menos aprobado.	Falta de compromiso con la seguridad de la información de la empresa.	Actualizar e implementar el manual o políticas de seguridad de la información.
015	No se realizan revisiones periódicas a las políticas de seguridad de la información.	No cuenta con comité de seguridad de la información que esté al tanto de los cambios en cuanto a seguridad de la Información.	Crear un Comité de Seguridad de la Información.
016	No están documentadas, ni implementadas las reglas de uso aceptable de la información y activos de información. Existe un Manual de políticas de seguridad de la información y un manual de protección de datos personales, pero no se cumple, no se ha implementado.	Falta de implementación de Políticas de seguridad de la información, que especifiquen la manera como se debe usar la Información.	Incluir dentro de las Políticas de Seguridad de la Información este punto, que el empleado sepa cuál es el uso aceptable de la información y de los activos; además implementar dicha política.
017	No existe control de las devoluciones de activos, por parte del usuario al momento de finalizar el contrato o empleo.	Falta de control de los activos de la empresa. No existe ni siquiera el acta por el cual el empleado se hace responsable de los activos que utiliza mientras tiene alguna vinculación con la Cámara de Comercio de Aguachica.	Formalizar el proceso, llenar las actas de entrega de activos al momento de emplear y actas de entrega al momento que se desvincula el funcionario o contratista.
018	Solo la información del área de registro está clasificada en función de los requisitos legales, criticidad y susceptibilidad	No se tiene conciencia de la importancia de clasificar toda la información de la empresa, tanto privada como publica	Al igual que está clasificada la información de registros públicos, realizar el proceso para clasificar la información de las demás dependencias de la Cámara de Comercio de Aguachica.
019	No existen procedimientos para el manejo de activos de acuerdo al esquema de clasificación de la organización.	No se tiene conciencia de la importancia de clasificar los activos de acuerdo al esquema de clasificación de la información. El esquema de clasificación de la información es solo de registros públicos más no de toda la información de la entidad.	Realizar la clasificación para toda la entidad y definir los procedimientos adecuados para el manejo de los activos de acuerdo a dicha información.

020	No existen políticas para gestionar los medios removibles, para proteger la información contenida en las diferentes formas almacenamiento.	No se tiene conciencia de la importancia de proteger los diferentes sitios donde se almacena la información.	Definir dentro de las políticas de seguridad la gestión de los medios removibles dentro de la entidad.	15/09/2016
021	No se encuentran protegidos los medios que contienen información contra acceso no autorizado, uso indebido o corrupción durante el transporte, como el dispositivo con interfaz USB para firmado digital.	No existe conciencia sobre la protección que se le debe dar a estos medios.	Especificar dentro de las políticas de seguridad de la información la forma como se deben proteger estos medios.	
022	No está oficializada la asignación de la función de administrador de la seguridad a la ingeniera de sistemas.	No está actualizado el manual de funciones de cada cargo de la Cámara de Comercio de Aguachica	Actualizar el Manual de funciones de acuerdo a las nuevas funciones de cada empleado.	
023	La coordinadora de sistemas y La Ingeniera de sistemas tienen acceso como administradores de los sistemas de información SII y DocuWare, lo recomendable es que solo un usuario pueda realizar los cambios como administrador. Esto puede generar inconsistencias a la hora de presentar desfiguración del sistema, al no saber con certeza quien es el culpable.	Falta de definir en el manual de funciones que le corresponde hacer a cada funcionario, para que no se mezclen las funciones.	Reestructuración del manual de funcionalidades de los empleados.	
024	No existe ninguna medida para controlar el uso de quemadoras de CD, unidades ZIP y memorias USB, exponiendo la información de la cámara de comercio.	No existen políticas implementadas que indiquen como se deben controlar estas situaciones.	Agregar a la política de seguridad de la información un ítem que controle el uso de Quemadoras de CD, Unidades ZIP y USB.	
025	Solo cuentan con antivirus para la protección de los equipos de cómputo, no tienen instalados otra medida de seguridad como IDS, FIREWALLS, entre otros. La manera como protegen sus servidores físicamente es aislándolos del personal no autorizado y de manera lógica con contraseñas de acceso.	Confianza en el equipo de trabajo, y falta de inversión en el aspecto de seguridad.	Tomar conciencia de la importancia de establecer medidas de seguridad tanto físicas como lógicas para salvaguardar el activo más importante de la empresa como lo es la información.	
026	No existen controles por medio de pruebas de auditorías (Audit trails).	Nunca se ha realizado auditorias de sistemas. La base de datos no permite ver el registro de auditorías.	Establecer procedimientos para que el DBMS, ejecute auditorías a la base de datos y que constantemente se realicen auditorias de sistemas a todas las áreas de la Cámara de Comercio.	
027	Disponen de un manual de Seguridad de la Información que establece los criterios para la creación de contraseñas robustas, pero este	No cuentas con un comité de seguridad que lidere estos procesos, como la implementación del manual de	Crear el comité de seguridad de la información, crear nuevamente el manual o políticas de seguridad de la	

	manual no está implementado y nunca se ha actualizado.	seguridad de la información y que además constantemente lo actualicen de acuerdo a los cambios.	Información con base a los cambios efectuados en los sistemas de información e implementarlo.	
028	No existe ningún control para los visitantes, y ellos no son acompañados para visitar las áreas de la cámara de comercio, excepto el área de sistemas.	Falta de políticas de establezcan el ingreso controlado a las instalaciones de la Cámara de Comercio.	Establecer dentro de las Políticas de Seguridad de la información el control de acceso físico a las instalaciones.	
029	Sobre el cuarto donde está alojado el Data Center, existe un baño, lo que genera riesgo de daño de los dispositivos electrónicos por la humedad en el data Center.	Mal planificación y diseño de la Cámara de Comercio de Aguachica.	Reubiquen el baño que está ubicado en el segundo piso, sobre el Data Center.	
030	Cualquier persona puede ingresar a donde así lo desee, generando un problema de seguridad. El personal pregunta en recepción hacia donde desea ir, la funcionaria indica la ubicación y la persona se dirige a las instalaciones sin ningún problema, excepto al cuarto donde está el Data center o que siempre está bajo llave.	Exceso de confianza y falta de políticas que controlen estos aspectos de acceso a las instalaciones de la Cámara de Comercio.	Actualizar las Políticas de Seguridad de la información para incluir el acceso a las Instalaciones de la Cámara de Comercio.	
031	Si existe un sistema interno de grabación de circuito cerrado de tv, pero solo graba por siete días seguidos, después de ahí se reescribe la información.	El disco Duro del DVR no cuenta con el suficiente espacio para almacenar más de videos.	Adquirir un nuevo DVR o ampliar el disco duro para aumentar los días de grabado.	
032	La Cámara de comercio cuenta con alarmas, pero no están monitoreadas por alguna estación central.	Desconocimiento o exceso de confianza	Incluir en la Política, la obligatoriedad de tener monitoreada la alarma por un ente central.	
033	No está documentada la ubicación de la alarma de detección de humo y tampoco está conectada a la central de bomberos	Inconsistencias en el diseño del plan de emergencias y evacuación.	Actualizar el plan de emergencias y evacuación.	
034	No existen sistemas de supresión de fuego	No hay implementado un plan de contingencia.	Desarrollar un plan de contingencia.	
035	El lugar donde está ubicado el Data Center, sólo cuenta con una puerta como control de acceso, no utiliza sistemas biométricos y tampoco cuenta con controles de temperatura y humedad.	Falta de políticas de seguridad de la información, de plan de contingencia y de inversión.	Implementar las políticas de seguridad de la información y plan de contingencia.	
036	La Cámara de Comercio de Aguachica, no cuenta con fuentes de poder separadas para cada equipo de cómputo, tiene instalada una UPS de 1KW con capacidad de 15 min, que es utilizada para los dispositivos de	No existe plan de contingencia.	Desarrollar un plan de contingencia.	

	red, servidores y tres equipos computo. A esta UPS, no se le realizan pruebas.		
037	No existe medidas de seguridad que garanticen la continuidad del suministro eléctrico	No tienen plan de contingencia. No existe planta eléctrica en la Cámara de Comercio de Aguachica	Adquirir una Planta Eléctrica. Establecer mecanismos para poder continuar sin el fluido eléctrico.
038	No existen procedimientos para la eliminación de manera segura de información o dispositivos de cómputo. Cuando ya no es útil es alojada aun archivador físico o los dispositivos de cómputo se donan.	Falta de procedimientos para controlar, la información y dispositivos que no son utilizados.	Desarrollar un comité de calidad y actualizar las políticas de seguridad de la información que contemplen esta parte.
039	No existe control interno, o alguien que haga sus veces para verificar que se realizan los procedimientos como así están estipulados.	No existe control Interno	Establecer el control interno en la CC de Aguachica
040	No existe protección contra código malicioso	No cuentan con herramientas especializadas para este tipo de inconvenientes.	Adquirir nuevas herramientas de seguridad de la información e implementar las Políticas de Seguridad de la información.
041	No existe un procedimiento que para realizar las copias de seguridad y tampoco que indique la manera de restauración. Actualmente se realizan copias pero sin seguir un procedimiento y sin saber cómo restaurar en caso de pérdida de información.	Falta de un comité de seguridad y de las Políticas de Seguridad de la información. Falta de plan de contingencia.	Desarrollar un procedimiento para poder saber con certeza como realizar las copias y restauración de la información.
042	No se lleva un registro de actividades y supervisión y nunca se han realizado auditorias de Sistemas.	Falta de personal Capacitado en el área de Auditoria, y no le dan importancia a los registros de supervisión y actividades.	Desarrollar un plan de auditorías y concienciar a los funcionarios encargados del área de la importancia de llevar registros de las actividades y supervisión.
043	La CC de Aguachica, no dispone de políticas de gestión y control de las redes para proteger la información en sistemas y aplicaciones.	Falta de políticas dentro de la CC que indiquen como se deben gestionar los procesos.	Implementación de las Políticas de Seguridad de la información.
044	No existe ninguna documentación de los mecanismos de seguridad ni tampoco de los niveles de prestación y los requisitos de gestión de seguridad de los servicios de red.	Falta de Comité de sistemas de gestión. Falta de comité de seguridad de la información. Falta de control Interno	Nombrar los diferentes comités y exigir la creación de políticas internas para establecer los mecanismos de seguridad de la red y los requisitos de gestión de la misma y documentarlos.

045	No se documentan, ni revisan los requisitos para acuerdos de confidencialidad o no divulgación para la protección de la información.	Falta de control interno. Falta de Políticas de Seguridad de la información.	Definir las políticas de seguridad de la información e implementarlas.
046	La CC de Aguachica no dispone de ninguna herramienta para filtrar contenido web.	Falta de disposición económica para la adquisición de un sistema de protección, como Firewalls.	Incluir dentro del presupuesto, la necesidad de adquirir un sistema de filtrado web.
047	Gestión de requerimientos para adquirir nuevos sistemas de información o mejorar los existentes.	Falta de planeación	Planear y gestionar los requerimientos que contribuyan a la toma de decisiones en el momento de adquirir nuevos sistemas de información o mejorar los existentes
048	No se garantizan las características fundamentales de la seguridad de la información en las aplicaciones.	No se estiman los riesgos inherentes a la información y el valor que ésta tiene para la organización	Tipificar, clasificar la información que se transmite hacia y desde la red y que opera bajo las plataformas organizacionales
049	No existe un procedimiento de control formal para realizar cambios a los sistemas	Desconocimiento de la importancia de identificar los activos de la organización, sus funciones y su utilización	Documentar detalladamente todo el proceso de adquisición y mantenimiento y cambios en los sistemas
050	No se realiza supervisión y seguimiento de sistemas contratados externamente	Falta de Gestión y pertinencia a las contrataciones	Mantener de manera organizada el proceso de seguimientos a las diferentes contrataciones.
051	En la política de seguridad de la información existente, no se contempla la relación con los suministradores ni gestión de riesgos presentes en este proceso	No se contempla el proceso de adquisición como factor importante de la seguridad de la información	Ampliar el alcance y contemplar factores estratégicos en la política de seguridad de la información
052	Falta documentación y control de servicios prestados por terceros	No se contempla como proceso importante tener seguimiento de los temas que tienen que ver con terceros	Plantear dentro de las políticas y gestión de riesgos la trazabilidad de procesos con terceros.
053	No se realiza gestión de incidentes de seguridad de la información	No se tiene en cuenta como factor de riesgo el control y reporte de los incidentes asociados a la seguridad de la información	Contemplar en la política de seguridad de la información los incidentes de seguridad y cómo actuar sobre estos.
054	La cámara de comercio de Aguachica no cuenta con un plan de contingencia y de manejo de accidentes, incidentes en caso de desastres naturales o cualquier otro fallo de seguridad y de operaciones	No existe plan de contingencia	Realizar el plan de contingencia y aplicar medidas de seguridad y continuidad del negocio
055	No se realizan con frecuencia respaldos de información ni copias de seguridad de la configuración del servidor y de los equipos activos de red.	El jefe de sistema no tiene programada la realización de Backups mensual como lo indico en la entrevista	Realizar un plan para la realización de Backup

056	No se contemplan procesos de cifrado de información sensible de la organización	Falta mayor incorporación de las políticas de seguridad de la información	Actualizar las Políticas de seguridad de la información mejoradas y gestión de riesgo
057	No se revisa ni se actualizan periódicamente elementos que puedan mejorarse en la política de seguridad de la información	Falta de concientización por parte del personal encargado y de valoración de la información como activo vital de la empresa	Revisar periódicamente de manera documentada y organizada las política de seguridad de la información

Elaborado (Nombre y Firma) Alex Meneses Martínez Erney Alberto Ramírez Camargo María Alejandra Merchán Villalba Yaditza Suarez de la Cruz	**Aprobó (Nombre y Firma)** Alex Meneses Martínez Erney Alberto Ramírez Camargo María Alejandra Merchán Villalba Yaditza Suarez de la Cruz

Fuente: Autores del proyecto.

Dictamen. Oficio de entrega del dictamen, ver **Apéndice D**

Tabla 11. Dictamen

Aguachica - Cesar, 07 de Junio 2016 Dr. EDUARDO SOLANO FORERO Director Ejecutivo Cámara de Comercio
Aguachica Presente: Debido a las constantes falencias que se presentan en cuanto a la seguridad de la información y de acuerdo a los lineamientos establecidos por la dirección general, se emite ante usted de manera oficial el resultado obtenido en el proceso de Auditoria, la cual se practicó en la oficina de Sistemas de la Cámara de Comercio de Aguachica, con el fin de evaluar el estado actual de la seguridad de la información en dicha dependencia en donde usted figura como Director Ejecutivo de la entidad, la cual se llevó a cabo desde el 25 de mayo de 2016 al 05 de junio de 2016. De las deducciones obtenidas durante la evaluación se le comunica a usted las siguientes observaciones:

Se efectuaron labores de auditoría sobre el uso que se le da a las tecnologías de la información y a los sistemas de información como parte del proceso que apoya a todos los procesos misionales de la Cámara de Comercio de Aguachica, comprendiendo la seguridad de la información desde la estructura organizacional, el esquema físico y lógico de la red, la manera como se salvaguarda la información y los recursos de software y hardware que soportan el área para el correcto funcionamiento, basado en el estándar ISO/IEC 27001: 2013; se realizó un análisis a la información recolectada y observada, a través de instrumentos como: entrevistas, observación directa, listas de verificación y encuesta; se dictaminó que las medidas que se emplean actualmente en esta área son carentes de políticas establecidas por las directivas de la entidad que tengan como finalidad reglamentar las áreas y proteger la información que es el activo más importante de las organizaciones y por ende cumplir los objetivos misionales de la institución. Comprendiendo lo anterior se hace mención de manera general de las inconsistencias que se presentan actualmente, comenzando desde la estructura organizacional entendiendo que la información manejada por los usuarios es el eslabón más débil de la cadena, con esto encontramos como primera falla lo relacionado a los cargos y funciones, existe un manual de funciones que no está actualizado y no es del conocimiento de los funcionarios, uno de los inconvenientes detectados por la anterior falla es que existe un responsable de la seguridad pero este no ha sido nombrado oficialmente con esta nueva función, lo que puede generar descuido por parte del funcionario al no tener encargado de manera formal esta labor, además no se notifican los accidentes en la seguridad de la información.

Seguido a esto se evidenció que el tratamiento que se le da a la información no es el adecuado debido a que existe un manual de políticas de seguridad de la información pero no está implementado, ni actualizado, además al no realizar capacitaciones a los funcionarios, ellos desconocen de buenas prácticas de seguridad de la información, lo que pone en riesgo la integridad, confidencialidad y disponibilidad del insumo principal de la empresa que es la información de los comerciantes; además no se contempla dentro del manual de políticas de seguridad de la información las fases de los empleados como son antes del ingreso, durante el empleo y el retiro de la entidad, es de suma importancia incluirlos comprendiendo que el empleado maneja la información de la Cámara de Comercio.

La información se debe clasificar de acuerdo a la criticidad y al grado de importancia que tenga dentro de la entidad, no se encuentran documentadas e implementadas reglas para el uso de información y activos de información. Se deben crear procedimientos para realizar labores como: copias de seguridad de la información, restauración y demás procesos que carecen de los mismos, necesitan de un responsable de las operaciones que esté al tanto de las funciones realizadas.

La cámara de comercio no tiene un plan de contingencia y planes de emergencia que especifiquen que se debe realizar en momentos de crisis; carece de mecanismos para garantizar el fluido eléctrico como UPS de mayor capacidad, planta eléctrica; también existe carencia en los dispositivos y herramientas para administrar la red de datos y proteger los equipos de software maliciosos. Otras desviaciones encontradas es que las cámaras de seguridad no gravan lo suficiente, no son reportados los cambios realizados a dispositivos electrónicos e instalaciones físicas, se requiere control con el manejo de medios removibles como USB, CD, DVD, además faltan políticas para la eliminación controlada de información en estos medio y tampoco existe

control para dar de baja por finalizado el uso de un dispositivo electrónico que contenga información de la entidad.

Existen falencias en la seguridad física de las instalaciones, no se realiza acompañamiento del personal a los diferentes despachos, no existe ningún control de acceso excepto la puerta de entrada, además las alarmas no están conectadas a un nodo central como la policía, no existe dentro de los planos la ubicación de las alarmas anti humo, no están conectadas a los bomberos y el archivo y cuarto de telecomunicaciones están ubicadas debajo de un baño, exponiendo la información física y logia de la entidad; el cuarto de telecomunicaciones no posee controles de temperatura ni humedad.

Comprendiendo las situaciones detectadas y con el fin de mejorar los procesos, ofrecer un mejor servicio y garantizar las características de la seguridad de la información como primera medida es necesario la reestructuración, aprobación e implementación de las Políticas de Seguridad que contemple la seguridad de la información desde el aspecto organizacional, que involucre las normativas en las funciones a los empleados y demás aspectos mencionados anteriormente, seguido a esto es necesario desarrollar un plan de realización de copias de seguridad y restauración; la infraestructura física y lógica es esencial para soportar los procesos de la Cámara de Comercio de Aguachica, por esto se recomienda la elaboración de un plan de contingencia, planes de emergencia y análisis de riesgo, para tener identificados los puntos débiles y tener las medidas necesarias para reducir los niveles de riesgos. Se hace necesario la iniciativa de la alta gerencia en cuanto a directrices y lineamientos que enmarquen todo el contexto organizacional y de esta manera se acojan todas las estancias administrativas.

Atentamente,
Alexander Meneses Martínez
Erney Ramírez Camargo
María Alejandra Merchán Villalba
Yaditza Suarez de la Cruz

Fuente: Autores del proyecto.

4.2. Los riesgos asociados al uso de las tecnologías de la información y la comunicación a partir de metodologías para la identificación, análisis y evaluación de amenazas, vulnerabilidades e impactos.

4.2.1. Reconocer, analizar y evaluar el riesgo. Con el transcurrir de los tiempos la información de la Cámara de Comercio de Aguachica, Cesar, ha pasado de ser el resultado de desarrollo de las actividades y procesos a ser un insumo de alto valor, fundamental para el

cumplimiento de los objetivos, metas y subsistencia de las mismas, con el objeto de brindar eficiencia y agilizar la administración, los procesos, incorporan la utilización de sistemas automatizados de procesamiento de información.

Hoy, la relevancia que ha tomado la información, no eximió a la Cámara de Comercio de Aguachica, Cesar, de una serie de amenazas, que se han incrementado por las nuevas vulnerabilidades que han surgido del uso de tecnologías de la información y las comunicaciones. De esta manera, la Entidad, se encontró constantemente expuesta a una serie de riesgos, resultando complejo establecer un entorno totalmente seguro.

La gestión de riesgos se tomó como una de las actividades más importantes para salvaguardar los activos de información de la institución, por consiguiente, garantizó cumplir la capacidad de los principales objetivos. En el diseño del sistema de gestión de seguridad de la información (SGSI) que está dirigido para los Procesos Soportados por el Área de Sistemas en la Cámara de Comercio de Aguachica, Cesar, se buscó con la utilización de metodologías de tratamiento de riesgo tales como la MAGERIT V3, desarrollada por el Ministerio de Hacienda y Administraciones Públicas de España, garantizar a esta entidad a tener una visión clara y especifica de la identificación de los riesgos potenciales a los cuales están expuesta a diario, con la misión de minimizar la ocurrencia del mismo.

Las necesidades actuales de la Cámara de Comercio es identificar claramente el riesgos al que están expuestos sus activos, con esto determinar la importancia del diseño del Sistema de Gestión de Seguridad, por este motivo no se abarco el tratamiento del riesgo y tampoco se siguió

paso a paso la metodología Magerit, realizamos un análisis de riesgo cualitativo, el cual busca saber qué es lo que hay sin cuantificarlo con precisión; en donde determinamos el impacto y riesgo potencial, asociados a los activos y no tuvimos en cuanta la dependencia de los activos ni el riesgo acumulado ni repercutido, debido a que las necesidades actuales de la cámara conciernen a la identificación del riesgo y salvaguardas.

Los problemas asociados a la seguridad de la información alcanzan a todo tipo de organización. En particular, a la Cámara de Comercio de Aguachica, la cual maneja grandes volúmenes de información, que por su variedad e importancia la hacen blanco de ataques.

La figura a continuación, recoge de una manera clara el proceso de análisis de riesgos.

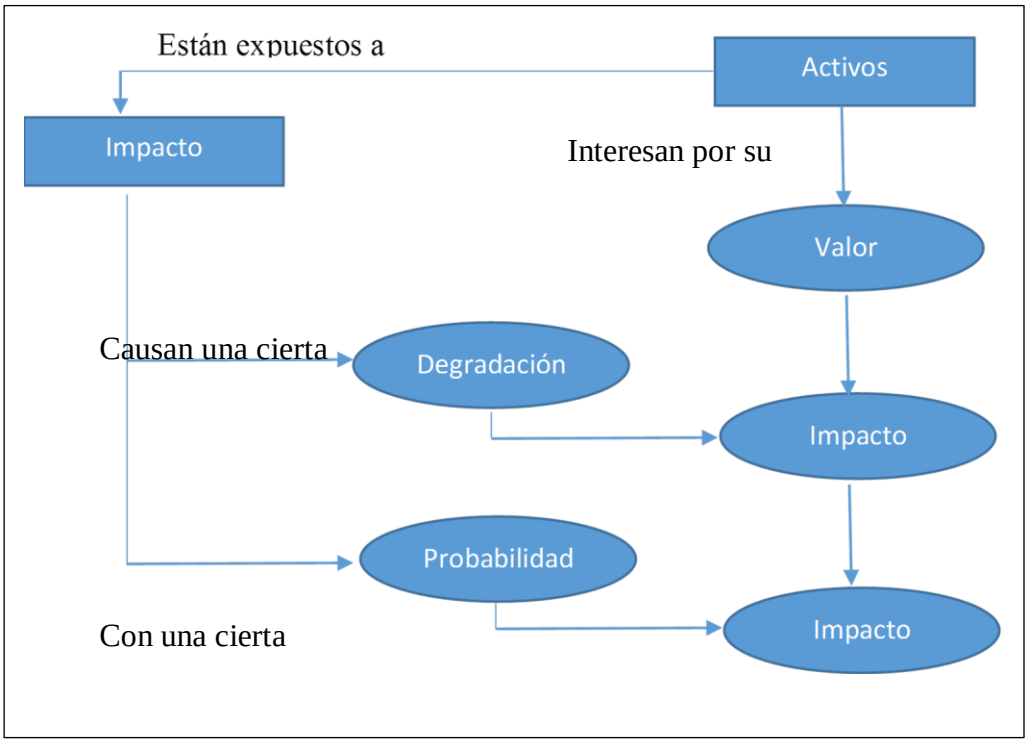

Figura 4. Flujo del análisis de riesgos potenciales, basado de Magerit V3, Libro 1 métodos.
Fuente: Autores del proyecto.

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados, utilizaremos MAGERIT, es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España. Actualizada en 2012 en su versión 3.

El análisis de riesgo se lleva a cabo por medio de las siguientes tareas:

- Caracterización de los activos
    - Identificación de los activos
    - Valoración de los activos
        - Dimensión
- Caracterización de las amenazas
    - Identificación de las amenazas
    - Valoración de las amenazas
- Caracterización de las salvaguardas
    - Identificación de las salvaguardas pertinentes
- Estimación del estado de riesgo
    - Estimación del impacto potencial
    - Estimación del riesgo potencial

En otras palabras se realiza lo siguiente:

1. determinar los activos relevantes para la Organización, su interrelación y su valor, en el

sentido de qué perjuicio (coste) supondría su degradación

2. determinar a qué amenazas están expuestos aquellos activos
3. determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Caracterización de Activos

Identificación de activos de información

Alcance: la gestión de la seguridad de la información dentro de la Cámara de Comercio de Aguachica, será administrada a través de sus activos de información, todos aquellos recursos de valor para la entidad que generan, procesan, almacenan o transmiten información.

Los activos están conformados por:

1. Información y datos, compuesto por todos los elementos generados por parte de la institución y por quienes la conforman; dichos componentes pueden ser tangibles y/o digitales.

2. Funciones del área de sistemas que soporta los procesos de la Cámara de Comercio de Aguachica, todas aquellas actividades que son efectuadas por el departamento de

sistemas de la cámara de comercio de Aguachica, están enmarcados en las siguientes actividades:

Tabla 12. Actividades efectuadas por el departamento de sistemas de la cámara de comercio de Aguachica, Cesar.

Arquitectura del sistema (arch)	
(ip)	Router Board Mikrotik de UNE
(sap)	Modem Huawei de UNE
(ext)	Multiservice Gateway Allied Telesis, Equipo de Confecámaras
(ip)	Router Cisco 1700
(ext)	Modem Miltrastar de Movistar 4 m
(ext)	Modem Nukon de Movistar 2 m
Información (D)	
(int)	información de registro
(int)	Información contable
(int)	Información administrativa
(Backup)	Copias de respaldo de la información de registro, administrativa y financiera.
(Conf)	Datos de configuración
(int)	Datos de gestión interna (usuarios, permiso)
(log)	Registro de actividades
Claves criptográficas (keys)	
(Sign)	Firma digital
Servicios (s)	
(email)	Correo electrónico empresarial
(ext)	Soporte a usuarios externos (manejo de trámites en línea) a través de chat online y vía telefónica.
(int)	Gestión de privilegios en los sistemas de información SII y DocuWare
(ftp)	Servicio de transferencia de fichero FTP hacia el servidor SIREP
(ext)	Servicio de registros públicos a usuarios externos a través de la web
(int)	Servicio de registros públicos a usuarios internos.
(int)	Servicio radicación y consulta de expedientes digitalizados a usuarios internos.
Aplicaciones informáticas (sw)	
(sub)	SIREP

(sub)	DocuWare
(sub)	SII
(sub)	Jsp7
(office)	Microsoft Office Hogar y Empresa 2013
(av)	Antivirus kaspersky
(email_server)	Cpanel, administrador de Servidor de correo electrónico y pagina web.
(dbms)	SQL Server 2012 Sistema de Gestión de Base de Datos
(browser)	Mozilla Firefox 47.0.1
(browser)	Google Chrome
(SO)	Windows Server 2012
(SO)	Windows 8.1
(SO)	Windows 8
(SO)	Windows 7 professional
Equipamiento informático (HW)	
(host)	Servidor hp prolian
(Peripheral) (print)	Impresoras Lexmark, Hp, Xerox
(Peripheral) (scan)	Escáner Fujitsu 7160, 6140, 6770
(Network) (modem)	Switch hp v1910
(Network) (modem)	Switch Planet FNSW 2401
(Network) (modem)	Switch 3Com 4200
(wap)	Access Point Ubiquiti
(pabx)	Planta Telefónica
(mid)	DVR Gsecurity
(pc)	Computador personal
(mobile)	Celular empresarial
Redes de comunicaciones (com)	
(lan)	Red Local
(wifi)	Red Inalámbrica
(psnt)	Red telefónica
(internet)	Internet banda ancha 4 m
(internet)	Internet banda ancha 2 m
(internet)	Internet dedicado 8 m
Soportes de información (media)	
(disk)	Disco duro extraíble de 1 T
(usb)	Memorias USB
(dvd)	DVD de respaldo
Equipamiento auxiliar (aux)	
(ac)	Aire Acondicionado
(ups)	1 UPS de 1Kva
(cabling)(fiber)	Cableado en fibra optica
(cabling)(wire)	Cableado eléctrico

(furmiture)	Escritorios
(furmiture)	Rack de piso de 24 u
Instalaciones (L)	
(building)	Edificio
Persona (p)	
(ue)	Comerciantes y población en general
(Adm)	Director Administrativo y Financiero Ingeniero de Sistemas Coordinadora de Sistemas
(dba)	Ingeniero de Sistemas
(op)	Jefe de Archivo Mileydis Fonseca, Auxiliar de Archivo Yuri Gonzales, Auxiliar de Archivo Harold Pacheco, Auxiliar de Archivo Jefe de Caja Piedad, Auxiliar de Caja Auxiliar de Caja Auxiliar de Registro Asistente de Registros Publico Jefe de Registros Públicos Juridico Jefe de Conciliación Secretaria General Coordinadora de Desarrollo Empresarial Asistente Administrativa y Contable
(pro)	CertiCámara s UNE Movistar ConfeCámara s
(Dev)	Confecámaras
(ui) servicios generales	Servicios generales

Fuente: Autores del proyecto.

Valoración de Activos. "La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes." Pág. 24 de métodos magerit

Tabla 13. Criterios de valoración.

Criterios de Valoración	
Valor	**Criterio**
MA	Muy alto
A	Alto
M	Medio
B	Bajo
MB	Muy Bajo

Fuente: Autores del proyecto

Dimensiones de valoración

(D)Disponibilidad

(I) Integridad

(C) Confidencialidad

(A) Autenticidad

(T) Trazabilidad

Tabla 14. Valoración de activos.

	Dimensiones				
Activos	**D**	**I**	**C**	**A**	**T**
Arquitectura					
Router Board Mikrotik de UNE	A	A	A	M	B
Modem Huawei de UNE	MA	A	A	M	B
Multiservice Gateway Allied Telesis, Equipo de Confecámaras	MA	MA	M	M	B
Router Cisco 1700	MA	MA	M	M	B
Modem Miltrastar de Movistar 4 m	A	A	A	M	B
Modem Nukon de Movistar 2 m	A	A	A	M	B
Información					
información de registro	MA	MA	MB	A	A

Información contable	MA	MA	A	A	A
Información administrativa	A	A	B	A	A
Copias de respaldo de la información de registro, administrativa y financiera.	A	A	MB	B	MB
Datos de configuración	A	A	B	MB	MB
Datos de gestión interna (usuarios, permiso)	A	MA	M	M	M
Registro de actividades	M	M	B	B	M
Claves criptográficas					
Firma digital	A	MA	A	M	B
Servicios					
Correo electrónico empresarial	A	A	MA	A	M
Soporte a usuarios externos (manejo de trámites en línea) a través de chat online y vía telefónica.	A	M	MB	MB	MB
Gestión de privilegios en los sistemas de información SII y DocuWare	A	A	B	M	B
Servicio de transferencia de fichero FTP hacia el servidor SIREP	MA	MA	M	M	B
Servicio de registros públicos a usuarios externos a través de la web	A	A	B	MB	M
Servicio de registros públicos a usuarios internos.	MA	MA	A	A	M
Servicio radicación y consulta de expedientes digitalizados a usuarios internos.	A	A	M	M	M
Aplicaciones informáticas					
SIREP	MA	MA	M	M	M
DocuWare	A	A	M	M	M
SII	MA	MA	M	M	M
Jsp7	MA	MA	A	A	A
Microsoft Office Hogar y Empresa 2013	B	B	MB	MB	MB
Antivirus kaspersky	B	B	MB	MB	MB
Cpanel, administrador de Servidor de correo electrónico y pagina web.	M	B	M	M	M
SQL Server 2012 Sistema de Gestión de Base de Datos	A	MA	B	M	M
Mozilla Firefox 47.0.1	MB	MB	MB	MB	MB
Google Chrome	MB	MB	MB	MB	MB
Windows Server 2012	MA	A	A	M	M
Windows 8.1	A	B	MB	B	MB
Windows 8	A	B	MB	B	MB
Windows 7 professional	A	B	MB	B	MB
Equipamiento informático					
Servidor hp proliant	MA	MA	M	M	B
Impresoras Lexmark, Hp, Xerox	A	M	MB	MB	MB

Escáner Fujitsu 7160, 6140, 6770	A	M	MB	MB	MB
Switch hp v1910	MA	MA	MB	B	B
Switch Planet FNSW 2401	MA	MA	MB	B	B
Switch 3Com 4200	MA	MA	MB	B	B
Access Point Ubiquiti	MB	MB	MB	MB	MB
Planta Telefónica	A	A	A	MB	MB
DVR Gsecurity	M	M	M	M	MB
Computador personal	A	M	B	M	MB
Celular empresarial	M	B	B	MB	MB
Redes de comunicaciones					
Red Local	MA	A	A	M	M
Red Inalámbrica	M	B	M	B	MB
Red telefónica	A	A	B	MB	MB
Internet banda ancha 4 m	MA	A	MB	MB	MB
Internet banda ancha 2 m	MA	A	MB	MB	MB
Internet dedicado 8 m	MA	A	MB	MB	MB
Soportes de información					
Disco duro extraíble de 1 T	A	A	MB	MB	MB
Memorias USB	MB	MB	MB	MB	MB
DVD de respaldo	A	A	MB	MB	MB
Equipamiento auxiliar					
Aire Acondicionado	M	B	MB	MB	MB
1 UPS de 1Kva	A	M	MB	MB	MB
Cableado en fibra óptica	MA	A	MB	MB	MB
Cableado eléctrico	MA	MB	MB	MB	MB
Escritorios	M	MB	MB	MB	MB
Rack de piso de 24 u	MB	MB	MB	MB	MB
Instalaciones					
Edificio	MA	A	MB	MB	MB
Personal					
Comerciantes y población en general	A	MB	MB	MB	MB
Director Administrativo y Financiero Ingeniero de Sistemas Coordinadora de Sistemas	M	MB	A	MB	MB
Ingeniero de Sistemas	M	MB	A	MB	MB
Jefe de Archivo, Auxiliar de Archivo Auxiliar de Archivo Auxiliar de Archivo Jefe de Caja Auxiliar de Caja Auxiliar de Caja Auxiliar de Registro Asistente de Registros Publico Jefe de Registros Públicos	B	MB	M	MB	MB

Jurídico Jefe de Conciliación Secretaria General Coordinadora de Desarrollo Empresarial Asistente Administrativa y Contable					
CertiCámara s UNE Movistar ConfeCámara s	M	MB	M	MB	MB
Confecámaras	M	MB	M	MB	MB
Servicios generales	MB	MB	B	MB	MB

Fuente: autores del proyecto.

Caracterización de las amenazas. Las amenazas fueron clasificadas de acuerdo a lo que dispone la metodología Magerit v3, se realiza de la siguiente manera:

(N) Desastres Naturales

(I) De origen Industrial

(E) Errores y Fallos no intencionados

(A) Ataques intencionados

Identificación de las amenazas. En la siguiente tabla se identifican las amenazas para cada activo, pero en muchas ocasiones para varios activos recaen las mismas amenazas, decidimos agrupar los activos a los cuales le pueden afectar las mismas amenazas.

Tabla 15. Identificación de amenazas para cada activo.

ACTIVOS	**AMENAZAS**
*Router Board Mikrotik de UNE. *Modem Huawei de UNE. *Multiservice Gateway Allied	**[E.15] Alteración de la información**
	[E.18] Destrucción de la información
	[E.19] Fugas de Información

Telesis, Equipo de Confecámaras. *Router Cisco 1700. *Modem Miltrastar de Movistar 4 m. *Modem Nukon de Movistar 2 m	**[A.5] Suplantación de identidad**
	[A.11] Acceso no Autorizado
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de información
*Información de registro. *Información contable. *Información administrativa	**[E.1] Errores de los usuarios**
	[E.2] Errores del Administrador de sistema / de la seguridad
	[E.15] Alteración de la información
	[E.19] Fugas de Información
	[A.5] Suplantación de identidad
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de información
Copias de respaldo de la información de registro, administrativa y financiera.	**[E.1] Errores de los usuarios**
	[E.2] Errores del Administrador de sistema / de la seguridad
	[E.15] Alteración de la información
	[E.18] Destrucción de la información
	[E.19] Fugas de información
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de información
Datos de configuración Datos de gestión interna (usuarios, permiso)	**[E.1] Errores de los usuarios**
	[E.2] Errores del Administrador de sistema / de la seguridad
	[E.18] Errores de configuración
	[E.15] Alteración de la información
	[E.18] Destrucción de la información
	[E.19] Fugas de Información
	[A.4] Manipulacion de los ficheros de configuración
	[A.5] Suplantación de la identidad

	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
	[A.15] Modificación de la información
	[A.19] Revelación de información
Registro de actividades	**[E.1] Errores de los usuarios**
	[E.2] Errores del Administrador de sistema / de la seguridad
	[E.3] Errores de monitorización (log)
	[E.15] Alteración de la información
	[E.18] Destrucción de la información
	[E.19] Fugas de Información
	[A.3] Manipulación de los registros de actividad (log)
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
	[A.13] Repudio (negación de actuaciones)
	[A.15] Modificación de la información
	[A.19] Revelación de información
Firma digital	**[E.1] Errores de los usuarios**
	[E.2] Errores del Administrador de sistema / de la seguridad
	[E.19] Fugas de información
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
	[A.19] Revelación de información
Correo electrónico empresarial	**[I.9] Interrupción de otros servicios o suministros esenciales**
	[E.15] Alteración de la información
	[E.18] Destrucción de la información
	[E.19] Fugas de información
	[A.5] Suplantación de la identidad
	[A.13] Repudio (negación de actuaciones)
	[A.15] Modificación de la información
	[A.19] Relevación de información
	[A.24] Denegación de servicio
Soporte a usuarios externos	**[E.1] Errores de los usuarios**

(manejo de trámites en línea) a través de chat online y vía telefónica. Gestión de privilegios en los sistemas de información SII y DocuWare Gestión de privilegios en los sistemas de información SII y DocuWare Servicio de transferencia de fichero FTP hacia el servidor SIREP Servicio de registros públicos a usuarios externos a través de la web Servicio de registros públicos a usuarios internos. Servicio radicación y consulta de expedientes digitalizados a usuarios internos.	**[E.2] Errores del administrador del sistema / de la seguridad**
	[E.15] Alteración de la información
	[E.18] Destrucción de la información
	[E.19] Fugas de información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.11] Acceso no autorizado
	[A.13] Repudio (negación de actuaciones)
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de la información
	[A.24] Denegación de servicio
*SIREP. *DocuWare. *SII. *Jsp7. *Microsoft Office Hogar y Empresa 2013. *Antivirus kaspersky. *Cpanel, administrador de Servidor de correo. electrónico y pagina web. *SQL Server 2012 Sistema de Gestión de Base de Datos *Mozilla Firefox 47.0.0 *Google Chrome. *Windows Server 2012. *Windows 7, 8.1 y 8.	**[I.5] Avería de origen físico o lógico**
	[E.1] Errores de los usuarios
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.8] Difusión de software dañado
	[E.15] Alteración de la información
	[E.18] Destrucción de la información
	[E.19] Fugas de información
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)
	[A.5] Suplantación de identidad
	[A.6] Abuso de privilegios de acceso
	[A.8] Difusión de software dañino
	[A.11] Acceso no autorizado
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de información
	[A.22] Manipulación de programas
*Servidor hp proliant. *Impresoras Lexmark, Hp, Xerox.	**[N.1] Fuego**
	[N.2] Daños por agua

*Escáner Fujitsu 7160, 6140, 6770. *Switch hp v1910. *Switch Planet FNSW 2401. *Switch 3Com 4200. *Access Point Ubiquiti. *Planta Telefónica. *DVR Gsecurity. *UPS StarUPS APC 2200. *Computador personal. *Celular empresarial.	**[I.*] Desastres industriales**
	[I.3] Contaminación medioambiental
	[I.4] Contaminación electromagnética
	[I.5] Avería de origen físico o lógico
	[I.6] Coste del suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[I.11] Emanaciones electromagnéticas
	[I.2] Errores del administrador del sistema/ de la seguridad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[E.24] Caída del sistema por agotamiento de recursos
	[E.25] Perdida de equipos
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.11] Acceso no autorizado
	[A.23] Manipulación del hardware
	[A.24] Denegación de servicio
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
Red Local	**[I.8] Fallo de servicios de comunicaciones**
	[E.9] Errores de re-encaminamiento
	[E.10] Errores de secuencia
	[A.5] Suplantación de identidad del usuario
	[A.9] Re-encaminamiento de mensajes
	[A.10] Alteración de secuencia
	[A.11] Acceso no autorizado
	[E.2] Errores del administrador del sistema / de la seguridad
	[A.18] Destrucción de la información
Red Inalámbrica	**[I.8] Fallo de servicios de comunicaciones**
	[E.9] Errores de re-encaminamiento
	[A.5] Suplantación de identidad del usuario
	[A.12] Análisis de tráfico
	[A.10] Alteración de secuencia

	[E.2] Errores del administrador del sistema / de la seguridad
	[A.18] Destrucción de la información
Red telefónica	**[E.9] Fugas de información**
	[A.14] Interceptación de información (escucha)
	[1.3] Contaminación medioambiental
	[1.3.3] Polvo
	[I.8] Fallo de servicio de comunicaciones
	[A.25] Robo de equipos
*Internet banda ancha 4 m *Internet banda ancha 2 m *Internet dedicado 8 m	**[I.8] Fallo de servicios de comunicación**
	[E.9] Fugas de información
	[A.14] Interceptación de información (escucha)
	[1.3] Contaminación medioambiental
	[1.3.3] Polvo
	[I.8] Fallo de servicio de comunicaciones
	[A.25] Robo de equipos
	[E.24] Caída del sistema por agotamiento de recursos
*Disco duro extraíble de 1 T. *Memorias USB. *DVD de respaldo.	**[N.1] Fuego**
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.*] Desastres industriales
	[I.3] Contaminación medioambiental
	[I.4] Contaminación Electromagnética
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[I.10] Degradación de los soportes de almacenamiento de la información
	[E.18] Destrucción de la información
	[A.11] Acceso no autorizado
	[A.15] Modificación de la información
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
	[A.19] Revelación de información
Aire Acondicionado	**[N.1] Fuego**
	[N.2] Daños por agua
	[N.*] Desastres naturales

	[I.*] Desastres industriales
	[I.3] Contaminación medioambiental
	[I.6] Corte del suministro eléctrico
	[I.9] Interrupción de otros servicios o suministros esenciales
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[A.23] Manipulación de hardware
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
UPS de 1Kva	**[N.1] Fuego**
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.*] Desastres industriales
	[I.3] Contaminación medioambiental
	[I.9] Interrupción de otros servicios o suministros esenciales
	[A.23] Manipulación de hardware
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
*Cableado en fibra óptica. * Cableado eléctrico	**[N.1] Fuego**
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.*] Desastres industriales
	[I.3] Contaminación medioambiental
	[I.4] Contaminación electromagnética
	[I.11] Emanaciones electromagnéticas
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[A.11] Acceso no autorizado
	[A.23] Manipulación de hardware
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
Escritorios	**[N.1] Fuego**
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.*] Desastres industriales
	[I.3] Contaminación medioambiental

	[A.23] Manipulación de hardware
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
Rack de piso de 24 u	**[N.1] Fuego**
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.*] Desastres industriales
	[I.3] Contaminación medioambiental
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
Edificio	**[N.1] Fuego**
	[N.2] Daños por agua
	[N.*.1] Tormentas
	[N.*.4] Terremotos
	[N.*.11] Calor extremo
	[I.*] Desastres industriales
	[A.27] Ocupación enemiga
*Comerciantes y población en general. *Director Administrativo y Financiero. *Ingeniero de Sistemas *Coordinadora de Sistemas. *Jefe de Archivo. *Jefe de Caja. *Auxiliar de Caja. *Auxiliar de Registro. *Asistente de Registros *Publico Jurídico. *Jefe de Conciliación. *Secretaria General. *Coordinadora de Desarrollo Empresarial. *Asistente Administrativa y Contable. *CertiCámaras. *UNE. *Movistar. *ConfeCámaras. *Servicios generales.	**[E.15] Alteración de la información**
	[E.19] Fugas de información
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de información
	[A.28] Indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería social (picaresca)

Fuente: autores del proyecto.

Valoración de las amenazas. Para valorar las amenazas de cada activo se han tomado en cuenta la degradación de valor y la probabilidad de ocurrencia.

1. Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo
2. Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse

Tabla 16. Rango porcentual de impacto o degradación en los activos para cada dimensión de seguridad

Rango porcentual de impacto o degradación en los activos para cada dimensión de seguridad	
Impacto	**Valor cuantitativo**
1% - 34%	Leve
35% - 68%	Media
69% - 100%	Alta

Fuente: Autores del proyecto

Tabla 17. Degradación.

Probabilidad de ocurrencia [P]	
MA	prácticamente seguro
A	probable
M	posible
B	poco probable
MB	muy raro

Fuente: Autores del proyecto

Tabla 18. Probabilidad de ocurrencia, basado en Magerit V3, Libro 3 guía de técnicas

ACTIVOS	AMENAZAS	[P]	[D]	[I]	[C]	[A]	[T]
*Router Board Mikrotik de UNE. *Modem Huawei de UNE. *Multiservice Gateway Allied Telesis, Equipo de Confecámaras. *Router Cisco 1700. *Modem Miltrastar de Movistar 4 m. *Modem Nukon de Movistar 2 m	**Total**		**50%**	**50%**	**50%**	**50%**	**0%**
	[E.15] Alteración de la información	M		10%			
	[E.18] Destrucción de la información	M	10%				
	[E.19] Fugas de Información	M			10%		
	[A.5] Suplantación de identidad	M		50%	50%	50%	
	[A.11] Acceso no Autorizado	M		50%	50%		
	[A.15] Modificación de la información	M		50%			
	[A.18] Destrucción de la información	M	50%				
	[A.19] Revelación de información	M			50%		
*Información de registro. *Información contable. *Información administrativa	**Total**		**50%**	**100%**	**100%**	**100%**	**0%**
	[E.1] Errores de los usuarios	MA	10%	10%	10%		
	[E.2] Errores del Administrador de sistema / de la seguridad	M	20%	20%	20%		
	[E.15] Alteración de la información	M		1%			
	[E.19] Fugas de Información	M			10%		
	[A.5] Suplantación de identidad	MA		10%	50%	100%	
	[A.6] Abuso de privilegios de acceso	MA	1%	10%	50%		
	[A.11] Acceso no autorizado	MA		10%	50%		
	[A.15] Modificación de la información	MA		100%			
	[A.18] Destrucción de la información	MA	50%				

	[A.19] Revelación de información	MA			100%		
Copias de respaldo de la información de registro, administrativa y financiera.	**Total**		**50%**	**100%**	**50%**	**100%**	**0%**
	[E.1] Errores de los usuarios	MA	10%	10%	10%		
	[E.2] Errores del Administrador de sistema / de la seguridad	M	20%	20%	20%		
	[E.15] Alteración de la información	M		1%			
	[E.18] Destrucción de la información	M	1%				
	[E.19] Fugas de información	M			10%		
	[A.5] Suplantación de la identidad	MA		10%	50%	100%	
	[A.6] Abuso de privilegios de acceso	MA	1%	10%	50%		
	[A.11] Acceso no autorizado	MA		10%	50%		
	[A.15] Modificación de la información	MA		100%			
	[A.18] Destrucción de la información	MA	50%				
	[A.19] Revelación de información	MA			100%		
*Datos de configuración *Datos de gestión interna (usuarios, permiso)	**Total**		**20%**	**100%**	**100%**	**100%**	**0%**
	[E.1] Errores de los usuarios	MA	10%	10%	10%		
	[E.2] Errores del Administrador de sistema / de la seguridad	M	20%	20%	20%		
	[E.18] Errores de configuración	M		1%			
	[E.15] Alteración de la información	M		1%			
	[E.18] Destrucción de la información	M	1%				
	[E.19] Fugas de Información	M			10%		

	[A.4] Manipulación de los ficheros de configuración	MA	10%	10%	10%		
	[A.5] Suplantación de la identidad	MA		10%	50%	100%	
	[A.6] Abuso de privilegios de acceso	MA	1%	10%	50%		
	[A.11] Acceso no autorizado	MA		10%	50%		
	[A.15] Modificación de la información	MA		100%			
	[A.19] Revelación de información	MA			100%		
	Total		**20%**	**100%**	**100%**	**100%**	**0%**
Registro de actividades	**[E.1] Errores de los usuarios**	MA	10%	10%	10%		
	[E.2] Errores del Administrador de sistema / de la seguridad	M	20%	20%	20%		
	[E.3] Errores de monitorización (log)	M		1%			
	[E.15] Alteración de la información	M		1%			
	[E.18] Destrucción de la información	M	1%				
	[E.19] Fugas de Información	M			10%		
	[A.3] Manipulación de los registros de actividad (log)	MA		50%			
	[A.5] Suplantación de la identidad	MA		10%	50%	100%	
	[A.6] Abuso de privilegios de acceso	MA	1%	10%	50%		
	[A.11] Acceso no autorizado	MA		10%	50%		
	[A.13] Repudio (negación de actuaciones)	MA		100%		100%	

	[A.15] Modificación de la información	MA		100%			
	[A.19] Revelación de información	MA			100%		
Firma digital	**Total**		**100%**	**20%**	**100%**	**100%**	**0%**
	[E.1] Errores de los usuarios	B	10%	10%	10%		
	[E.2] Errores del Administrador de sistema / de la seguridad	M	20%	20%	20%		
	[E.19] Fugas de información	M			50%		
	[A.5] Suplantación de la identidad	MA			100%	100%	
	[A.6] Abuso de privilegios de acceso	MA	100%		50%	50%	
	[A.11] Acceso no autorizado	MA			100%	100%	
	[A.19] Revelación de información	MA			100%		
Correo electrónico empresarial	**Total**		**50%**	**50%**	**100%**	**100%**	**100%**
	[I.9] Interrupción de otros servicios o suministros esenciales	M	50%				
	[E.15] Alteración de la información	M		10%			
	[E.18] Destrucción de la información	B	10%				
	[E.19] Fugas de información	B			10%		
	[A.5] Suplantación de la identidad	MA		20%	100%	100%	
	[A.13] Repudio (negación de actuaciones)	MB					100%
	[A.15] Modificación de la información	M		50%			
	[A.19] Relevación de información	M			50%		

	[A.24] Denegación de servicio	M	50%				
Soporte a usuarios externos (manejo de trámites en línea) a través de chat online y vía telefónica. *Gestión de privilegios en los sistemas de información SII y DocuWare Gestión de privilegios en los sistemas de información SII y DocuWare Servicio de transferencia de fichero FTP hacia el servidor SIREP *Servicio de registros públicos a usuarios externos a través de la web *Servicio de registros públicos a usuarios internos. *Servicio radicación y consulta de expedientes digitalizados a usuarios internos.	**Total**		**50%**	**50%**	**50%**	**100%**	**100%**
	[E.1] Errores de los usuarios	M	10%	10%	10%		
	[E.2] Errores del administrador del sistema / de la seguridad	A	20%	20%	20%		
	[E.15] Alteración de la información	A	50%	5%			
	[E.18] Destrucción de la información	M	10%				
	[E.19] Fugas de información	M			10%		
	[E.24] Caída del sistema por agotamiento de recursos	MA	50%				
	[A.5] Suplantación de la identidad	M		50%	50%	100%	
	[A.6] Abuso de privilegios de acceso	M	1%	10%	10%	100%	
	[A.7] Uso no previsto	M	1%	10%	10%		
	[A.11] Acceso no autorizado	M		10%	50%	100%	
	[A.13] Repudio (negación de actuaciones)	MA					100%
	[A.15] Modificación de la información	MA		50%			
	[A.18] Destrucción de la información	M	50%				
	[A.19] Revelación de la información	M			50%		
	[A.24] Denegación de servicio	MA	50%				

	Total		**50%**	**100%**	**100%**	**100%**	**0%**
	[I.5] Avería de origen físico o lógico	M	50%				
	[E.1] Errores de los usuarios	M	1%	10%	10%		
	[E.2] Errores del administrador del sistema / de la seguridad	M	20%	20%	20%		
	[E.8] Difusión de software dañado	A	10%	10%	10%		
*SIREP. *DocuWare. *SII. *Jsp7. *Microsoft Office Hogar y Empresa 2013. *Antivirus kaspersky. *Cpanel, administrador de Servidor de correo electrónico y pagina web. *SQL Server 2012 Sistema de Gestión de Base de Datos *Mozilla Firefox 47.0.0 *Google Chrome. *Windows Server 2012. *Windows 7, 8.1 y 8.	**[E.15] Alteración de la información**	M		1%			
	[E.18] Destrucción de la información	M	50%				
	[E.19] Fugas de información	M			10%		
	[E.20] Vulnerabilidades de los programas (software)	M	1%	20%	20%		
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	MA	5%	5%			
	[A.5] Suplantación de identidad	M		50%	50%	100%	
	[A.6] Abuso de privilegios de acceso	M	1%	10%	10%		
	[A.8] Difusión de software dañino	M	1%	10%	10%		
	[A.11] Acceso no autorizado	M		10%	50%		
	[A.15] Modificación de la información	M		50%			
	[A.18] Destrucción de la información	M	50%				
	[A.19] Revelación de información	M			50%		
	[A.22] Manipulación de programas	M	50%	100%	100%		

	Total		**100%**	**20%**	**100%**	**0%**	**0%**
	[N.1] Fuego	M	100%				
	[N.2] Daños por agua	M	50%				
	[I.*] Desastres industriales	M	100%				
	[I.3] Contaminación medioambiental	B	50%				
	[I.4] Contaminación electromagnética	M	10%				
*Servidor hp proliant. *Impresoras Lexmark, Hp, Xerox. *Escáner Fujitsu 7160, 6140, 6770. *Switch hp v1910. *Switch Planet FNSW 2401. *Switch 3Com 4200. *Access Point Ubiquiti. *Planta Telefonica. *DVR Gsecurity. *UPS StarUPS APC 2200. *Computador personal. *Celular empresarial.	**[I.5] Avería de origen físico o lógico**	M	50%				
	[I.6] Coste del suministro eléctrico	M	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	100%				
	[I.11] Emanaciones electromagnéticas	M			1%		
	[I.2] Errores del administrador del sistema/ de la seguridad	M	20%	20%	20%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	10%				
	[E.24] Caída del sistema por agotamiento de recursos	M	50%				
	[E.25] Perdida de equipos	B	100%		100%		
	[A.6] Abuso de privilegios de acceso	M	10%	10%	50%		
	[A.7] Uso no previsto	M	1%	1%	10%		
	[A.11] Acceso no autorizado	M	10%	10%	50%		

	[A.23] Manipulación del hardware	M	50%		50%		
	[A.24] Denegación de servicio	M	100%				
	[A.25] Robo de equipos	B	100%		100%		
	[A.26] Ataque destructivo	M	100%				
Red Local	**Total**		**75%**	**75%**	**100%**	**100%**	**50%**
	[I.8] Fallo de servicios de comunicaciones	MA	75%	75%	20%	20%	5%
	[E.9] Errores de re-encaminamiento	A			20%		
	[E.10] Errores de secuencia	B	30%		20%		
	[A.5] Suplantación de identidad del usuario	M		5%	100%	80%	5%
	[A.9] Re-encaminamiento de mensajes	M	50%		20%		50%
	[A.10] Alteración de secuencia	M		10%			
	[A.11] Acceso no autorizado	M		10%	50%	100%	
	[E.2] Errores del administrador del sistema / de la seguridad	M	30%	20%	20%		
	[A.18] Destrucción de la información	M	50%	70%	20%	20%	10%
Red Inalámbrica	**Total**		**60%**		**100%**	**100%**	
	[I.8] Fallo de servicios de comunicaciones	M	60%				
	[E.9] Errores de re-encaminamiento	M			10%		
	[A.5] Suplantación de identidad del usuario	M		10%	50%	100%	

	[A.12] Análisis de tráfico	M			100%	5%	5%
	[A.10] Alteración de secuencia	M		10%			
	[E.2] Errores del administrador del sistema / de la seguridad	M	30%	20%	20%		
	[A.18] Destrucción de la información	M	50%	70%	20%	20%	10%
Red telefónica	**Total**		**100%**	**50%**	**100%**	**75%**	**50%**
	[E.9] Fugas de información	M			40%		
	[A.14] Interceptación de información (escucha)	M	5%	20%	100%	75%	5%
	[1.3] Contaminación medioambiental	B	5%	5%	5%	5%	5%
	[1.3.3] Polvo	M	5%	5%	5%	5%	5%
	[I.8] Fallo de servicio de comunicaciones	MA	100%	50%	50%	20%	50%
	[A.25] Robo de equipos	MB	100%				
*Internet banda ancha 4 m *Internet banda ancha 2 m *Internet dedicado 8 m	**Total**		**100%**	**50%**	**50%**	**40%**	**5%**
	[I.8] Fallo de servicios de comunicación	A	80%				
	[E.9] Fugas de información	M				40%	5%
	[A.14] Interceptación de información (escucha)	M			10%	15%	
	[1.3] Contaminación medioambiental	MB	5%				
	[1.3.3] Polvo	A	5%				
	[I.8] Fallo de servicio de comunicaciones	MA	100%	50%	50%		
	[A.25] Robo de equipos	B	100%				

	[E.24] Caída del sistema por agotamiento de recursos	A	100%				
*Disco duro extraíble de 1 T. *Memorias USB. *DVD de respaldo.	**Total**		**100%**	**100%**	**100%**	**75%**	**5%**
	[N.1] Fuego	B	100%				
	[N.2] Daños por agua	B	50%				
	[N.*] Desastres naturales	B	100%				
	[I.*] Desastres industriales	M	100%				
	[I.3] Contaminación medioambiental	M	100%				
	[I.4] Contaminación Electromagnética	M	100%				
	[I.5] Avería de origen físico o lógico	M	50%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	100%				
	[I.10] Degradación de los soportes de almacenamiento de la información	M	100%				
	[E.18] Destrucción de la información	M	100%				
	[A.11] Acceso no autorizado	A		10%	50%		
	[A.15] Modificación de la información	A		100%	40%		
	[A.25] Robo de equipos	A	50%				
	[A.26] Ataque destructivo	M	50%	75%	100%	75%	5%
	[A.19] Revelación de información	M			100%	20%	
Aire Acondicionado	**Total**		**20%**	**0%**	**0%**	**0%**	**0%**
	[N.1] Fuego	B	5%				
	[N.2] Daños por agua	B	5%				

	[N.*] Desastres naturales	A	20%				
	[I.*] Desastres industriales	M	10%				
	[I.3] Contaminación medioambiental	M	10%				
	[I.6] Corte del suministro eléctrico	M	10%				
	[I.9] Interrupción de otros servicios o suministros esenciales	M	10%				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	10%				
	[A.23] Manipulación de hardware	M	10%				
	[A.25] Robo de equipos	M	10%				
	[A.26] Ataque destructivo	M	10%				
UPS de 1Kva	**Total**		**50%**	**0%**	**0%**	**0%**	**0%**
	[N.1] Fuego	B	50%				
	[N.2] Daños por agua	B	5%				
	[N.*] Desastres naturales	B	5%				
	[I.*] Desastres industriales	M	5%				
	[I.3] Contaminación medioambiental	M	5%				
	[I.9] Interrupción de otros servicios o suministros esenciales	B	5%				
	[A.23] Manipulación de hardware	M	5%				
	[A.25] Robo de equipos	M	50%				

	[A.26] Ataque destructivo	M	50%				
*Cableado en fibra óptica. * Cableado eléctrico	**Total**		**100%**	**10%**	**100%**	**5%**	**0%**
	[N.1] Fuego	B	100%				
	[N.2] Daños por agua	B	100%				
	[N.*] Desastres naturales	B	50%				
	[I.*] Desastres industriales	M	100%				
	[I.3] Contaminación medioambiental	B	100%				
	[I.4] Contaminación electromagnética	M	100%				
	[I.11] Emanaciones electromagnéticas	M			5%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	100%				
	[A.11] Acceso no autorizado	M		10%	100%	5%	
	[A.23] Manipulación de hardware	M	100%		50%		
	[A.25] Robo de equipos	M	100%				
	[A.26] Ataque destructivo	M	100%				
Escritorios	**Total**		**100%**	**0%**	**50%**	**0%**	**0%**
	[N.1] Fuego	M	100%				
	[N.2] Daños por agua	B	50%				
	[N.*] Desastres naturales	B	100%				
	[I.*] Desastres industriales	M	100%				
	[I.3] Contaminación medioambiental	B	50%				

	[A.23] Manipulación de hardware	M	50%		50%		
	[A.25] Robo de equipos	M	50%				
	[A.26] Ataque destructivo	M	50%				
Rack de piso de 24 u	**Total**		**100%**	**0%**	**0%**	**0%**	**0%**
	[N.1] Fuego	B	100%				
	[N.2] Daños por agua	B	50%				
	[N.*] Desastres naturales	B	100%				
	[I.*] Desastres industriales	M	100%				
	[I.3] Contaminación medioambiental	B	50%				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	10%				
	[A.25] Robo de equipos	M	20%				
	[A.26] Ataque destructivo	M	50%				
Edificio	**Total**		**100%**	**0%**	**50%**	**0%**	**0%**
	[N.1] Fuego	M	100%				
	[N.2] Daños por agua	M	100%				
	[N.*.1] Tormentas	M	100%				
	[N.*.4] Terremotos	M	100%				
	[N.*.11] Calor extremo	M	20%				
	[I.*] Desastres industriales	B	20%				
	[A.27] Ocupación enemiga	M	100%		50%		
*Comerciantes y población en general. *Director Administrativo y Financiero. *Ingeniero de	**Total**		**100%**	**100%**	**100%**	**20%**	**20%**
	[E.15] Alteración de la información	M		50%			5%
	[E.19] Fugas de información	M			50%		

Sistemas *Coordinadora de Sistemas. *Jefe de Archivo. *Jefe de Caja. *Auxiliar de Caja. *Auxiliar de Registro. *Asistente de Registros *Publico Jurídico. *Jefe de Conciliación. *Secretaria General. *Coordinadora de Desarrollo Empresarial. *Asistente Administrativa y Contable. *CertiCámaras. *UNE. *Movistar. *ConfeCámaras. *Servicios generales.	**[A.15] Modificación de la información**	M		100%	50%	5%	
	[A.18] Destrucción de la información	M	100%	20%	20%	20%	20%
	[A.19] Revelación de información	A			100%		
	[A.28] Indisponibilidad del personal	B	100%				
	[A.29] Extorsión	M	20%	10%	50%		
	[A.30] Ingeniería social (picaresca)	M	50%	100%	100%		

Fuente: Autores del proyecto.

Caracterización de Salvaguardas. Identificación de Salvaguardas

Tabla 19. Identificación de salvaguardas.

ACTIVOS	AMENAZAS	SALVAGUARDA

*Router Board Mikrotik de UNE. *Modem Huawei de UNE. *Multiservice Gateway Allied Telesis, Equipo de Confecámaras. *Router Cisco 1700. *Modem Miltrastar de Movistar 4 m. *Modem Nukon de Movistar 2 m	**[E.15] Alteración de la información**	16.1.2 Notificación de los eventos de seguridad de la información. 16.1.3 Notificación de puntos débiles de la seguridad. 9.1.2 Control de acceso a las redes y servicios asociados 13.2.1 Políticas y procedimientos de intercambio de información.
	[E.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información. 13.1.2 Mecanismos de seguridad asociados a servicios en red.
	[E.19] Fugas de Información	9.4.1 Restricción del acceso a la información. 10.1.2 Gestión de claves. 16.1.2 Notificación de los eventos de seguridad de la información. 12.4.2 Protección de los registros de información
	[A.5] Suplantación de identidad	9.2.5 Revisión de los derechos de acceso de los usuarios. 9.3.1 Uso de información confidencial para la autenticación. 12.4.3 Registros de actividad del administrador y operador del sistema. 16.1.2 Notificación de los eventos de seguridad de la información.
	[A.11] Acceso no Autorizado	9.2.6 Retirada o adaptación de los derechos de acceso 9.1.2 Control de acceso a las redes y servicios asociados

	[A.15] Modificación de la información	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.3.1 Copias de seguridad de la información. 12.4.2 Protección de los registros de información. 9.1.2 Control de acceso a las redes y servicios asociados.
	[A.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información
	[A.19] Revelación de información	13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información. 9.1.2 Control de acceso a las redes y servicios asociados.
*Información de registro. *Información contable. *Información administrativa	**[E.1] Errores de los usuarios**	7.2.2 Concienciación, educación y capacitación en seguridad de la información.
	[E.2] Errores del Administrador de sistema / de la seguridad	7.2.1 Responsabilidades de gestión. 7.2.3 Proceso disciplinario.
	[E.15] Alteración de la información	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.3.1 Copias de seguridad de la información. 9.4.1 Restricción del acceso a la información.

	[E.19] Fugas de Información	9.4.1 Restricción del acceso a la información. 10.1.2 Gestión de claves. 16.1.2 Notificación de los eventos de seguridad de la información. 12.4.2 Protección de los registros de información. 9.4.3 Gestión de contraseñas de usuario
	[A.5] Suplantación de identidad	9.2.5 Revisión de los derechos de acceso de los usuarios. 9.3.1 Uso de información confidencial para la autenticación. 12.4.3 Registros de actividad del administrador y operador del sistema. 16.1.2 Notificación de los eventos de seguridad de la información.
	[A.6] Abuso de privilegios de acceso	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.3.1 Uso de información confidencial para la autenticación. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.4.1 Restricción del acceso a la información.
	[A.11] Acceso no autorizado	9.2.6 Retirada o adaptación de los derechos de acceso 9.2.2 Gestión de los derechos de acceso asignados a usuarios

	[A.15] Modificación de la información	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.3.1 Copias de seguridad de la información. . 12.4.2 Protección de los registros de información.
	[A.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información
	[A.19] Revelación de información	9.4.1 Restricción del acceso a la información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información
Copias de respaldo de la información de registro, administrativa y financiera.	**[E.1] Errores de los usuarios**	7.2.2 Concienciación, educación y capacitación en seguridad de la información.
	[E.2] Errores del Administrador de sistema / de la seguridad	7.2.1 Responsabilidades de gestión. 7.2.3 Proceso disciplinario.
	[E.15] Alteración de la información	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.3.1 Copias de seguridad de la información. 9.4.1 Restricción del acceso a la información.

	[E.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información
	[E.19] Fugas de información	9.4.1 Restricción del acceso a la información. 10.1.2 Gestión de claves. 16.1.2 Notificación de los eventos de seguridad de la información. 12.4.2 Protección de los registros de información
	[A.5] Suplantación de la identidad	9.2.5 Revisión de los derechos de acceso de los usuarios. 9.3.1 Uso de información confidencial para la autenticación. 12.4.3 Registros de actividad del administrador y operador del sistema. 16.1.2 Notificación de los eventos de seguridad de la información.
	[A.6] Abuso de privilegios de acceso	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.3.1 Uso de información confidencial para la autenticación. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.4.4 Uso de herramientas de administración de sistemas.
	[A.11] Acceso no autorizado	9.2.6 Retirada o adaptación de los derechos de acceso 9.2.2 Gestión de los derechos de acceso asignados a usuarios

	[A.15] Modificación de la información	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.3.1 Copias de seguridad de la información. . 12.4.2 Protección de los registros de información.
	[A.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información
	[A.19] Revelación de información	9.4.1 Restricción del acceso a la información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información
*Datos de configuración *Datos de gestión interna (usuarios, permiso)	**[E.1] Errores de los usuarios**	7.2.2 Concienciación, educación y capacitación en seguridad de la información.
	[E.2] Errores del Administrador de sistema / de la seguridad	7.2.1 Responsabilidades de gestión. 7.2.3 Proceso disciplinario.
	[E.18] Errores de configuración	7.2.2 Concienciación, educación y capacitación en seguridad de la información. 12.1.2 Gestión de cambios. 2.1.1 Documentación de procedimientos de operación.
	[E.15] Alteración de la información	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.3.1 Copias de seguridad de la información. 9.4.1 Restricción del acceso a la información.

	[E.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información
	[E.19] Fugas de Información	9.4.1 Restricción del acceso a la información. 10.1.2 Gestión de claves. 16.1.2 Notificación de los eventos de seguridad de la información. 12.4.2 Protección de los registros de información
	[A.4] Manipulación de los ficheros de configuración	12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.4.1 Restricción del acceso a la información.
	[A.5] Suplantación de la identidad	9.2.5 Revisión de los derechos de acceso de los usuarios. 9.3.1 Uso de información confidencial para la autenticación. 12.4.3 Registros de actividad del administrador y operador del sistema. 16.1.2 Notificación de los eventos de seguridad de la información.
	[A.6] Abuso de privilegios de acceso	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.3.1 Uso de información confidencial para la autenticación. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.4.4 Uso de herramientas de administración de sistemas.

	[A.11] Acceso no autorizado	9.2.6 Retirada o adaptación de los derechos de acceso 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.4.2 Protección de los registros de información.
	[A.15] Modificación de la información	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.3.1 Copias de seguridad de la información. . 12.4.2 Protección de los registros de información.
	[A.19] Revelación de información	9.4.1 Restricción del acceso a la información. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.3.1 Uso de información confidencial para la autenticación. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información
Registro de actividades	**[E.1] Errores de los usuarios**	7.2.2 Concienciación, educación y capacitación en seguridad de la información.
	[E.2] Errores del Administrador de sistema / de la seguridad	7.2.1 Responsabilidades de gestión. 7.2.3 Proceso disciplinario.
	[E.3] Errores de monitorización (log)	12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes.

	[E.15] Alteración de la información	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.3.1 Copias de seguridad de la información. 9.4.1 Restricción del acceso a la información. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema.
	[E.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información. 12.4.2 Protección de los registros de información.
	[E.19] Fugas de Información	9.4.1 Restricción del acceso a la información. 10.1.2 Gestión de claves. 16.1.2 Notificación de los eventos de seguridad de la información. 12.4.2 Protección de los registros de información
	[A.3] Manipulación de los registros de actividad (log)	12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 9.2.5 Revisión de los derechos de acceso de los usuarios.

	[A.5] Suplantación de la identidad	9.2.5 Revisión de los derechos de acceso de los usuarios. 9.3.1 Uso de información confidencial para la autenticación. 12.4.3 Registros de actividad del administrador y operador del sistema. 16.1.2 Notificación de los eventos de seguridad de la información.
	[A.6] Abuso de privilegios de acceso	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.3.1 Uso de información confidencial para la autenticación. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.4.4 Uso de herramientas de administración de sistemas. 12.4.2 Protección de los registros de información.
	[A.11] Acceso no autorizado	9.2.6 Retirada o adaptación de los derechos de acceso. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.4.2 Protección de los registros de información.
	[A.13] Repudio (negación de actuaciones)	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información.

	[A.15] Modificación de la información	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.3.1 Copias de seguridad de la información. . 12.4.2 Protección de los registros de información.
	[A.19] Revelación de información	9.4.1 Restricción del acceso a la información. 12.4.2 Protección de los registros de información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información
Firma digital	**[E.1] Errores de los usuarios**	7.2.2 Concienciación, educación y capacitación en seguridad de la información.
	[E.2] Errores del Administrador de sistema / de la seguridad	7.2.1 Responsabilidades de gestión.7.2.3 Proceso disciplinario.
	[E.19] Fugas de información	9.4.1 Restricción del acceso a la información. 10.1.2 Gestión de claves. 16.1.2 Notificación de los eventos de seguridad de la información. 12.4.2 Protección de los registros de información
	[A.5] Suplantación de la identidad	9.2.5 Revisión de los derechos de acceso de los usuarios. 9.3.1 Uso de información confidencial para la autenticación. 12.4.3 Registros de actividad del administrador y operador del sistema. 16.1.2 Notificación de los eventos de seguridad de la información.

	[A.6] Abuso de privilegios de acceso	8.3.1 Gestión de soportes extraíbles. 9.1.1 Política de control de accesos. 16.1.2 Notificación de los eventos de seguridad de la información. 9.3.1 Uso de información confidencial para la autenticación. 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
	[A.11] Acceso no autorizado	9.1.2 Control de acceso a las redes y servicios asociados. 9.1.1 Política de control de accesos.
	[A.19] Revelación de información	9.4.1 Restricción del acceso a la información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información
Correo electrónico empresarial	**[I.9] Interrupción de otros servicios o suministros esenciales**	13.2.1 Políticas y procedimientos de intercambio de información. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 16.1.5 Respuesta a los incidentes de seguridad.
	[E.15] Alteración de la información	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.3.1 Copias de seguridad de la información. 9.4.1 Restricción del acceso a la información.
	[E.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información

	[E.19] Fugas de información	9.4.1 Restricción del acceso a la información. 10.1.2 Gestión de claves. 16.1.2 Notificación de los eventos de seguridad de la información. 12.4.2 Protección de los registros de información
	[A.5] Suplantación de la identidad	9.2.5 Revisión de los derechos de acceso de los usuarios. 9.3.1 Uso de información confidencial para la autenticación. 12.4.3 Registros de actividad del administrador y operador del sistema. 16.1.2 Notificación de los eventos de seguridad de la información.
	[A.13] Repudio (negación de actuaciones)	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información.
	[A.15] Modificación de la información	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.3.1 Copias de seguridad de la información. . 12.4.2 Protección de los registros de información.
	[A.19] Relevación de información	9.4.1 Restricción del acceso a la información. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información
	[A.24] Denegación de servicio	12.3.1 Copias de seguridad de la información. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.1.1 Política de control de accesos. 16.1.5 Respuesta a los incidentes de seguridad.

*Soporte a usuarios externos (manejo de trámites en línea) a través de chat online y vía telefónica. *Gestión de privilegios en los sistemas de información SII y DocuWare *Servicio de transferencia de fichero FTP hacia el servidor SIREP *Servicio de registros públicos a usuarios externos a través de la web *Servicio de registros públicos a usuarios internos. *Servicio radicación y consulta de expedientes digitalizados a usuarios internos.	**[E.1] Errores de los usuarios**	7.2.2 Concienciación, educación y capacitación en seguridad de la información.
	[E.2] Errores del administrador del sistema / de la seguridad	7.2.1 Responsabilidades de gestión. 7.2.3 Proceso disciplinario.
	[E.15] Alteración de la información	9.4.1 Restricción del acceso a la información. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información
	[E.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información
	[E.19] Fugas de información	9.4.1 Restricción del acceso a la información. 10.1.2 Gestión de claves. 16.1.2 Notificación de los eventos de seguridad de la información. 12.4.2 Protección de los registros de información
	[E.24] Caída del sistema por agotamiento de recursos	12.3.1 Copias de seguridad de la información. 12.1.3 Gestión de capacidades. 15.1.1 Política de seguridad de la información para suministradores. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades.
	[A.5] Suplantación de la identidad	9.2.5 Revisión de los derechos de acceso de los usuarios. 9.3.1 Uso de información confidencial para la autenticación. 12.4.3 Registros de actividad del administrador y operador del sistema. 16.1.2 Notificación de los eventos de seguridad de la información.

	[A.6] Abuso de privilegios de acceso	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.3.1 Uso de información confidencial para la autenticación. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.4.4 Uso de herramientas de administración de sistemas. 12.4.2 Protección de los registros de información.
	[A.7] Uso no previsto	9.1.1 Política de control de accesos.
	[A.11] Acceso no autorizado	9.2.6 Retirada o adaptación de los derechos de acceso. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.4.2 Protección de los registros de información.
	[A.13] Repudio (negación de actuaciones)	16.1.2 Notificación de los eventos de seguridad de la información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información.
	[A.15] Modificación de la información	14.2.5 Uso de principios de ingeniería en protección de sistemas. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.4.2 Protección de los registros de información.
	[A.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información

	[A.19] Revelación de la información	9.4.1 Restricción del acceso a la información. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
	[A.24] Denegación de servicio	12.3.1 Copias de seguridad de la información. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.1.1 Política de control de accesos. 16.1.5 Respuesta a los incidentes de seguridad.
*SIREP. *DocuWare. *SII. *Jsp7. *Microsoft Office Hogar y Empresa 2013. *Antivirus kaspersky. *Cpanel, administrador de Servidor de correo electrónico y pagina web. *SQL Server 2012 Sistema de Gestión de Base de Datos *Mozilla Firefox 47.0.0 *Google Chrome. *Windows Server 2012. *Windows 7, 8.1 y 8.	**[I.5] Avería de origen físico o lógico**	11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 12.3.1 Copias de seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. 17.1.1 Planificación de la continuidad de la seguridad de la información. 11.2.4 Mantenimiento de los equipos. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
	[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información.
	[E.2] Errores del administrador del sistema / de la seguridad	7.2.1 Responsabilidades de gestión. 7.2.3 Proceso disciplinario.
	[E.8] Difusión de software dañado	16.1.7 Recopilación de evidencias. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.

	[E.15] Alteración de la información	9.4.1 Restricción del acceso a la información. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información
	[E.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información
	[E.19] Fugas de información	9.4.1 Restricción del acceso a la información. 10.1.2 Gestión de claves. 16.1.2 Notificación de los eventos de seguridad de la información. 12.4.2 Protección de los registros de información
	[E.20] Vulnerabilidades de los programas (software)	12.6.2 Restricciones en la instalación de software. 14.2.1 Política de desarrollo seguro de software. 14.2.2 Procedimientos de control de cambios en los sistemas.
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	12.3.1 Copias de seguridad de la información. 14.2.5 Uso de principios de ingeniería en protección de sistemas.
	[A.5] Suplantación de identidad	9.2.5 Revisión de los derechos de acceso de los usuarios. 9.3.1 Uso de información confidencial para la autenticación. 12.4.3 Registros de actividad del administrador y operador del sistema. 16.1.2 Notificación de los eventos de seguridad de la información.

	[A.6] Abuso de privilegios de acceso	9.4.2 Procedimientos seguros de inicio de sesión. 16.1.2 Notificación de los eventos de seguridad de la información. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.3.1 Uso de información confidencial para la autenticación. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.4.4 Uso de herramientas de administración de sistemas. 12.4.2 Protección de los registros de información.
	[A.8] Difusión de software dañino	16.1.7 Recopilación de evidencias. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.
	[A.11] Acceso no autorizado	9.1.2 Control de acceso a las redes y servicios asociados. 9.4.2 Procedimientos seguros de inicio de sesión. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.4.2 Protección de los registros de información
	[A.15] Modificación de la información	14.2.5 Uso de principios de ingeniería en protección de sistemas. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.4.2 Protección de los registros de información.

	[A.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información
	[A.19] Revelación de información	9.4.1 Restricción del acceso a la información. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información
	[A.22] Manipulación de programas	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 8.1.3 Uso aceptable de los activos. 8.2.3 Manipulación de activos.
*Servidor hp proliant. *Impresoras Lexmark, Hp, Xerox. *Escáner Fujitsu 7160, 6140, 6770. *Switch hp v1910. *Switch Planet FNSW 2401. *Switch 3Com 4200. *Access Point Ubiquiti. *Planta Telefónica. *DVR Gsecurity. *UPS StarUPS APC 2200. *Computador personal. *Celular empresarial.	**[N.1] Fuego**	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridadde la información.
	[I.3] Contaminación medioambiental	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
	[I.4] Contaminación electromagnética	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

	[I.5] Avería de origen físico o lógico	11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 12.3.1 Copias de seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de lainformación. 17.1.1 Planificación de la continuidad de la seguridad de la información. 11.2.4 Mantenimiento de los equipos. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en elsistema operativo.
	[I.6] Coste del suministro eléctrico	11.1.1 Perímetro de seguridad física. 11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 17.1.1 Planificación de la continuidad de la seguridad de la información. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
	[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.1 Perímetro de seguridad física. 11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 17.1.1 Planificación de la continuidad de la seguridad de la información. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
	[I.11] Emanaciones electromagnéticas	11.1.1 Perímetro de seguridad física. 11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 17.1.1 Planificación de la continuidad de la seguridad de la información. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

	[I.2] Errores del administrador del sistema/ de la seguridad	7.2.1 Responsabilidades de gestión. 7.2.3 Proceso disciplinario.
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	12.3.1 Copias de seguridad de la información. 11.2.4 Mantenimiento de los equipos. 11.2.1 Emplazamiento y protección de equipos.
	[E.24] Caída del sistema por agotamiento de recursos	12.3.1 Copias de seguridad de la información. 12.1.3 Gestión de capacidades. 15.1.1 Política de seguridad de la información para suministradores. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 11.2.4 Mantenimiento de los equipos.
	[E.25] Perdida de equipos	12.4.2 Protección de los registros de información. 12.3.1 Copias de seguridad de la información.
	[A.6] Abuso de privilegios de acceso	9.2.6 Retirada o adaptación de los derechos de acceso 9.4.1 Restricción del acceso a la información. 16.1.2 Notificación de los eventos de seguridad de la información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.1.2 Control de acceso a las redes y servicios asociados. 9.1.1 Política de control de accesos.
	[A.7] Uso no previsto	9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y
	[A.11] Acceso no autorizado	9.2.6 Retirada o adaptación de los derechos de acceso. 12.4.2 Protección de los registros de información. 9.1.2 Control de acceso a las redes y servicios asociados. 9.1.1 Política de control de accesos.

	[A.23] Manipulación del hardware	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 8.1.3 Uso aceptable de los activos. 8.2.3 Manipulación de activos.
	[A.24] Denegación de servicio	12.3.1 Copias de seguridad de la información. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.1.1 Política de control de accesos. 16.1.5 Respuesta a los incidentes de seguridad.
	[A.25] Robo de equipos	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos.
	[A.26] Ataque destructivo	12.2.1 Controles contra el código malicioso. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
Red Local	**[I.8] Fallo de servicios de comunicaciones**	13.1.2 Mecanismos de seguridad asociados a servicios en red. 14.1.3 Protección de las transacciones por redes telemáticas. 15.2.2 Gestión de cambios en los servicios prestados por terceros. 13.1.1 Controles de red. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

	[E.9] Errores de re-encaminamiento	13.1.1 Controles de red. 13.1.3 Segregación de redes.
	[E.10] Errores de secuencia	13.1.1 Controles de red. 13.1.3 Segregación de redes.
	[A.5] Suplantación de identidad del usuario	9.2.5 Revisión de los derechos de acceso de los usuarios. 9.3.1 Uso de información confidencial para la autenticación. 12.4.3 Registros de actividad del administrador y operador del sistema. 16.1.2 Notificación de los eventos de seguridad de la información.
	[A.9] Re-encaminamiento de mensajes	13.1.1 Controles de red. 13.2.2 Acuerdos de intercambio.
	[A.10] Alteración de secuencia	13.1.1 Controles de red
	[A.11] Acceso no autorizado	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.1.2 Control de acceso a las redes y servicios asociados. 9.1.1 Política de control de accesos.
	[E.2] Errores del administrador del sistema / de la seguridad	7.2.1 Responsabilidades de gestión. 7.2.3 Proceso disciplinario.
	[A.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información

Red Inalámbrica	**[I.8] Fallo de servicios de comunicaciones**	13.1.2 Mecanismos de seguridad asociados a servicios en red. 14.1.3 Protección de las transacciones por redes telemáticas. 15.2.2 Gestión de cambios en los servicios prestados por terceros. 13.1.1 Controles de red. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
	[E.9] Errores de re-encaminamiento	13.1.1 Controles de red
	[A.5] Suplantación de identidad del usuario	9.2.5 Revisión de los derechos de acceso de los usuarios. 9.3.1 Uso de información confidencial para la autenticación. 12.4.3 Registros de actividad del administrador y operador del sistema. 16.1.2 Notificación de los eventos de seguridad de la información.
	[A.12] Análisis de tráfico	12.6.1 Gestión de las vulnerabilidades técnicas. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes.
	[A.10] Alteración de secuencia	13.1.2 Mecanismos de seguridad asociados a servicios en red.
	[E.2] Errores del administrador del sistema / de la seguridad	7.2.1 Responsabilidades de gestión. 7.2.3 Proceso disciplinario.
	[A.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información

Red telefónica	**[E.9] Fugas de información**	9.4.1 Restricción del acceso a la información. 10.1.2 Gestión de claves. 16.1.2 Notificación de los eventos de seguridad de la información. 12.4.2 Protección de los registros de información
	[A.14] Interceptación de información (escucha)	12.6.1 Gestión de las vulnerabilidades técnicas. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes.
	[1.3] Contaminación medioambiental	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 11.2.3 Seguridad del cableado.
	[1.3.3] Polvo	11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales.
	[I.8] Fallo de servicio de comunicaciones	13.1.2 Mecanismos de seguridad asociados a servicios en red. 14.1.3 Protección de las transacciones por redes telemáticas. 15.2.2 Gestión de cambios en los servicios prestados por terceros. 13.1.1 Controles de red. 17.2.1 Disponibilidad de instalaciones para el procesamiento de lainformación.

	[A.25] Robo de equipos	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos.
*Internet banda ancha 4 m *Internet banda ancha 2 m *Internet dedicado 8 m	**[I.8] Fallo de servicios de comunicación**	15.2.2 Gestión de cambios en los servicios prestados por terceros. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 14.1.3 Protección de las transacciones por redes telemáticas. 15.2.2 Gestión de cambios en los servicios prestados por terceros. 13.1.1 Controles de red. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
	[E.9] Fugas de información	9.4.1 Restricción del acceso a la información. 10.1.2 Gestión de claves. 16.1.2 Notificación de los eventos de seguridad de la información. 12.4.2 Protección de los registros de información
	[A.14] Interceptación de información (escucha)	12.6.1 Gestión de las vulnerabilidades técnicas. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes.

	[1.3] Contaminación medioambiental	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridadde la información.
	[1.3.3] Polvo	11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales.
	[I.8] Fallo de servicio de comunicaciones	13.1.2 Mecanismos de seguridad asociados a servicios en red. 14.1.3 Protección de las transacciones por redes telemáticas. 15.2.2 Gestión de cambios en los servicios prestados por terceros. 13.1.1 Controles de red. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
	[A.25] Robo de equipos	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos.

	[E.24] Caída del sistema por agotamiento de recursos	12.3.1 Copias de seguridad de la información. 12.1.3 Gestión de capacidades. 15.1.1 Política de seguridad de la información para suministradores. 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.3 Cadena de suministro en tecnologías de la información ycomunicaciones. 15.2.1 Supervisión y revisión de los servicios prestados por terceros. 15.2.2 Gestión de cambios en los servicios prestados por terceros.
*Disco duro extraíble de 1 T. *Memorias USB. *DVD de respaldo.	**[N.1] Fuego**	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridadde la información.
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
	[I.3] Contaminación medioambiental	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

	[I.4] Contaminación Electromagnética	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridadde la información.
	[I.5] Avería de origen físico o lógico	11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 12.3.1 Copias de seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. 17.1.1 Planificación de la continuidad de la seguridad de la información. 11.2.4 Mantenimiento de los equipos.
	[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.1 Perímetro de seguridad física. 11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 17.1.1 Planificación de la continuidad de la seguridad de la información. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
	[I.10] Degradación de los soportes de almacenamiento de la información	8.1.3 Uso aceptable de los activos. 8.2.3 Manipulación de activos. 8.3.1 Gestión de soportes extraíbles. 8.3.3 Soportes físicos en tránsito.

	[E.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información
	[A.11] Acceso no autorizado	9.1.1 Política de control de accesos. 8.2.3 Manipulación de activos
	[A.15] Modificación de la información	9.1.2 Control de acceso a las redes y servicios asociados. 12.3.1 Copias de seguridad de la información. . 8.3.1 Gestión de soportes extraíbles
	[A.25] Robo de equipos	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos.
	[A.26] Ataque destructivo	12.2.1 Controles contra el código malicioso. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
	[A.19] Revelación de información	8.3.1 Gestión de soportes extraíbles. 9.4.1 Restricción del acceso a la información. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información.
Aire Acondicionado	**[N.1] Fuego**	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física.

	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física.
	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física.
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física.
	[I.3] Contaminación medioambiental	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos.
	[I.6] Corte del suministro eléctrico	15.2.2 Gestión de cambios en los servicios prestados por terceros. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. 11.1.5 El trabajo en áreas seguras.

	[I.9] Interrupción de otros servicios o suministros esenciales	12.1.1 Documentación de procedimientos de operación. 15.2.1 Supervisión y revisión de los servicios prestados por terceros. 15.2.2 Gestión de cambios en los servicios prestados por terceros. 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.1 Política de seguridad de la información para suministradores.
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	11.2.4 Mantenimiento de los equipos. 11.2.1 Emplazamiento y protección de equipos.
	[A.23] Manipulación de hardware	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 8.1.3 Uso aceptable de los activos. 8.2.3 Manipulación de activos.
	[A.25] Robo de equipos	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos.
	[A.26] Ataque destructivo	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.1 Perímetro de seguridad física. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridadde la información.

UPS de 1Kva	**[N.1] Fuego**	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física.
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física.
	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física.
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física.
	[I.3] Contaminación medioambiental	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos.
	[I.9] Interrupción de otros servicios o suministros esenciales	12.1.1 Documentación de procedimientos de operación. 15.2.1 Supervisión y revisión de los servicios prestados por terceros. 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.1 Política de seguridad de la información para suministradores. 16.1.5 Respuesta a los incidentes de seguridad.

	[A.23] Manipulación de hardware	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 8.1.3 Uso aceptable de los activos. 8.2.3 Manipulación de activos.
	[A.25] Robo de equipos	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos.
	[A.26] Ataque destructivo	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.1 Perímetro de seguridad física. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
*Cableado en fibra óptica. * Cableado eléctrico	**[N.1] Fuego**	11.2.3 Seguridad del cableado. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física.
	[N.2] Daños por agua	11.2.3 Seguridad del cableado. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física.

	[N.*] Desastres naturales	11.2.3 Seguridad del cableado. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física.
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física.
	[I.3] Contaminación medioambiental	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 11.2.3 Seguridad del cableado.
	[I.4] Contaminación electromagnética	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 11.2.3 Seguridad del cableado.

	[I.11] Emanaciones electromagnéticas	11.1.1 Perímetro de seguridad física. 11.1.5 El trabajo en áreas seguras. 11.2.2 Instalaciones de suministro. 17.1.1 Planificación de la continuidad de la seguridad de la información. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en elsistema operativo. 11.2.3 Seguridad del cableado.
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	11.2.4 Mantenimiento de los equipos. 11.2.1 Emplazamiento y protección de equipos. 11.2.3 Seguridad del cableado.
	[A.11] Acceso no autorizado	9.1.2 Control de acceso a las redes y servicios asociados. 9.1.1 Política de control de accesos. 11.2.3 Seguridad del cableado
	[A.23] Manipulación de hardware	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 8.1.3 Uso aceptable de los activos. 8.2.3 Manipulación de activos.
	[A.25] Robo de equipos	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 9.1.2 Control de acceso a las redes y servicios asociados.
	[A.26] Ataque destructivo	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.1 Perímetro de seguridad física. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Escritorios	**[N.1] Fuego**	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física. 11.1.5 El trabajo en áreas seguras.
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física. 11.1.5 El trabajo en áreas seguras.
	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.1 Perímetro de seguridad física. 11.1.5 El trabajo en áreas seguras.
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.5 El trabajo en áreas seguras.
	[I.3] Contaminación medioambiental	11.1.5 El trabajo en áreas seguras. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos.
	[A.23] Manipulación de hardware	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 8.1.3 Uso aceptable de los activos. 8.2.3 Manipulación de activos.
	[A.25] Robo de equipos	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos.

	[A.26] Ataque destructivo	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.1 Perímetro de seguridad física. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridadde la información.
Rack de piso de 24 u	**[N.1] Fuego**	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.5 El trabajo en áreas seguras.
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.5 El trabajo en áreas seguras.
	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.5 El trabajo en áreas seguras.
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.5 El trabajo en áreas seguras.
	[I.3] Contaminación medioambiental	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.5 El trabajo en áreas seguras.
	[E.23] Errores de mantenimiento / actualización de	11.2.4 Mantenimiento de los equipos. 11.2.1 Emplazamiento y protección de equipos.

	equipos (hardware)	11.2.3 Seguridad del cableado.
	[A.25] Robo de equipos	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos.
	[A.26] Ataque destructivo	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.1 Perímetro de seguridad física. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridadde la información.
Edificio	**[N.1] Fuego**	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.5 El trabajo en áreas seguras.
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.5 El trabajo en áreas seguras.

	[N.*.1] Tormentas	11.1.4 Protección contra las amenazas externas y ambientales. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
	[N.*.4] Terremotos	11.1.4 Protección contra las amenazas externas y ambientales. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridadde la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de lainformación.
	[N.*.11] Calor extremo	11.1.4 Protección contra las amenazas externas y ambientales. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.5 El trabajo en áreas seguras.
	[A.27] Ocupación enemiga	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras.
*Comerciantes y población en general. *Director Administrativo y Financiero. *Ingeniero de Sistemas *Coordinadora de Sistemas. *Jefe de Archivo. *Jefe de Caja. *Auxiliar de Caja. *Auxiliar de Registro. *Asistente de Registros *Publico Jurídico. *Jefe de Conciliación. *Secretaria General. *Coordinadora de Desarrollo Empresarial. *Asistente Administrativa y Contable. *CertiCámara s. *UNE.	**[E.15] Alteración de la información**	9.4.1 Restricción del acceso a la información. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 7.2.3 Proceso disciplinario. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
	[E.18] Destrucción de la información	9.4.1 Restricción del acceso a la información. 8.2.1 Directrices de clasificación 12.3.1 Copias de seguridad de la información. 7.2.3 Proceso disciplinario.
	[E.19] Fugas de información	9.4.1 Restricción del acceso a la información. 10.1.2 Gestión de claves. 16.1.2 Notificación de los eventos de seguridad de la información. 12.4.2 Protección de los registros de información. 7.2.3 Proceso disciplinario.

*Movistar. *ConfeCámara s. *Servicios generales.	**[A.15] Modificación de la información**	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.3.1 Copias de seguridad de la información. . 12.4.2 Protección de los registros de información. 9.1.2 Control de acceso a las redes y servicios asociados. 7.2.2 Concienciación, educación y capacitación en seguridad de la información 7.2.3 Proceso disciplinario.
	[A.19] Revelación de información	9.4.1 Restricción del acceso a la información. 13.2.4 Acuerdos de confidencialidad y secreto. 13.2.1 Políticas y procedimientos de intercambio de información. 7.2.2 Concienciación, educación y capacitación en seguridad de la información. 7.2.3 Proceso disciplinario. 18.1.4 Protección de datos y privacidad de la información personal. 6.1.1 Asignación de responsabilidades para la seguridad de la información.
	[A.28] Indisponibilidad del personal	17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridadde la información. 6.1.1 Asignación de responsabilidades para la seguridad de la información.

	[A.29] Extorsión	7.1.1 Investigación de antecedentes. 7.2.2 Concienciación, educación y capacitación en seguridad de la información. 7.2.3 Proceso disciplinario. 7.3.1 Cese o cambio de puesto de trabajo. 18.2.2 Cumplimiento de las políticas y normas de seguridad.
	[A.30] Ingeniería social (picaresca)	18.2.2 Cumplimiento de las políticas y normas de seguridad. 7.2.2 Concienciación, educación y capacitación en seguridad de la información. 7.2.3 Proceso disciplinario.

Fuente: Autores del proyecto.

Estimación del estado de riesgo.

Estimación del Impacto Potencial. Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

Tabla 20. Estimación del impacto potencial.

IMPACTO		**Degradación**		
		1% - 34%	**35% - 68%**	**69% - 100%**
Valor Activo	**MA**	A	MA	MA
	A	M	A	A
	M	B	M	M
	B	MB	B	B
	MB	MB	MB	MB

Fuente: Autores del proyecto.

Para hallar el impacto seleccionamos el valor de activo de la tabla valoración de activos y el acumulado de la degradación por activo, de la tabla valoración de amenazas.

Tabla 21. Calculo del impacto

Activos	Valor x Degradación					Impacto
	D	I	C	A	T	
Arquitectura						
Router Board Mikrotik de UNE	M	M	M	B	MB	M
Modem Huawei de UNE	A	M	M	B	MB	A
Multiservice Gateway Allied Telesis, Equipo de Confecámaras	M	M	B	B	MB	M
Router Cisco 1700	A	A	B	B	MB	A
Modem Miltrastar de Movistar 4 m	M	M	M	B	MB	M
Modem Nukon de Movistar 2 m	M	M	M	B	MB	M
Información						
información de registro	A	MA	MB	A	B	MA
Información contable	A	MA	A	A	B	MA
Información administrativa	M	A	B	A	B	A
Copias de respaldo de la información de registro, administrativa y financiera.	B	A	MB	B	MB	A
Datos de configuración	B	A	B	MB	MB	A
Datos de gestión interna (usuarios, permiso)	B	MA	M	M	MB	MA
Registro de actividades	MB	M	B	B	MB	M
Claves criptográficas						
Firma digital	A	M	A	M	MB	A
Servicios						
Correo electrónico empresarial	M	M	MA	A	M	MA
Soporte a usuarios externos (manejo de trámites en línea) a través de chat online y vía telefónica.	B	MB	MB	MB	MB	B
Gestión de privilegios en los sistemas de información SII y DocuWare	M	M	MB	M	B	M
Servicio de transferencia de fichero FTP hacia el servidor SIREP	M	M	MB	M	B	M
Servicio de registros públicos a usuarios externos a través de la web	M	M	MB	MB	M	M

Servicio de registros públicos a usuarios internos.	A	A	M	A	M		A
Servicio radicación y consulta de expedientes digitalizados a usuarios internos.	M	M	B	M	M		M
Aplicaciones informáticas							
SIREP	A	MA	M	M	MB		MA
DocuWare	M	A	M	M	MB		A
SII	A	MA	M	M	MB		MA
Jsp7	A	MA	A	A	B		MA
Microsoft Office Hogar y Empresa 2013	MB	B	MB	MB	MB		B
Antivirus kaspersky	MB	B	MB	MB	MB		B
Cpanel, administrador de Servidor de correo electrónico y pagina web.	B	B	M	M	MB		B
SQL Server 2012 Sistema de Gestión de Base de Datos	M	MA	B	M	MB		MA
Mozilla Firefox 47.0.1	MB	MB	MB	MB	MB		MB
Google Chrome	MB	MB	MB	MB	MB		MB
Windows Server 2012	A	A	A	M	MB		A
Windows 8.1	M	B	MB	B	MB		M
Windows 8	M	B	MB	B	MB		M
Windows 7 professional	M	B	MB	B	MB		M
Equipamiento informático							
Servidor hp proliant	MA	M	M	MB	MB		MA
Impresoras Lexmark, Hp, Xerox	A	MB	MB	MB	MB		A
Escáner Fujitsu 7160, 6140, 6770	A	MB	MB	MB	MB		A
Switch hp v1910	MA	M	MB	MB	MB		MA
Switch Planet FNSW 2401	MA	M	MB	MB	MB		MA
Switch 3Com 4200	MA	M	MB	MB	MB		MA
Access Point Ubiquiti	MB	MB	MB	MB	MB		MB
Planta Telefónica	A	B	A	MB	MB		A
DVR Gsecurity	M	MB	M	MB	MB		M
Computador personal	A	MB	B	MB	MB		A
Celular empresarial	M	MB	B	MB	MB		M
Redes de comunicaciones							
Red Local	MA	A	A	M	B		MA
Red Inalámbrica	B	B	M	B	MB		M
Red telefónica	A	M	B	MB	MB		A
Internet banda ancha 4 m	MA	M	MB	MB	MB		MA
Internet banda ancha 2 m	MA	M	MB	MB	MB		MA
Internet dedicado 8 m	MA	M	MB	MB	MB		MA
Soportes de información							
Disco duro extraíble de 1 T	A	A	MB	MB	MB		A

Memorias USB	MB	MB	MB	MB	MB		MB
DVD de respaldo	A	A	MB	MB	MB		A
Equipamiento auxiliar							
Aire Acondicionado	B	MB	MB	MB	MB		B
1 UPS de 1Kva	M	M	MB	MB	MB		M
Cableado en fibra óptica	MA	B	MB	MB	MB		MA
Cableado eléctrico	MA	MB	MB	MB	MB		MA
Escritorios	M	MB	MB	MB	MB		M
Rack de piso de 24 u	MB	MB	MB	MB	MB		MB
Instalaciones							
Edificio	MA	B	MB	MB	MB		MA
Personal							
Comerciantes y población en general	A	MB	MB	MB	MB		A
Director Administrativo y Financiero	M	MB	A	MB	MB		A
Ingeniero de Sistemas	M	MB	A	MB	MB		A
Coordinadora de Sistemas	M	MB	A	MB	MB		A
Ingeniero de Sistemas	M	MB	A	MB	MB		A
Jefe de Archivo,	B	MB	M	MB	MB		M
Auxiliar de Archivo	B	MB	M	MB	MB		M
Auxiliar de Archivo	B	MB	M	MB	MB		M
Auxiliar de Archivo	B	MB	M	MB	MB		M
Jefe de Caja	B	MB	M	MB	MB		M
Auxiliar de Caja	B	MB	M	MB	MB		M
Auxiliar de Caja	B	MB	M	MB	MB		M
Auxiliar de Registro	B	MB	M	MB	MB		M
Asistente de Registros Publico	B	MB	M	MB	MB		M
Jefe de Registros Públicos	B	MB	M	MB	MB		M
Jurídico	B	MB	M	MB	MB		M
Jefe de Conciliación	B	MB	M	MB	MB		M
Secretaria General	B	MB	M	MB	MB		M
Coordinadora de Desarrollo Empresarial	B	MB	M	MB	MB		M
Asistente Administrativa y Contable	B	MB	M	MB	MB		M
CertiCámara s	M	MB	M	MB	MB		M
UNE	M	MB	M	MB	MB		M
Movistar	M	MB	M	MB	MB		M
ConfeCámara s	M	MB	M	MB	MB		M
Confecámaras	M	MB	M	MB	MB		M
Servicios generales	MB	MB	B	MB	MB		B

Fuente: Autores del proyecto.

Estimación del riesgo potencial. Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

Basados en la metodología Magerit, realizamos el cálculo para hallar el Riesgo potencial a través de la siguiente tabla.

Tabla 22. Calculo del riesgo potencial.

RIESGO		**Probabilidad**				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Autores del proyecto.

Para hallar el riesgo, seleccionamos el valor de la probabilidad de la ocurrencia de las amenazas en cada activo, se obtuvo el valor mayor en representación del activo y el valor del impacto seleccionado de la tabla de estimación del impacto potencial.

Tabla 23. Riesgo.

Activos	**Impacto x Probabilidad**						**Riesgo**
	D	I	C	A	T		
Arquitectura							
Router Board Mikrotik de UNE	M	M	M	B	MB		M
Modem Huawei de UNE	A	M	M	B	MB		A
Multiservice Gateway Allied Telesis, Equipo de Confecámaras	M	M	B	B	MB		M

Router Cisco 1700	A	A	B	B	MB		A
Modem Miltrastar de Movistar 4 m	M	M	M	B	MB		M
Modem Nukon de Movistar 2 m	M	M	M	B	MB		M
Información							
información de registro	MA	MA	MB	MA	M		MA
Información contable	MA	MA	MA	MA	M		MA
Información administrativa	A	MA	M	MA	M		MA
Copias de respaldo de la información de registro, administrativa y financiera.	A	MA	M	M	MB		MA
Datos de configuración	M	MA	M	B	B		MA
Datos de gestión interna (usuarios, permiso)	M	MA	A	A	B		MA
Registro de actividades	B	A	M	M	B		A
Claves criptográficas							
Firma digital	MA	A	MA	A	B		MA
Servicios							
Correo electrónico empresarial	A	A	MA	MA	A		MA
Soporte a usuarios externos (manejo de trámites en línea) a través de chat online y vía telefónica.	M	B	B	B	B		M
Gestión de privilegios en los sistemas de información SII y DocuWare	A	A	B	A	M		A
Servicio de transferencia de fichero FTP hacia el servidor SIREP	A	A	B	A	M		A
Servicio de registros públicos a usuarios externos a través de la web	A	A	B	B	A		A
Servicio de registros públicos a usuarios internos.	MA	MA	A	MA	A		MA
Servicio radicación y consulta de expedientes digitalizados a usuarios internos.	A	A	M	A	A		A
Aplicaciones informáticas							
SIREP	MA	MA	A	A	B		MA
DocuWare	A	MA	A	A	B		MA
SII	MA	MA	A	A	B		MA
Jsp7	MA	MA	MA	MA	M		MA
Microsoft Office Hogar y Empresa 2013	B	M	B	B	B		M
Antivirus kaspersky	B	M	B	B	B		M
Cpanel, administrador de Servidor de correo electrónico y pagina web.	M	M	A	A	B		A
SQL Server 2012 Sistema de Gestión de Base de Datos	A	MA	M	A	B		MA
Mozilla Firefox 47.0.1	B	B	B	B	B		B

Google Chrome	B	B	B	B	B		B
Windows Server 2012	MA	MA	MA	A	B		MA
Windows 8.1	A	M	B	M	B		A
Windows 8	A	M	B	M	B		A
Windows 7 professional	A	M	B	M	B		A
Equipamiento informático							
Servidor hp proliant	MA	M	M	MB	MB		MA
Impresoras Lexmark, Hp, Xerox	A	MB	MB	MB	MB		A
Escáner Fujitsu 7160, 6140, 6770	A	MB	MB	MB	MB		A
Switch hp v1910	MA	M	MB	MB	MB		MA
Switch Planet FNSW 2401	MA	M	MB	MB	MB		MA
Switch 3Com 4200	MA	M	MB	MB	MB		MA
Access Point Ubiquiti	MB	MB	MB	MB	MB		MB
Planta Telefónica	A	B	A	MB	MB		A
DVR Gsecurity	M	MB	M	MB	MB		M
Computador personal	A	MB	B	MB	MB		A
Celular empresarial	M	MB	B	MB	MB		M
Redes de comunicaciones							
Red Local	MA	MA	MA	A	M		MA
Red Inalámbrica	B	B	M	B	MB		M
Red telefónica	MA	A	M	B	B		MA
Internet banda ancha 4 m	MA	A	B	B	B		MA
Internet banda ancha 2 m	MA	A	B	B	B		MA
Internet dedicado 8 m	MA	A	B	B	B		MA
Soportes de información							
Disco duro extraíble de 1 T	MA	MA	B	B	B		MA
Memorias USB	B	B	B	B	B		B
DVD de respaldo	MA	MA	B	B	B		MA
Equipamiento auxiliar							
Aire Acondicionado	M	B	B	B	B		M
1 UPS de 1Kva	M	M	MB	MB	MB		M
Cableado en fibra óptica	MA	B	MB	MB	MB		MA
Cableado eléctrico	MA	MB	MB	MB	MB		MA
Escritorios	M	MB	MB	MB	MB		M
Rack de piso de 24 u	MB	MB	MB	MB	MB		MB
Instalaciones							
Edificio	MA	B	MB	MB	MB		MA
Personal							
Comerciantes y población en general	MA	B	B	B	B		MA
Director Administrativo y Financiero	A	B	MA	B	B		MA
Ingeniero de Sistemas	A	B	MA	B	B		MA
Coordinadora de Sistemas	A	B	MA	B	B		MA
Ingeniero de Sistemas	A	B	MA	B	B		MA

Jefe de Archivo,	M	B	A	B	B		A
Auxiliar de Archivo	M	B	A	B	B		A
Auxiliar de Archivo	M	B	A	B	B		A
Auxiliar de Archivo	M	B	A	B	B		A
Jefe de Caja	M	B	A	B	B		A
Auxiliar de Caja	M	B	A	B	B		A
Auxiliar de Caja	M	B	A	B	B		A
Auxiliar de Registro	M	B	A	B	B		A
Asistente de Registros Publico	M	B	A	B	B		A
Jefe de Registros Públicos	M	B	A	B	B		A
Jurídico	M	B	A	B	B		A
Jefe de Conciliación	M	B	A	B	B		A
Secretaria General	M	B	A	B	B		A
Coordinadora de Desarrollo Empresarial	M	B	A	B	B		A
Asistente Administrativa y Contable	M	B	A	B	B		A
CertiCámara s	A	B	A	B	B		A
UNE	A	B	A	B	B		A
Movistar	A	B	A	B	B		A
ConfeCámara s	A	B	A	B	B		A
Confecámaras	A	B	A	B	B		A
Servicios generales	B	B	M	B	B		M

Fuente: Autores del proyecto.

Mediante el análisis de riesgo se determinó que la Cámara de Comercio de Aguachica, se encuentra altamente expuesta a una serie de amenazas, obteniendo por consiguiente el riesgo inminente a cada uno de los activos de información de la entidad atentando contra la confidencialidad integridad, disponibilidad, autenticidad y Trazabilidad. Donde los riesgos representados con el color Gris Claro que se representan cualitativamente con la letra MB identifican el riesgo **despreciable**, color Gris Oscuro que se comprenden cualitativamente con la letra B es la estimación del riesgo **bajo**, el nivel de riesgo **apreciable** que está representado con el color amarillo y comprende con la letra M, el riesgo **importante** que se representa con el color rosado y comprende la letra A y el riesgo **crítico** con las letras MA.

Al Estimar el Riesgo Potenciar se evidencio lo siguiente:

Tabla 24. Resultados de estimación del riesgo.

MB	B	M	A	MA	Total de activos
2	3	14	35	34	88

Fuente: Autores del proyecto.

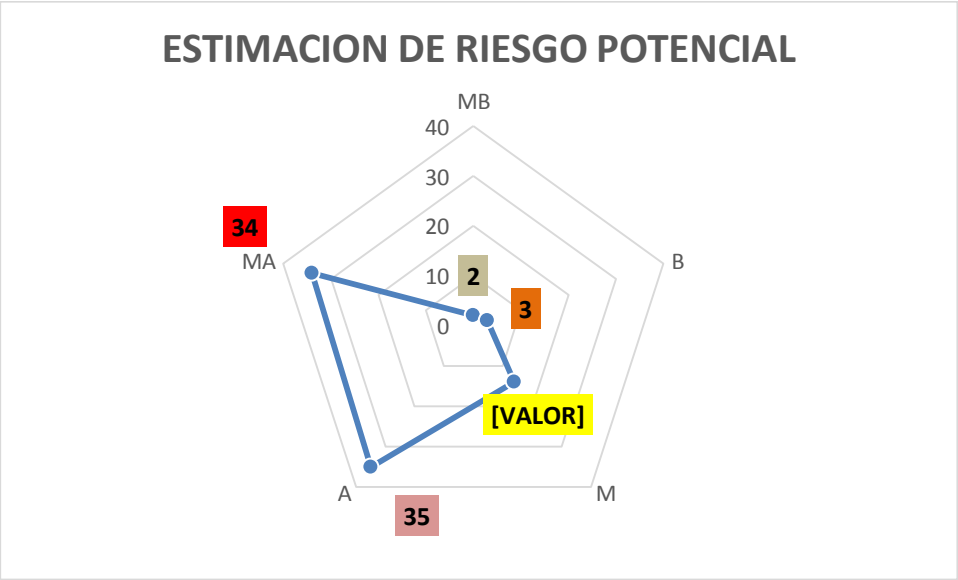

Tabla 25. Resultados del riesgo potencial

Fuente: Autores del proyecto.

A través de la anterior imagen se puede observar que de 88 activos de la Cámara de Comercio de Aguachica, el 40 % de ellos están en el nivel de riesgo Alto, el 39 % en Muy Alto, el 16 % en nivel Medio, el 3% en nivel Bajo y solo el 2% en nivel muy bajo.

Se evidencia que los activos de información como son (información de registro, Información Contable, Información administrativa, Copias de respaldo de la información de registro, administrativa y financiera y Datos de configuración) están en un nivel de riesgo muy alto y el

activo de información (Datos de gestión interna (usuarios, permiso)), está en un nivel de Riesgo Alto, esto quiere decir que los activos de mayor importancia de acuerdo a la valoración para la Cámara de Comercio de Aguachica, son los que mayor riesgo tienen para el sistema.

Oficio de entrega de análisis de riesgos, ver **Apéndice E**

4.2.2. Enunciado de aplicabilidad, los objetivos de control y los controles que son relevantes al SGSI de la organización.

Políticas de seguridad.

POLÍTICAS DE SEGURIDAD		
POLÍTICAS DE SEGURIDAD LA INFORMACIÓN.	• Dirección de la Alta Gerencia para la Seguridad de la Información.	Control que **Aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que esta es la autorización de la alta gerencia de la cámara de Comercio de Aguachica, Cesar, (Gerencia) para el diseño de la política de seguridad de la información.
	• Políticas de Seguridad de la Información.	Control que **Aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido que mediante esta se puede proporcionar indicaciones para la gestión y soporte de la seguridad de la información de acuerdo con los requisitos empresariales, con la legislación y las normativas aplicables en la Cámara de Comercio de Aguachica,
	• Revisión de las Políticas de Seguridad de la Información.	Control que **Aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, la política de seguridad de la información debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a

		fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.		
Organización Interna	• Organización Interna	Control que **Aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que este promueve la gestión de la seguridad de la información dentro de las instalaciones de la institución.
	• Roles y Responsabilidad de Seguridad de la Información.	Control que **Aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que cada uno de los funcionarios de la institución debe tener obligaciones de acuerdo a la política de seguridad de la información de la institución.
	• Contacto con autoridades.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido la institución no tiene contacto con los distintos entes autoritarios tales como: agencia colombiana de protección datos, alianza internacional de protección y seguridad cibernética, Inteco-OSI, entre otros.
	• Seguridad de la Información en la gestión de proyectos.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido la institución no cuenta con políticas de seguridad de la información en la elaboración de proyectos de investigación.
	• Segregación de deberes.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que consiste en que un trabajador que realiza una tarea puede ser supervisado por otro trabajador para que la tarea se complete de manera satisfactoria.
	• Dispositivos móviles y teletrabajo.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la institución no cuenta con la tecnología necesaria para implementar este tipo de herramientas que facilitan el desempeño de las

		funciones.
	• Política de dispositivos móviles.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, para el regalamiento de la conectividad de los Smartphone a las redes de la institución
	• Teletrabajo.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la institución no cuenta con la tecnología necesaria para implementar este tipo de herramientas que facilitan el desempeño de las funciones.
SEGURIDAD EN LOS RECURSOS HUMANOS.		
Previo al Empleo.	• Previo al Empleo.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, para asegurar que los empleados, los contratistas y los terceros entiendan sus responsabilidades, y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de Hurto, fraude o de uso indebido de los recursos.
	• Verificación de antecedentes	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, debido a que la alta gerencia debe de indagar sobre los antecedentes previos del personal profesional que se encuentra en proceso de contratación, mitigando el riesgo que se puede presentar al contratar personal poco idóneo para la realización de las tareas.
	• Términos y condiciones del empleo.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, donde se especifican los términos y condiciones legales y contractuales para los cuales está contratado el personal profesional.
Durante el Empleo.	• Durante el Empleo.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde la dirección verifica el cumplimiento de las labores para las

		cuales fueron contratados.
	• Responsabilidades de la Alta Gerencia.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la alta gerencia de la institución debe tener el compromiso y responsabilidades en todos los procesos realizados por dichos estamentos.
	• Conciencia, educación y entrenamiento de Seguridad de la Información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la alta gerencia puede promulgar la capacitación del personal de la Organización en el manejo de normativas que garanticen la seguridad de los datos.
	• Proceso disciplinario.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la alta gerencia puede establecer procesos disciplinarios, cuando los funcionarios de la misma se excedan de sus funciones.
• Terminación y Cambio de Empleo.	Terminación y Cambio de Empleo.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la alta gerencia debe asegurar que todos los usuarios internos o contratistas de la institución, que ya no laboren, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será pertinente hasta que la institución lo considere.
	• Término de responsabilidades o cambio de empleo.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la alta gerencia debe asegurarse que cuando usuarios internos o contratistas cambien de puesto de trabajo, hayan firmado un acuerdo de confidencialidad cuyo cumplimiento será pertinente hasta que la institución lo considere.
GESTIÓN DE ACTIVOS		

Responsabilidad de los Activos.	• Inventario de activos.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la alta gerencia debe tener todos los activos claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
	• Propiedad de activos.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que toda la información y activos asociados a los recursos para el tratamiento de la información deben pertenecer a una parte designada de la Organización.
	• Uso aceptable de los activos.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido los activos de información deben garantizarse su integridad, disponibilidad y confidencialidad.
	• Clasificación de la Información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la alta gerencia debe tener la clasificación de la información sensible de la institución y a si mismo medidas que garanticen las características básicas de la misma.
	• Etiquetado de la información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se debe desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización.
	• Manejo de activos.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido los activos de información deben garantizarse su integridad, disponibilidad y confidencialidad.
	• Devolución de activos.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde la alta gerencia debe cerciorarse de la que los activos

		cuentes al momento de su devolución con la respectiva integridad.
	• Manejo de Medios.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que en la institución existe una política en donde se evite la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio. Estos medios se deberían controlar y proteger de forma física.
	• Gestión de medios removibles.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la alta gerencia puede regular el uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información de la institución y estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera.
	• Eliminación de medios.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, en donde se debe establecer la eliminación de información sensible de la organización de medios removibles como (CDs, DVDs, USBs)
	• Transporte de medios físicos	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.
CONTROL DE ACCESO		

Requerimientos de Negocio para el Control de Acceso	• Política de control de acceso	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido que en la institución pueden reglamentar mecanismos de control de acceso a las instalaciones físicas y a los recursos de la Organización mediante la cartelización y entre otros mecanismos que regulen el acceso del personal y a su vez clasificándolo mediante roles.
	• Política en el uso de servicios de red	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que en la Institución pueden reglamentar el uso de los servicios de red con la que la Organización cuenta, mediante restricciones a páginas web, entre otras.
	• Gestión de Accesos de Usuario	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido que la alta gerencia puede implementar políticas en donde se garanticen el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.
	• Registro y baja del usuario	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la institución cuenta con sistemas de automatizados que les permita realizar estas funciones.
	• Gestión de privilegios	Control que que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, cuenta con sistemas de automatizados que les permita realizar estas funciones.
	• Gestión de información de autenticación secreta de usuarios.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, cuenta con sistemas automatizados que les permita realizar estas funciones.
	• Revisión de derechos de acceso de usuarios.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que se encuentra

		establecida una política de seguridad de la información dentro de la institución que reglamente dicho control.
	• Responsabilidades del Usuario	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que se encuentra establecida una política de seguridad de la información dentro de la institución que reglamente dicho control.
	• Uso de información de autenticación secreta.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que se encuentra establecida una política de seguridad de la información dentro de la institución que reglamente dicho control.
	• Control de Acceso de Sistemas y Aplicaciones.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que se encuentra establecida una política de seguridad de la información dentro de la institución que reglamente dicho control.
	• Restricción de acceso a la información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la alta gerencia restringe el acceso a la información sensible de la institución.
	• Procedimientos de conexión segura.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la institución no implementa procedimientos para establecer conexiones seguras en la red.
	• Sistema de gestión de contraseñas.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la institución no cuenta con servidores de contraseñas que les brinde este servicio.
	• Uso de programas y utilidades privilegiadas.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido dentro de la institución no se tiene estandarizado la utilización

		de un sistema de información automatizado.
	• Control de acceso al código fuente del programa.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que los usuarios de la institución no tienen acceso a los códigos fuentes de las aplicaciones utilizadas dentro de la organización.
CIFRADO.		
Controles Criptográficos	• Política en el uso de controles criptográficos.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que en la institución no se aplican políticas de cifrado de la información.
	• Gestión de llaves.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la institución no cuenta con servidores de contraseñas que les brinde este servicio.
SEGURIDAD FÍSICA Y AMBIENTAL.		
Áreas Seguras	• Perímetro de seguridad físico.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, puesto que ya se realizó en encerramiento de las instalaciones, y en la institución cuentan con los mecanismos para la protección de las instalaciones física de la Organización.
	• Controles físicos de entrada.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que en la institución no cuentan con mecanismos de acceso de ingreso a las instalaciones de la Organización.
	• Seguridad de oficinas, habitaciones y facilidades.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que las instalaciones y oficinas cuentan con los requerimientos mínimos de seguridad en los recintos.
	• Protección contra amenazas externas y del ambiente.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, puesto que la Organización no se cuenta con la infraestructura para la

		prevención de amenazas externas y desastres naturales.
	• Trabajo en áreas seguras.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, debido a que los funcionarios de la Organización realizan sus labores en áreas seguras.
	• Áreas de entrega y carga.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la tipo de actividad económica realizada por la institución.
Equipo.	• Instalación y protección de equipo.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, puesto a que la alta gerencia contrata periódicamente personal capacitado para realizar estas funciones.
	• Servicios de soporte.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, puesto a que la alta gerencia contrata periódicamente personal capacitado para realizar estas funciones.
	• Seguridad en el cableado.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que el estado del cableado estructurado de la institución se encuentra en óptimas condiciones.
	• Mantenimiento de equipos.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, puesto a que la alta gerencia contrata periódicamente personal capacitado para realizar estas funciones.
	• Retiro de activos.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, cuando la alta gerencia logra la adquisición de nuevos activos para la institución.
	• Seguridad del equipo.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la alta gerencia tiene personal a cargo de la vigilancia y aseguramiento de los equipos.

	• Eliminación segura o reúso del equipo.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que los usuarios no realizan eliminación segura de la información que albergan en sus equipos de cómputo.
	• Equipo de usuario desatendido.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que los funcionarios de la Organización no aplican ningún método para suspender o hibernar sus equipos, quedando estos desprotegidos a cualquier tipo de riesgo.
	• Política de escritorio limpio y pantalla limpia.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que el personal administrativo de la Organización no implementa la buena práctica de mantener el escritorio limpio sin ningún tipo de icono o archivos.
SEGURIDAD EN LAS OPERACIONES.		
Procedimientos Operacionales y Responsabilidades.	• Documentación de procedimientos operacionales.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que en la institución no cuentan con manuales de procedimientos que le permitan realizar sus labores.
	• Gestión de cambios.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, debido a que no se realizan e implementen adecuadamente todos los cambios necesarios en la infraestructura y servicios de TI
	• Gestión de la capacidad.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que los servicios TI no están respaldados por una capacidad de proceso y almacenamiento suficiente y correctamente dimensionada.
	• Separación de los ambientes de desarrollo, pruebas y operación.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la Organización no cuenta con ambientes de desarrollo y de operación.

Protección de Software Malicioso	• Controles contra software malicioso.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido que dentro de la Organización se pueden realizar controles y políticas para el uso de software contra código malicioso.
Copias de seguridad.	• Respaldo de información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la alta gerencia puede establecer políticas para el respaldo y resguardo de la información crítica de la institución.
Registro de actividad y supervisión.	• Registro de eventos.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, donde se llevara todos los registros de los eventos que realicen lo funcionarios en cada uno de los sistemas de información de la Organización.
	• Protección de registros de información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se pueden llevar de forma segura los registros de la información sensible de la institución.
	• Registros de Administrador y Operador.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se deben registrar las actividades del administrador del sistema y de la operación del sistema.
	• Sincronización de relojes.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se deben sincronizar los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad, con una fuente acordada y exacta de tiempo.
Control de Software Operacional.	• Instalación de software en sistemas operacionales.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se debe realizar la instalación de software seguro y confiable en las dependencias que lo requiera para la realización de sus labores.

Gestión de Vulnerabilidades Técnicas.	• Gestión de Vulnerabilidades Técnicas.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, contribuyendo a reducir los riesgos originados por la explotación de vulnerabilidades técnicas publicadas.
	• Restricciones en la instalación de software.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido que la alta gerencia debe regular y restringir la instalación de software no seguro para garantizar la integridad, confidencialidad y disponibilidad de la información.
Consideraciones de Auditoria de Sistemas de información.	• Controles de Auditoría de Sistemas de Información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica Cesar. debido a que la institución cuenta con una oficina de auditoria interna que le permita hacer seguimiento a los sistemas de información
SEGURIDAD EN LAS TELECOMUNICACIONES.		
Gestión de Seguridad en Red.	• Controles de red.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en el cual se deben mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.
	• Seguridad de los servicios en red.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en los cuales la alta gerencia puede implementar herramientas que brinden la seguridad en la red de datos.
	• Segregación en redes	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se debe segregar o dividir los grupos de usuarios, servicios y sistemas de información en las redes, lo cual garantiza la seguridad de la información en cada una de las redes de datos de la institución.
Transferencia de Información.	• Políticas y procedimientos para la	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en la alta gerencia por medio de

	transferencia de información.	la política de seguridad de la información establezca procedimiento para la transferencia segura de la información de la institución.
	• Acuerdos en la transferencia de información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se deben establecer acuerdos para el intercambio de información y software entre la organización y las partes externas.
	• Mensajería electrónica.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se proteja adecuadamente la información contenida en la mensajería electrónica. Con herramientas gratuitas que generan firmas codificadas según el formato PKCS#7 o CMS.
	• Acuerdos de confidencialidad o no-revelación	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en los cuales al momento de la contratación el personal administrativo acepte un acuerdo de confidencialidad en las labores en las que se desempeñara.
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.		
Requerimientos de Seguridad de Sistemas de Información	• Análisis y especificación de requerimientos de seguridad.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, al momento de adquirir nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes deberían especificar los requisitos de los controles de seguridad, que garanticen la confidencialidad, integridad y disponibilidad de los datos.
	• Aseguramiento de servicios de aplicación en redes públicas.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido que la institución cuenta con aplicaciones en redes públicas.
	• Protección de transacciones de servicios de aplicación.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido que la institución cuenta con servicios de aplicación.

Seguridad en los Procesos de Desarrollo y Soporte.	• Política de desarrollo seguro.	Control que **aplica** dentro del Comercio de Aguachica. En donde se debe establecer una política por la alta gerencia para el desarrollo de software seguro y confiable.
	• Procedimientos de control de cambios. .	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se deberán controlar los cambios en los sistemas y en los recursos de tratamiento de la información.
	• Revisión técnica de aplicaciones después de cambios a la plataforma operativa.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se deberá revisar y probar las aplicaciones críticas de negocio cuando se realicen cambios en el sistema operativo, con objeto de garantizar que no existen impactos adversos para las actividades o seguridad de la Organización.
	• Restricción de cambios a paquetes de software.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Se deberá desaconsejar la modificación de los paquetes de software, restringiéndose a lo imprescindible y todos los cambios deberían ser estrictamente controlados.
	• Procedimientos de desarrollo de sistemas.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se deberán documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten.
	• Entorno de desarrollo seguro.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, en donde el desarrollador no se encuentra en entorno de desarrollo seguro para la realización del software
	• Desarrollo tercerizado.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la institución recurre a terceros para el desarrollo de software que le permite realizar los procesos propios de la institución

		como lo es el Academusoft, SIJADIT, entre otros.
	• Pruebas de seguridad del sistema.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido que al momento de adquirir u nuevo software este debe de estar sometido para determinar qué tan segura estará la información almacenada en él.
	• Pruebas de aceptación del sistema.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido que, dentro de la institución a la hora de adquirir un nuevo software, se debe realizar este tipo de pruebas para determinar el nivel de aceptación que tendrá en la institución.
Datos de Prueba.	• Protección de datos de prueba.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la actividad económica de la Institución no es el desarrollo de software.
RELACIONES CON PROVEEDORES.		
Seguridad en Relaciones con el Proveedor.	• Política de Seguridad de la Información para relaciones con proveedores.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la institución al contratar o recibir productos o servicios estos deben de garantizar que se le binde las características primordiales de la información.
	• Atención de tópicos de seguridad dentro de los acuerdos con proveedores.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que dentro de los contratos establecidos con los proveedores se deben establecer tópicos para la seguridad de la información.
	• Cadena de suministros de TIC.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a las adquisiciones de equipos tecnológicos que realiza la institución con los proveedores.

	• Gestión de Entrega de Servicios de Proveedor.	Control que aplica dentro de la Organización, debido a que los funcionarios encargados de estas labores pueden verificar la adecuada entrega de los servicios
	• Monitoreo y revisión de servicios de proveedor	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la organización, debe monitorear periódicamente los productos servicios que los proveedores ofrecen.
	• Gestión de cambios a servicios de proveedor.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, puesto que la organización puede gestionar los cambios a los servicios que ofrecen los distintos productos o servicios que ofrecen los proveedores.
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.		
Gestión de Incidentes de Seguridad de la Información y Mejoras.	• Responsabilidades y Procedimientos.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la alta gerencia debe implementar y asegurar la operación correcta y segura de los recursos y el tratamiento de la información.
	• Reporte de eventos de Seguridad de la Información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en el cual se debe llevar un reporte detallado de los eventos ocurridos que involucran la seguridad de la información.
	• Reporte de debilidades de Seguridad de la Información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se debe llevar un reporte especificado de los sucesos ocurridos en los cuales se vea comprometidos las características básicas de la información.
	• Valoración y decisión de eventos de Seguridad de la Información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde la alta gerencia debe tomar medidas preventivas y correctivas sobre los sucesos que hayan comprometido la

		confidencialidad, integridad y disponibilidad de la información de la institución.
	• Respuesta a incidentes de Seguridad de la Información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde la alta gerencia implanta planes de contingencia para mitigar el riesgo de pérdida de la información.
	• Aprendizaje de incidentes de Seguridad de la Información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde los incidentes presentados relacionados con la seguridad de la información sirvan como mecanismos de defensa y acciones correctivas para que los incidentes relacionados con la seguridad de la información no se vuelvan a presentar.
	• Colección de evidencia.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se realiza la recolección de toda la información con los incidentes y riesgos que se han presentado con respecto a la seguridad de la información.
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO.		
Seguridad de la Información en la Continuidad.	• Planeación de Seguridad de la Información en la continuidad.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en el cual se debe desarrollar y mantener un proceso de gestión de la continuidad del negocio en la organización que trate los requerimientos de seguridad de la información necesarios para la continuidad del negocio.
	• Implementación de Seguridad de la Información en la continuidad.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en el cual se aplican estándares y metodologías que le permitan a la Organización poder continuar con el sistema de gestión de la seguridad de la información.

	• Verificación, revisión y evaluación de Seguridad de la Información en la continuidad.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido que aquí es donde se evalúa los resultados que se obtienen median el ciclo PHVA que estipula la norma, el cual es dinámico en el cual se establecen parámetros para la continuidad del negocio.
CUMPLIMIENTO		
Cumplimiento de los requisitos legales y contractuales	• Identificación de legislación aplicable y requerimientos contractuales.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en donde se analizan todos los requisitos estatutarios, de regulación u obligaciones contractuales relevantes, así como las acciones de la Empresa para cumplir con los requisitos, que deben ser explícitamente definidos, documentados y actualizados para cada uno de los sistemas de información y la Organización.
	• Derechos de propiedad intelectual (IPR)	Control que **no aplica** dentro de la cámara de comercio de Aguachica, debido a que dentro de esta no se registra propiedades intelectuales.
	• Protección de información documentada.	Control que **aplica** dentro de la cámara de comercio de Aguachica, debido a que la información vital de la organización debe ser respaldada.
	• Privacidad y protección de información personal identificable.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, debido a que en la política de Seguridad de la Información debe estar contemplado un capitulo dirigido a la privacidad de la información.
	• Regulación de controles criptográficos.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la institución no cuenta con la infraestructura tecnológica suficiente para implementar estas técnicas de cifrado de datos.
	• Regulación de controles criptográficos.	Control que **no aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido a que la institución no

		cuenta con la infraestructura tecnológica suficiente para implementar estas técnicas de cifrado de datos.
	Revisión independiente de Seguridad de la Información.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido después de la implementación de políticas de seguridad de la información, se realiza una análisis independiente muy minucioso de cada una de las partes que conforman el sistema de gestión de seguridad de la información en la organización.
	• Cumplimiento con políticas y estándares de seguridad.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, aquí es donde se verifica por parte de la alta gerencia si se logró el cumplimento de la políticas y de los estándares de seguridad propuestos.
	• Inspección de cumplimiento técnico.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en este ítem se verifica que el cumplimiento de la política cumpla con todas especificaciones técnicas.
Revisiones de la seguridad de la información.	• Revisión independiente de la seguridad de la información	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, debido que se debe de hacer seguimiento y evaluación a la política de seguridad de la información.
	• Cumplimiento de las políticas y normas de seguridad.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en este ítem se verifica que el cumplimiento de la política cumpla con todas especificaciones técnicas.
	• Comprobación del cumplimiento.	Control que **aplica** dentro de la Cámara de Comercio de Aguachica, Cesar, en este ítem se verifica que el cumplimiento de la política cumpla con todas especificaciones técnicas.

Fuente: Autores del proyecto.

4.3. El alcance y las políticas del sistema de gestión de seguridad de la información (SGSI) para la cámara de comercio de Aguachica Cesar.

Introducción. Con el ánimo de mejorar la estrategia de Seguridad de la información de la CÁMARA DE COMERCIO DE AGUACHICA. 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 tecnológicos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

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.

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;
- Proveedores de recursos informáticos.

- Entidades de Control

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

- Otras Entidades

- DIAN;
- ICONTEC

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.

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 o poner en riesgo a un sistema u organización.

Backup: Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.

Coordinación de Planeación e Innovación: Es el 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.

Comité de Seguridad: Equipo de trabajo conformado por el presidente ejecutivo, coordinador de tecnología 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, trazabilidad 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 no autorizados.

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 encriptación: 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.

RESPONSABLE

Compromiso de la dirección

- La dirección debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento 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; o 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 la necesidades de la mejora continua;

- Asegurando que se realizan auditorías internas.

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; o 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.

Procedimiento. 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.

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.

Políticas generales de seguridad de la información. Estas normas son de obligatorio cumplimiento por parte de todos los usuarios de recursos informáticos y se han clasificado en:

- Directrices de la organización en seguridad de la información.
- Aspectos organizativos de la seguridad de la información.
- Seguridad ligada a los recursos humanos.
- Gestión de activos.
- Control de accesos.
- Cifrado.
- Seguridad física y ambiental.
- Seguridad en la operativa.
- Seguridad en las telecomunicaciones.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Relaciones con suministradores.
- Gestión de incidentes en la seguridad de la información.
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
- Cumplimiento.

Dispositivos para movilidad y teletrabajo.

Dispositivos móviles: al interior de la Cámara de comercio de Aguachica, se reconoce el alto grado de exposición que presenta la información y los datos de la institución almacenados en dispositivos móviles (computadores portátiles, notebooks, PDA, Smartphone, entre otros.).

Corresponde a la dirección administrativa y funcionarios gestores de los recursos tecnológicos, elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información.

Las redes inalámbricas potencialmente introducen nuevos riesgos de seguridad que deben ser identificados, valorados y tratados de acuerdo a los lineamientos de la Política de Seguridad de la información en materia de redes.

- Los usuarios necesitaran permiso para instalar o desinstalar aplicaciones en los dispositivos móviles. Que sean de propiedad de la organización, No se les permite acceder al sistema y a las aplicaciones virtuales de las máquinas.

- No acceder a los enlaces solicitados a través de SMS/MMS/Email podría ser código malicioso.

- La configuración, modificación o eliminación de software aplicativo sobre los dispositivos móviles es responsabilidad exclusiva del área asignada para tal fin.

- Para computadores portátiles, lo recomendable es que los usuarios pertenezcan al dominio de red existente en la organización, con políticas de complejidad y caducidad adecuadas. En el caso de teléfonos móviles/tablets, el PIN o contraseña del dispositivo debe, al menos, existir. En el caso de dispositivos Android, deben evitarse los controles de acceso basados en patrones de puntos, siendo lo más deseable el control biométrico

por huella dactilar, en aquellos dispositivos que lo soporten. En caso que sea necesario un PIN o contraseña, se recomienda forzar teclado alfanumérico, y cierta complejidad en la contraseña exigiendo letras minúsculas, mayúsculas y números, así como el bloqueo temporal según se va fallando en la autenticación. En algunos dispositivos con información muy sensible, podría Activarse incluso el check de borrado completo del dispositivo si hay 10 fallos seguidos en la autenticación.

Tanto en computadores portátiles como en Smartphone y tablets, habrá de activarse las políticas de bloqueo de sesión (o de apagado de pantalla) solicitando autenticación o PIN para volver a interactuar con el dispositivo. El periodo máximo de inactividad antes de dicho bloqueo se recomienda que se fije en 1 minuto para Smartphone y tablets, así como 3 minutos para computadores portátiles.

Tapar físicamente las cámaras integradas, el malware de hoy en día permite activar la webcam incorporada en dispositivos móviles a voluntad del atacante, por lo que es posible disponer de una cámara y un micrófono de forma remota, escuchando y viendo al usuario. A fin de proteger la privacidad del usuario, así como de la información hablada por su parte (y que pueda ser monitorizada en remoto, a través del micrófono), se recomienda bloquear físicamente la webcam con cinta aislante negra, con la opacidad necesaria para que no se pueda ver nada. Igualmente, en computadores portátiles, se recomienda desactivar el micrófono incorporado en el equipo

Computación en nube: la información producida por los procesos de la Cámara de comercio de Aguachica, no debe ser alojada en dispositivos de almacenamiento en la nube, ya que se expondría a afectarse la integridad y confidencialidad de los datos, en caso tal de contratarse un servicio de cloud computing para la institución, podrán alojarse los archivos que requieran copias de seguridad, almacenamiento y difusión masiva.

Política de uso de portátiles.

- 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 estar cifrada.
- Cuando el equipo deba ser devuelto a La Cámara de Comercio para reparación, mantenimiento etc. La información confidencial deberá respaldarse en una copia de seguridad y posteriormente borrada.
- De la información de usuario debe generarse copia de respaldo, por solicitud del usuario al área de sistemas
- Protección del equipo portátil
- No dejar el computador móvil en lugares públicos
- Cuando viaje el computador portátil no debe ir dentro de su maletero siempre debe llevarse en su equipaje mano.

- No es permitido que el computador portátil sea utilizado por familiares y/o amigos

Seguridad ligada a los recursos humanos. Se debe considerar como recurso humano a todo el personal interno, externo, temporal en el aseguramiento de las responsabilidades que son asignadas a cada uno, asociadas con sus respectivos roles, para reducir el riesgo de Hurto, fraude, sabotaje o uso inadecuado de los activos de información.

Todos y cada uno de los individuos que conforman la organización deben estar conscientes de las vulnerabilidades y amenazas que afectan la seguridad de la información y sus obligaciones y deberes en cuanto a acatar la política de seguridad de la organización; establecida para la reducción del riesgo de error humano.

La responsabilidad de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe de departamento o supervisor del contrato; en todo caso el proceso de cambio de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

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.

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

Antes de la contratación. Para toda persona que ingrese a la Cámara de Comercio de Aguachica, la dirección administrativa debe asegurar las responsabilidades sobre seguridad de la información de manera previa a la contratación. Así mismo incluir un acuerdo de confidencialidad, Esta tarea debe reflejarse en una adecuada descripción del cargo, funciones, investigación de antecedentes y en los términos y condiciones de la contratación.

Durante la contratación. Definición de las responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de los empleados de la cámara de Comercio.

A todos los usuarios empleados, contratistas y terceras personas se les proporcionará un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad de la información y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de mitigar los posibles riesgos de seguridad.

Se deberá establecer un proceso disciplinario normal para gestionar las brechas en seguridad.

Se debe realizar una revisión anual por RRHH de los contratos junto con los empleados para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información.

Cese o cambio de puesto de trabajo. La dirección administrativa debe asegurar que todos los funcionarios, contratistas, terceras partes, que no laboren más en la empresa o cambien de puesto de trabajo, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será vigente hasta que la institución lo considere conveniente, incluso después de la finalización del puesto de trabajo o del contrato; también que se devuelve todo el equipamiento y se eliminan completamente todos los derechos de acceso.

Se debe realizar devolución de los activos de la organización por parte de los empleados responsables, para esto se debe verificar el inventario de activos regularmente.

Examinar qué accesos necesita revocar apremiantemente y priorizadamente.

Realizar un seguimiento del uso del e-mail de estas personas antes de salir definitivamente de la empresa, para evitar fuga confidencial (sujeto a las políticas aplicables y a consideraciones legales sobre privacidad).

Acuerdo de confidencialidad. Para el uso de los recursos tecnológicos las Cámaras de Comercio, todo usuario debe firmar un acuerdo de confidencialidad (Apéndice G) 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 de las soluciones de autenticación biométrica en línea con su respectivo kit de hardware.

Cada dependencia debe operar bajo término de perfiles que asocien a los usuarios con sus respectivas funciones y tareas, estos deben predefinirse y actualizarse por cada estamento organizativo; cada usuario debe cumplir con unos parámetros de buenas prácticas de seguridad de la información, descritos a continuación los usuarios deben portar dentro de las instalaciones de la institución un carné que los identifique como funcionarios y/o contratistas.

- Cada usuario que se denomine como personal interno será responsable por el mal uso del equipo de cómputo en el cual realiza sus tareas, incluyendo infecciones de virus.

- Los usuarios no deben bajo ninguna circunstancias descargar de internet archivos, que pudiera ser considerado pornográfico, difamatoria, racista, videos, música, entre otros. o que atente contra las buenas costumbres o principios, excepto que sus funciones administrativas así lo amerite.
- Los usuarios no deben utilizar los dispositivos electrónicos propios de la institución para su uso personal, es por ello que no deberán acceder desde estos a redes sociales ni correos electrónicos personales.

- Todos los usuarios deben realizar el envío de información únicamente a través del correo institucional.

- Se plantea que los usuarios que se adscriben como personal interno deben utilizar cuentas de usuario para acceso al sistema de los computadores a su cargo.

- Los usuarios no deben utilizar memorias USB para el tránsito de información en los equipos de cómputo propios de la entidad.

Responsabilidades de usuarios externos. Se entiende por usuario externo a las personas que hagan parte de organizaciones externas que tengan convenios o relaciones con la Cámara de Comercio de Aguachica. Todos los usuarios denominados como externos o terceros y personal de empresas externas, deben estar autorizados por un miembro del personal de la organización, quien será responsable del control y vigilancia del uso adecuado de la información y los recursos tecnológicos institucionales, del uso que estos tengan; ellos deben acatar los siguientes reglamentos.

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.

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.

Gestión de activos.

Responsabilidad sobre los activos.

- Mantener la protección adecuada de los activos de la organización.

- Todos los activos se deben incluir en el inventario y deben tener un propietario designado.

- Se deben identificar los propietarios para todos los activos y asignar la responsabilidad para el mantenimiento de los controles. La implementación de los controles específicos puede ser delegada por el propietario según el caso, pero él sigue siendo responsable de la protección adecuada de los activos.

- Los recursos informáticos de la Cámara de Comercio, dispuestos para la operación registral, solo deben ser usados para fines laborales, entre los cuales, se resalta la prestación del servicio de autenticación biométrica en línea a los usuarios de la Cámara de Comercio usuaria de este servicio. 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.

- El uso del computador personal y demás recursos informáticos por parte del empleado, trabajadores o usuarios del sistema de autenticación biométrica en línea, debe someterse a todas las instrucciones técnicas, que imparta el comité de seguridad.

Clasificación de la Información

- La información se debe clasificar para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información.

- La información tiene diferentes grados de sensibilidad e importancia. Algunos elementos pueden requerir un grado adicional de protección o manejo especial. Se debe utilizar un esquema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales de manejo.

- Toda la información generada por la Organización debe estar disponible para funcionarios tanto externos como internos que requieran del acceso y consulta de ésta, siempre y cuando se manejen los controles de acceso y confidencialidad apropiados.
- Se deben asignar responsabilidades en cuanto a la propiedad de los activos de información a usuarios encargados de mantener la integridad de la información. Es responsabilidad del administrador de la información asignar los respectivos controles de

acceso a la información.

- 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.

- 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.

Manejo de los soportes de almacenamiento.

- Está terminantemente prohibido compartir los discos duros o las carpetas de los computadores de escritorio, aunque estén protegidos por contraseña. Cuando exista la necesidad de compartir recursos esto se debe hacer con autorización previa y restringir por Dominio.

- Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Cifre todos los datos sensibles o valiosos antes de ser transportados.

Control de accesos.

Política de control de acceso. 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.

El acceso de los usuarios a los sistemas de información y acceso al sistema debe estar controlado y gestionado por perfiles de usuarios y contraseñas de accesos a dichos sistemas, El acceso a información restringida debe estar controlado. Se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas digitales. Por consiguiente se deben tener en cuenta los siguientes parámetros.

- Cada usuario es responsables de los mecanismos de control de acceso que les sean proporcionado; esto es, su nombre de usuario y contraseña necesarios para acceder al sistema, grupo de trabajo y/o dominio de red, por lo que se deberá mantener de forma confidencial.

Política de 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.

- 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.

- 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.

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

- Bajo ninguna circunstancia los usuarios deberán guardar sus contraseñas, en ningún tipo de papel, agenda, entre otros.
- Una contraseña para ser considerada segura debe poseer las siguientes características: Longitud, Las contraseñas deben tener como mínimo 8 caracteres de extensión, aleatoriedad: Una contraseña debe ser difícil de descifrar. Se deben utilizar combinaciones de palabras y números, fechas entre otros., Complejidad: se deben utilizar una mezcla de números y letras, signos de puntuación, caracteres especiales, mayúsculas y minúsculas en sus contraseñas; Exclusividad: se debe utilizar una contraseña por cada uno de las cuentas de usuario y correos electrónicos que utilice; Actualización: Las contraseñas deben ser cambiadas cada 2 o 3 meses, Gestión: los usuarios no deben dar a conocer sus contraseñas, ni plasmarlas en ningún documento o apuntador ya sea físico o

digital, ni pegarlas en los monitores, debajo de los teclados, tampoco en un fichero de texto que lleve el nombre contraseñas.

- No se debe revela la contraseña en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo.

- No se debe compartir la contraseña con familiares y/o amigos.

- No se debe utilizar la característica de "Recordar o guardar Contraseña".

- Se recomienda no incluir en las contraseñas datos personales, tampoco nombre de familiares, ni de mascotas.

- Se debe evitar compartir la contraseña en respuesta a un ejemplo de petición por correo electrónico o por teléfono, para verificar su identidad, incluso si parece ser de una compañía o persona de confianza.

Cifrado. Proteger la confidencialidad, autenticidad o integridad de la información que se envía y se recibe, aplicando controles criptográficos.

Se recomienda utilizar un sistema de cifrado en pre-boot, que pida una contraseña de acceso y descifrado del disco duro. De esta manera, en caso de pérdida o Hurto, no servirá para nada extraer el disco duro y montarlo desde otra plataforma puesto que el mismo estará cifrado

completamente. En Microsoft Windows se encuentra la herramienta Bitlocker. Así mismo puede utilizarse Truecrypt como alternativa, aunque es recomendable Bitlocker por estar soportada por Microsoft de forma corporativa. En caso que no se desee hacer un cifrado completo del disco, al menos será altamente recomendable que la información tratada en local se guarde en un contenedor cifrado. Para este fin, se recomienda la utilización de soluciones como Truecrypt, compatible con sistemas operativos Windows, Mac y Linux.

- 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.

- Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados.

Seguridad física y ambiental.

Áreas Seguras. Evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la organización.

Los servicios de procesamiento de información sensible o crítica deben estar ubicados en áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad y

controles de entrada adecuados, Dichas áreas deberían estar protegidas físicamente contra acceso no autorizado, daño e interferencia.

La protección suministrada debe estar acorde con los riesgos identificados.

Seguridad de los Equipos. Evitar pérdida, daño, robo o puesta en peligro de los activos, y la interrupción de las actividades de la organización.

Los equipos deberían estar protegidos contra amenazas físicas y ambientales.

La protección del equipo (incluyendo el utilizado por fuera) es necesaria para reducir el riesgo de acceso no autorizado a la información y para proteger contra pérdida o daño. También se debería considerar la ubicación y la eliminación de los equipos. Es posible que se requieran controles especiales para la protección contra amenazas físicas y para salvaguardar los servicios de soporte tales como energía eléctrica e infraestructura de cableado.

Los equipos que hacen parte de la infraestructura tecnológica de la Cámara de comercio Aguachica, tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, Hurto o acceso no autorizado a los mismos. De igual manera, se deben adoptar los controles necesarios para mantener los equipos

alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los equipos servidores, dispositivos activos de red que contengan información y servicios de carácter institucional, deben ser mantenidos en un ambiente seguro y protegido por los menos con:

- Controles de acceso y seguridad física.

- Detección de incendio y sistemas de extinción de conflagraciones.

- Controles de humedad y temperatura.
- Bajo riesgo de inundación.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).Los computadores deben bloquearse después de diez (10) minutos de inactividad, el usuario tendrá que autenticarse antes de reanudar su sesión. Todos los usuarios deben bloquear la sesión al retirarse de los dispositivos.
- No se deben introducir dispositivos extraíbles como memorias USB, cámaras, entre otros. ya que pueden ser portadores de software malicioso y además se pueden utilizar para copiar información sensible de la Cámara de Comercio de Aguachica, Cesar.
- En caso de daño o mantenimiento se debe tener cuidado con el proceso desinstalación y retirada del equipo, de tal manera que estos se hagan de forma controlada y segura. Garantizar la protección de los equipos, incluso cuando se utilizan fuera de la oficina, es

necesaria para reducir el riesgo no autorizado de acceso a la información y para protegerlo contra pérdida o Hurto.

Los equipos de cómputo deben estar correctamente protegidos y controlados por personal de la institución el cual debe tener conocimiento acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información de la institución.

Sistema de vigilancia con cámaras de seguridad: éste sistema deberá desarrollarse por las personas naturales o jurídicas, tendientes a prevenir o detener perturbaciones a la seguridad y tranquilidad en lo relacionado con la vida y los bienes propios o de terceros y la fabricación, comercialización, instalación y utilización de equipos para la vigilancia y seguridad privada, blindajes y transporte con este mismo fin.

- Se deben establecer las zonas bajo videovigilancia en donde estarán instaladas las cámaras, éstas se ubicaran dentro y fuera del edificio es decir en la entrada principal, pasillos, biblioteca, aulas de clase, áreas de acceso restringido,

- El sistema de video vigilancia se empleara únicamente a efectos de protección y seguridad. El sistema contribuye a garantizar la seguridad tanto de los edificios de la organización, su personal y visitantes como de los bienes contenidos en sus instalaciones y la información allí almacenada.

- En caso de necesidad, se recomienda contemplar y complementar con otros sistemas de seguridad físicos, por ejemplo sistemas de control de acceso y sistemas de detección de intrusiones.

- El sistema no deberá ser usado para ningún otro fin distinto, como por ejemplo vigilar el trabajo de los funcionarios u otros miembros del personal. El sistema se utilizará como herramienta de investigación o como prueba en investigaciones internas o procedimientos disciplinarios cuyo propósito exclusivo sea investigar un incidente de seguridad física.

Seguridad en la operativa. Protección contra software malicioso y *hacking**:** todos los sistemas informáticos utilizados en la entidad deben ser protegidos teniendo en cuenta las diferentes áreas que involucre controles humanos, físicos técnicos y administrativos; se deben implementar medidas que mitiguen los riesgos asociados a amenazas de software malicioso y técnicas de hacking.

La Cámara de comercio de Aguachica, establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad de la Dirección administrativa autorizar el uso de las herramientas y asegurar

que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente. Sobre el particular se establece los siguientes lineamientos:

- No se permite la desinstalación y/o desactivación de software y herramientas de seguridad.
- No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- No se permite utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo o avalado por la administración de la institución.
- En caso de presentarse fallas en la transmisión por medio de la red de datos de la institución, se debe informar a la persona encargada de administrar la red, y este deberá aplicar las medidas correctivas para descartar posibles intrusiones realizando seguimiento al tráfico de la red, y en caso de detectarse se deberá tomar medidas en el caso.

Recursos compartidos. Está terminantemente prohibido compartir los discos duros o las carpetas de los computadores de escritorio, aunque estén protegidos por contraseña. Cuando exista la necesidad de compartir recursos esto se debe hacer con autorización previa y restringir por Dominio.

- Todo monitoreo debe ser registrado e informado al jefe inmediato del usuario.
- Un usuario puede ser monitoreado bajo previa autorización del comité de seguridad.

- 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 cifrado y otros mecanismos de control de acceso que le puedan permitir obtener ingreso a sistemas no autorizados.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- Cuando un funcionario de La Cámara de Comercio inicie su relación laboral se debe diligenciar el documento de entrega de inventario.
- Configuración de sistema operativo de las estaciones de trabajo.
- Solamente los funcionarios del área técnica de sistemas están autorizados para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.
- 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.
- 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.
- 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 necesaria para la labor desempeñada.
- Ambientes separados de producción y desarrollo.

Todo sistema o aplicativo debe contar con ambiente de desarrollo y ambiente de producción. Así mismo para la realización de pruebas no se deben utilizar datos de producción.

Cumplimiento del procedimiento para cambios y/o actualizaciones.

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, serán evaluados en ambientes de prueba cuya función es determinar el correcto funcionamiento y compatibilidad con las herramientas base. Una vez determinado el correcto funcionamiento y compatibilidad con las herramientas base se debe crear un plan de trabajo para la migración del ambiente de producción a la nueva versión.

Documentación de cambios y/o actualizaciones.

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, debe tener la documentación respectiva.

Catalogación de programas.

Debe cumplirse con el procedimiento establecido para pasar programas del ambiente de desarrollo al ambiente de producción previa

Prueba por parte del área encargada.

- Medidas de seguridad deben ser implantadas y probadas antes de entrar en operación.
- Todos los controles de seguridad para los sistemas de información deben ser implantados y probados sobre ambientes de pruebas o desarrollo y antes que dicho sistema entre en operación.
- Dependencia de la autenticación de usuario en el sistema operativo.

Los desarrolladores de aplicaciones no deberán crear su propio sistema de control de acceso a la aplicación en desarrollo, esta labor deberá recaer en el sistema operativo o en un sistema de control de acceso que mejora las capacidades del sistema operativo. Esta política debe empezar a cumplirse desde la liberación de este documento.

Incorporación de contraseñas en el software. Ninguna contraseña deberá ser incorporada en el código de un software desarrollado o modificado por La Cámara de Comercio o sus proveedores, para permitir que las contraseñas sean cambiadas con la regularidad establecida en la política “Cambios periódicos de contraseñas”.

Acceso del usuario a los comandos del sistema operativo. Después de haber iniciado una sesión, el usuario debe mantenerse en menús que muestren solo las opciones habilitadas para dicho usuario y de esta manera impedir la ejecución de comandos del sistema operativo y la divulgación de las capacidades del sistema.

Se requieren registros de auditoria en sistemas que manejan información sensible.

Todo sistema que maneje información sensible para La Cámara de Comercio debe generar registros de auditoria que guarden toda modificación, adición y eliminación de dicha información.

Registros para los usuarios privilegiados en los sistemas en producción que lo permitan. Toda actividad realizada en los sistemas por usuarios con privilegios de administración debe ser registrada, si los mismos lo permiten, o de lo contrario debe existir un procedimiento alterno de control.

Los registros del sistema deben incluir eventos relevantes para la seguridad. Los sistemas de computación que manejan información sensible deben registrar todos los eventos de seguridad relevantes. Ejemplos de eventos de seguridad relevantes son: intentos de adivinación de contraseñas, intentos de uso de privilegios no otorgados, modificaciones a la aplicación y modificaciones al sistema.

Resistencia de los registros contra desactivación, modificación y eliminación. Los mecanismos para detectar y registrar eventos de seguridad informática significativos deben ser resistentes a ataques, en los sistemas que permitan dicha configuración. Estos ataques incluyen intentos por desactivar, modificar o eliminar el software de registro y/o los registros mismos.

Procesos controlados para la modificación de información del negocio en producción. La modificación de información en producción debe darse únicamente mediante procesos con privilegios dentro de la aplicación que maneja dicha información. Esto con el fin de evitar que la información pueda ser modificada por medios diferentes a los canales establecidos. Se excluyen los casos de emergencia, previa autorización de la Presidencia.

Validación de entradas en los desarrollos. El desarrollador debe tener en cuenta durante la elaboración de la aplicación, la validación de las entradas de código con el objeto de evitar la ejecución de comandos que pongan en riesgo la seguridad de los sistemas.

Diseño de seguridad para aplicaciones. El esquema de seguridad de aplicación, debe elaborarse de acuerdo con las definiciones establecidas para La Cámara de Comercio.

Personas autorizadas para leer los registros de auditoria. Los registros de sistemas y aplicaciones no deben estar disponibles para personal no autorizado. Personal no autorizado es aquel que no pertenece a auditoria interna, personal de seguridad informática, personal de administración de sistemas o administradores de bases de datos.

Archivo histórico de contraseñas. En todo sistema multiusuario, software del sistema o software desarrollado localmente se debe mantener un archivo histórico encriptado de las contraseñas anteriores. Este archivo deberá ser usado para prevenir que un usuario seleccione una contraseña ya usada (ver política "Las contraseñas creadas por usuarios no deben ser reutilizadas") y debe contener como mínimo las últimas cinco (5) contraseñas de cada usuario.

Políticas para administradores de sistemas

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.

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.

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.

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.

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".

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.

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.

Brindar acceso a personal externo. El ingeniero de soporte y 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.

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 Presidencia. Es obligatoria la firma del acuerdo de confidencialidad.

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

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.

Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito. Sin autorización escrita Dirección de TI de la Cámara de comercio, los administradores no deben otorgarle privilegios de administración a ningún usuario.

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

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 cifrado del software como tal.

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.

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 seguridad y todos los archivos potencialmente involucrados.

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.

Revisión regular de los registros del sistema. El área de sistemas debe revisar regularmente los registros de cada uno de los diferentes sistemas para tomar acción oportuna sobre los eventos relevantes de seguridad informática.

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.

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.

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.

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. A nivel Corporativo se cuenta con un firewall que proporciona un software de IDS (Instrusion Detection System), detección de virus y bloqueo de correo no deseado.

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.

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.

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

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

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

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

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

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.

Tipo de datos a los que se les debe hacer backup 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.

Seguridad en las telecomunicaciones. 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.

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.

Gestión de la seguridad en las redes. La configuración de los dispositivos activos de red, debe estar siempre documentada, se deberá tener copia de respaldo de las configuraciones. Todos los equipos de tecnología deben estar registrados y aplicarles permanentemente mantenimientos preventivos.

Para el fin pertinente se deben cumplir las siguientes premisas:

- Impedir el acceso del personal no autorizado a los servicios en red.
- Se deberán controlar los accesos a servicios internos y externos conectados en red.
- Se deberán emplear mecanismos de autenticación adecuados que se apliquen a los usuarios y equipos. Los métodos de autenticación que pueden tener son: implementación de redes locales virtuales, filtrado de direcciones IP a nivel de Host o Subredes.
- El encargado de administrar la red deberá llevar estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (p. ej., intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes/preocupantes/críticos).
- Se deberá realizar segmentación de dominios de broadcast, para separar cada instancia de la Cámara de Comercio de Aguachica, Cesar, fraccionando un segmento para

funcionarios, docentes, estudiantes, invitados; esto deberá aplicar para la red cableada e inalámbrica y un segmento para Smartphone.

- Se deben tener grupos de trabajo o dominios de red para los usuarios de orden administrativo.
- Hacer o intentar hacer cualquier cosa que afecte negativamente la habilidad de utilizar el servicio de internet por otros usuarios, incluyendo sin limitación alguna, "negación de servicios", ataques contra otros sistemas.
- Acceder al sistema o red, monitorear datos o tráfico.
- Sondear, copiar, probar firewalls o herramientas de hacking.
- Atentar contra la vulnerabilidad del sistema o redes.
- Violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red.

    - Navegación en internet: el uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades de la institución educativa y debe ser utilizado por los usuarios para realizar las funciones establecidas para su rol, por lo cual se definen los siguientes parámetros para su uso:

- Abstenerse de acceder a sitios web que salten la seguridad del servidor de acceso a Internet (proxy) o intentar hacerlo.
- No se deberá descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o medios

magnéticos.

- Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma actos ilegales, inmorales, engañosos y/o fraudulentos es una responsabilidad de los colaboradores de la organización; así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, actos obscenos, pornográficos, profanos, racistas, discriminatorios, actos que invadan la privacidad de los demás u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo.
- No se permitirá el acceso y el uso de mensajería instantánea como Facebook, Yahoo, Skype, twitter y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades de la organización.
- No se podrá realizar La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Jefe respectivo y personal encargado de los recursos tecnológicos, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

- Todos los usuarios de la Cámara de Comercio de Aguachica, deben ser responsables de dar uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.
    - Correo electrónico: todos los usuarios a los que se les sea asignada una cuenta de correo electrónico de carácter institucional deberán responsabilizarse de su uso, de todos los mensajes y archivos transmitidos y recibidos; así mismo esta debe ser usada solo para envío y recepción de información de índole corporativa, no se permitirá el uso y acceso de correo electrónicos de otro tipo dentro del ámbito institucional. Los usuarios deberán tener en cuenta lo siguiente:

- Los mensajes y la información contenida en los buzones del correo electrónico son propiedad de la Cámara de comercio de Aguachica, y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- No se permitirá enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

- No se permite la utilización de la dirección de correo electrónico de la Cámara de comercio de Aguachica, como punto de contacto en comunidades interactivas, redes sociales, tales como Facebook, twitter, entre otras, o cualquier otro sitio que no tenga que ver con las actividades institucionales.
- No se deberá realizar envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- No se deben enviar archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser exclusivamente de contenido didáctico y/o educativo.
- Los usuarios de la Cámara de comercio de Aguachica, deben evitar la utilización de la cuenta de correo electrónico institucional para el envío o reenvío de mensajes spam (no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades), hoax (es un intento de hacer creer que algo falso es real), con contenido que pueda resultar ofensivo o dañino para otros usuarios o que sea contrario a las políticas y normas institucionales.
- La contraseña de acceso al correo electrónico, debe ser cambiada periódicamente por cada usuario.
- Los usuarios no deberán abrir enlaces sospechosos llegados por correos electrónicos por ejemplo de bancos, tiendas, entre otros. ya que pueden ser víctimas de phishing.
- No completar datos personales en mensaje de correos electrónicos sospechosos.
- Eliminar periódicamente los correos no deseados (spam o sospechoso).
- 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”.

- 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.
- 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.
- 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 usuario.
- 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.
- Mensajes prohibidos. Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros ó 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.
- 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.
- 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.

- 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.
- 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.

Recursos tecnológicos: la instalación o desinstalación de cualquier elemento software o hardware en los equipos de cómputo de la organización, es responsabilidad del funcionario encargado del manejo de los elementos tecnológicos, y por tanto será el único autorizado para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por la institución a través de la Dirección.

- Los usuarios no deberán realizar modificaciones en los dispositivos de cómputo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales del dispositivo, fondo de escritorio y protector de pantalla institucional, entre otros. Estos cambios pueden ser realizados únicamente por el funcionario encargado de los recursos de Tecnología.

- Sólo usuarios autorizados pueden realizar actividades de administración remota de dispositivos de red, equipos de cómputo o servidores de la infraestructura de procesamiento de información de la Cámara de comercio de Aguachica; las conexiones

establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración que garanticen los principios básicos de seguridad de la información.

- No se permitirá la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. Deben haber constantes revisiones para verificar lo anterior expuesto y en caso de detectarse un evento de este tipo se deberá proceder a desinstalar el material encontrado y tomar las medidas correctivas correspondientes.

Políticas de uso de firewall.

Detección de intrusos. Todo segmento de red accesible desde Internet debe tener un sistema de detección de intrusos (IDS) con el fin de tomar acción oportuna frente a ataques.

Toda conexión externa debe estar protegida por el firewall. Toda conexión a los servidores de La Cámara de Comercio proveniente del exterior, sea Internet, acceso telefónico o redes externas debe pasar primero por el Firewall. Esto con el fin de limitar y controlar las puertas de entrada a la organización.

Toda conexión hacia Internet debe pasar por el Firewall. El firewall debe ser el único elemento conectado directamente a Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por el firewall.

Filtrado de contenido activo en el Proxy. La dirección de TI de las Cámaras de Comercio, debe asegurar que dentro de las definiciones de políticas de Proxy, se filtre todo contenido activo como applets de java, adobe flash player, controles de ActiveX debido a que estos tipos de datos pueden comprometer la seguridad de los sistemas de información de La Cámara de Comercio

Firewall debe correr sobre un computador dedicado o appliance. Todo firewall debe correr sobre un computador dedicado o modelo appliance para estos fines. Por razones de desempeño y seguridad no debe correr otro tipo de aplicaciones.

Inventario de conexiones. Se debe mantener un registro de las conexiones a redes externas con el fin de tener una imagen clara de todos los puntos de entrada a la organización, lo anterior se cumple con el diagrama de red.

El sistema interno de direccionamiento de red no debe ser público. Las direcciones internas de red y configuraciones internas deben estar restringidas de tal forma que sistemas y usuarios que no pertenezcan a la red interna no puedan acceder a esta información.

Revisión periódica y reautorización de privilegios de usuarios. Los privilegios otorgados a un usuario deben ser reevaluados una vez al año con el fin de analizar sí los privilegios actuales siguen siendo necesarios para las labores normales del usuario, o si se necesita otorgarle privilegios adicionales. Esta política debe ser ejecutada por el área de sistemas

con la participación de cada uno de los jefes de área, quienes harán la revisión y solicitud de cambios a la Presidencia.

Datos sensibles enviados a través de redes externas deben estar encriptados. Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados.

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.

Reglas de uso de la Intranet. La Cámara de Comercio utiliza la intranet como un recurso de publicación de los documentos que rigen la relación entre ésta y el empleado o trabajador. Por lo tanto, el empleado debe consultar la intranet permanentemente, así como todos los documentos que en ella se encuentran publicados.

Prohibición de publicitar la imagen de La Cámara de Comercio en sitios diferentes a los institucionales. La publicación de logos, marcas o cualquier tipo de información sobre La Cámara de Comercio o sus actividades en Internet solo podrá ser realizada a través de las páginas institucionales de la misma y previa autorización de la Presidencia. En consecuencia, se encuentra terminantemente prohibido el manejo de esta información en páginas personales de los empleados.

Prohibición establecer conexiones a los sitios Web de La Cámara de Comercio. Está prohibido igualmente establecer enlaces o cualquier otro tipo de conexión a cualquiera de los sitios Web de La Cámara de Comercio por parte de los empleados y de sus sitios Web o páginas particulares, salvo previa autorización de la Presidencia, dependiendo del caso. Particularmente se encuentra prohibido el establecimiento de links o marcos electrónicos, y la utilización de nombres comerciales o marcas de propiedad de la Entidad en sitios diferentes a los institucionales o como meta-etiquetas.

Prohibición de anuncios en sitios Web particulares. Está terminantemente prohibido anunciarse en los sitios Web particulares como empleados de La Cámara de Comercio o como sus representantes, o incluir dibujos o crear diseños en los mismos que lleven al visitante del sitio Web a pensar que existe algún vínculo con La Cámara de Comercio

Adquisición, desarrollo y mantenimiento de los sistemas de información.

MAdquisición, Desarrollo y Mantenimiento de Sistemas Software.

- Garantizar que la seguridad sea una parte integral de los sistemas de información.
- Se debe realizar un estudio de necesidades para así preparar el plan de desarrollo tecnológico.
- Se debe asegurar de que los programas desarrollados o adquiridos provean medidas de control o, de interoperabilidad con otros sistemas. Con este fin, el personal encargado del desarrollo o adquisición de programas o de otros componentes de programación debe tomar en cuenta que: Sean compatibles

con el equipo existente o cumplan con las especificaciones mínimas del proponente de la programación, Provean crecimiento, flexibilidad y adaptabilidad, sean funcionales en arquitectura; Existan maneras de controlar la creación y privilegios de los usuarios.

- El software de aplicaciones y software de base sólo debe ser puesto en producción después de ser probado; se deben incluir pruebas sobre la funcionalidad, la seguridad, los efectos sobre otros sistemas y las facilidades de usuario, y deben ser realizadas en ambiente de pruebas.

Control de cambios. Ver Apéndice H

Relaciones con suministradores.

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 Presidencia. Es obligatoria la firma del acuerdo de confidencialidad.

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.

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.

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. 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.

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.

Gestión de incidentes en la seguridad de la información

Comité de Seguridad de la información. El comité está conformado por un equipo de trabajo interdisciplinario encargado de garantizar una dirección clara y brindar apoyo visible a la Presidencia 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 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.

Cambio en los roles del ciclo de certificación.

- Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la presente política de La Cámara de Comercio El Presidente 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 su 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.

    - Oficial de Seguridad de la Información

Oficial de Seguridad de la Información (Jefe de Riesgos o persona designada para los temas de seguridad de la Entidad):

- Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información a los funcionarios de la compañía.

- Actualización y seguimiento periódico al mapa de riesgos de la compañía, validando con cada proyecto que se implemente como afecta el mapa de riesgos y tomando siempre como base este mapa para cualquier proyecto nuevo que se implemente.

- Dirigir el programa de manejo y seguimiento de incidentes.

- Crear y establecer una metodología de clasificación de la información según su importancia e impacto dentro de la compañía. Igualmente debe informarla a la compañía y validar que se cumpla. La metodología debe establecer niveles de acceso a la información.
- Crear y mantener un Programa de Concientización en seguridad de la información.

- Evaluar en forma continua la efectividad de la seguridad de la información de la organización con el propósito de identificar oportunidades de mejoramiento y necesidades de capacitación.

Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

Continuidad del negocio: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y asegurar su recuperación oportuna.

- Procedimientos de contingencia. Los cuales describen las acciones a tomar cuando ocurre un incidente que interrumpe las operaciones del negocio, proporcionando mecanismos alternos y temporales para continuar con el procesamiento.

- Procedimientos de retorno. Los cuales describen las acciones a seguir para regresar las operaciones normales a las instalaciones originales.

- Procedimientos de recuperación. Los cuales describen las acciones a seguir para trasladar las actividades del negocio a un centro alterno de recuperación.

- Actualización periódica. El plan debe actualizarse cuando cambios realizados en el ambiente operativo impacten su funcionalidad. Un análisis de impacto al negocio debe ser realizado como mínimo una vez al año, con el objeto de determinar la necesidad de la disponibilidad de la información en el grado y escala de tiempo requeridos después de una interrupción de las funciones críticas de la Organización.

- El Plan de Continuidad debe estar alineado con los riesgos identificados que puedan causar interrupción al servicio. Para este caso, se debe tener en cuenta las posibles consecuencias para la seguridad de la información.

Políticas generales de la presidencia

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"

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.

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.

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.

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.

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.

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.

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 va presentando.

Actualización, mantenimiento y divulgación de 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 deben 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.

Cumplimiento.

Auditoría y cumplimiento: todos los procesos de seguridad de la información y recursos tecnológicos, deben estar siempre sometidos a intervenciones de control y revisión los cuales arrojen datos que contribuyan a la toma de decisiones en cuanto a mejora o replanteamiento de parámetros previamente establecidos; todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos. La entidad no debe emprender procesos de desarrollo mantenimiento de sistemas software que tengan asociados riesgos altos no mitigados.

Todo uso y seguimiento a los recursos de TI en la Cámara de comercio de Aguachica, debe estar de acuerdo a las normas y estatutos internos así como a la legislación nacional en materia.

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 de La Cámara de Comercio y al comité de seguridad.

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.

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.

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 deben 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.

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 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 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.

Cambio en los roles del ciclo de certificación.

Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la presente política de La Cámara de Comercio El Presidente 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 su 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.

Oficial de Seguridad de la Información. Oficial de Seguridad de la Información (Jefe de Riesgos o persona designada para los temas de seguridad de la Entidad):

Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información a los funcionarios de la compañía.

Actualización y seguimiento periódico al mapa de riesgos de la compañía, validando con cada proyecto que se implemente como afecta el mapa de riesgos y tomando siempre como base este mapa para cualquier proyecto nuevo que se implemente.

Dirigir el programa de manejo y seguimiento de incidentes.

Crear y establecer una metodología de clasificación de la información según su importancia e impacto dentro de la compañía. Igualmente debe informarla a la compañía y validar que se cumpla. La metodología debe establecer niveles de acceso a la información.

Crear y mantener un Programa de Concientización en seguridad de la información.

Evaluar en forma continua la efectividad de la seguridad de la información de la organización con el propósito de identificar oportunidades de mejoramiento y necesidades de capacitación.

Oficio de entrega de Políticas de Seguridad de la Información, ver **Apéndice F**.

Capítulo 5. Conclusiones

Mediante la implementación de las técnicas e instrumentos de recolección de información, se concluyó y se evidencio la necesidad que existe en la Cámara de Comercio de Aguachica, de darle un tratamiento optimo a la información que se maneja en cada uno de los procesos llevados por los estamentos de la institución; mediante la implementación de normas que regulen, estandaricen y garanticen la confidencialidad, integridad y disponibilidad como principios fundamentales de la información como lo es ISO 27001.

Para el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) en la Cámara de Comercio de Aguachica, se adoptó la norma ISO 27001:2013 y a sí mismo el ciclo PHVA (Planear, Hacer, Verificar y actuar) que es la metodología de desarrollo e implementación del SGSI propuesto por la organización ISO, se desarrolló para la Cámara de Comercio de Seccional Aguachica el diseño de la Política de seguridad de la información, el diagnostico de análisis de riesgo de la entidad en donde se recurrió a la metodología MAGERIT desarrollada por el Ministerio de Hacienda y Administraciones públicas de España; la cual enmarca técnicas para el gestión del riesgo.

Se determinó que la información manejada en las dependencias de la Cámara de Comercio de Aguachica se encuentra expuesta a diferentes tipos de amenazas y vulnerabilidades que aumentan la probabilidad de riesgo afectando directamente el activo vital de la organización, la información.

Se estableció que los riesgos a los cuales se encuentra expuesta la empresa, principalmente son por el desconocimiento de buenas prácticas de seguridad de la información, por parte del personal administrativo de la misma.

La infraestructura de la red de la Cámara de Comercio de Aguachica, está altamente expuesta a cualquier tipo de ataque comprometiendo la seguridad de los datos que viajan a través de este medio, debido a que la red en el diagnóstico realizado representa los niveles más altos de riesgo.

Capítulo 6. Recomendaciones

Se sugiere a la gerencia de la Cámara de Comercio de Aguachica, la gestión para la adecuación del departamento de Sistemas, estancia en el cual se logra centralizar todo el manejo de los recursos de TI, y también el manejo de la Política de seguridad de la información que adopte la entidad.

Se recomienda que la organización adopte medidas para el mejoramiento de la red, mediante la segmentación de la misma la cual brindara mayor seguridad a la información y administrando las configuraciones se contribuirá a la seguridad de la información.

Al momento de implementar el sistema de gestión de seguridad de la información en la Cámara de Comercio de Aguachica, se debe realizar una auditoria por personal externo de la institución antes de realizar el proceso de certificación que expide ISO 27001, en pro de mejorar lo lineamientos establecidos por el SGSI.

Periódicamente se debe realizar un seguimiento a los riesgos a los cuales se encuentran expuestos los activos de información, de manera preventiva, y para la constante mitigación del riesgo.

Capacitar constantemente a los funcionarios de la empresa sobre manejo de la información, buenas prácticas de tecnologías de la Información y Comunicación, para que estén a la vanguardia de los cambios tecnológicos que ocurren constantemente en el mundo.

Referencias

Ley 23 de 1982. (15 de Febrero de 2014). Recuperado el 12 de Abril de 2016, de Derecho de autor y propiedad intelectual ley.: http:// http://legislacion.vlex.com.co/vid/ley-derechos-autor-71608275

Ley 44 de 1993 . (03 de Marzo de 2014). Recuperado el 11 de Abril de 2016, de Derecho de autor: http:// http://www.derechodeautor.gov.co/documents

Ley 527 De 1999 . (14 de Junio de 2014). Recuperado el 11 de Abril de 2016, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

Ley 719 de 2001. (15 de Junio de 2014). Recuperado el 12 de Abril de 2016, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5533 - ftp://ftp.camara.gov.co/

LEY ESTATUTARIA 1266 DE 2008. (15 de Febrero de 2014). Obtenido de Habeas data.: http://www.sic.gov.co/drupal/sites/default/files/normatividad/Decreto_2952_2010.pdf

AMERICANOS, O. D. (07 de Abril de 2013). *TENDENCIAS EN LA SEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA Y EL CARIBE Y RESPUESTAS DE LOS GOBIERNOS*. Recuperado el 26 de Marzo de 2016, de http://www.oas.org/es/ssm/cyber/documents/oastrendmicrolac_spa.pdf

AMPARO, P. (s.f.). Recuperado el 29 de Marzo de 2016, de http://www.proyectoamparo.net/files/manual_seguridad/manual_sp.pdf

CASADIEGOS SANTANA, A. L. (28 de Julio de 2014). *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE CONTABILIDAD DE LA E.S.E. HOSPITAL LOCAL DE RIO DE ORO CESAR*. Recuperado el 14 de Abril de 2016, de U iversidad Fran cisco de Paula Santander:

http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/901

CHACÓN HURTADO ANDRES FELIPE, M. S. (21 de Junio de 2012). *INFORMACIÓN PARA COMPUTACIÓN EN NUBES PRIVADAS Y COMUNITARIAS.* Recuperado el 26 de Marzo de 2016, de Universidad ICESI: http://bibliotecadigital.icesi.edu.co/biblioteca_digital/bitstream/10906/68436/1/definicio

ESTADISTICA. (2013). *La encuesta.* Obtenido de http://www.estadistica.mat.uson.mx/Material/queesunaencuesta.pdf

FABIÁN DÍAZ ANDRÉS, C. G. (05 de Agosto de 2011). *IMPLEMENTACION DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA COMUNIDAD NUESTRA SEÑORA DE GRACIA, ALINEADO TECNOLOGICAMENTE CON LA MNORMA ISO 27001.* Recuperado el 26 de Marzo de 2016, de NUESTRA SEÑORA DE GRACIA : http://www.konradlorenz.ed

HERNANDEZ SAMPIERI, R. -F.–B. (2010). *"Metodología de la investigación"* . Quinta edición Editorial Mac Graw Hills/Interamericana Editores Copyright.

ICONTEC, I. 2. (10 de Junio de 2014). *Certificación del Sistema de Gestión de Seguridad de la Información* . Recuperado el 12 de Abril de 2016, de http://www.icontec.org/index.php/es/sectores/agricultura-y-alimentos/50-colombia/certificacion-s

ISO. (s.f.). *27001.* Recuperado el 29 de Marzo de 2016, de http://www.27000.org/iso-27001.htm

JORGE, R. A. (2006). *Libro Electrónico de Seguridad Informática y Criptografía.* SEXTA EDICIÓN VERSION 4.1.

Ley 1273 5 de enero de 2009. (s.f.). Recuperado el 29 de Marzo de 2016, de Protección de la información y de los datos : http://www.mintic.gov.co/portal/604/articles-

3705_documento.pdf

LEY ESTATUTARIA 1581 DE 2012. (s.f.). Recuperado el 29 de Marzo de 2016, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

MOSQUERA QUINTERO, G. C. (02 de Diciembre de 2015). *ELABORACIÓN DE POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL BASADOS EN EL ESTÁNDAR INTERNACIONAL ISO/IEC 27002:2013 EN EL HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE ESE. DE LA CIUDAD DE AGUACHICA-CESAR.* Recuperado el 14 de Abril de 2016, de Universidad Francisco de Paula Santander: http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/901

NATALIA, J. M. (s.f.). *Temario especifico y test Técnicos de administración del ministerio de económia y hacienda* . Editorial MAD Copyright- .

PAVLOVIC, D. (s.f.). *Teoría de la seguridad por oscuridad Gaming* . Recuperado el 29 de Marzo de 2016, de Cornell University Library: http://arxiv.org/abs/1109.5542v1

PERSONALES, P. D. (s.f.). Recuperado el 12 de ABRIL de 2016, de http://www.sic.gov.co/drupal/sites/default/files/normatividad/Titulo%20V%20Proteccion_Datos_Personales.pdf

RAMOS, A. (s.f.). *El eslabón más débil de la cadena-–.* Recuperado el 29 de Marzo de 2016, de ISACA madrid : http://www.antonio-ramos.es/2007/06/el-eslabn-ms-dbil-de-la-cadena.html

SEGURIDAD, G. D. (s.f.). *INFORMACIÓN EN CONTEXTOS DE MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS DE LA REGIÓN.* Recuperado el 25 de Marzo de 2016, de http://repositorio.utp.edu.co/dspace/bitstream/11059/2514/1/0058A973.pdf

TOMAS, A. (15 de Junio de 2014). *Shannon, padre de la Teoría de la Información-* . Recuperado

el 10 de Abril de 2016, de ttp://bituchile.com/2011/05/teoria-de-la-informacion-concepto-bit-de-la-semana/

Apéndices

Apéndice A. Carta de inicio de auditoria

Aguachica – Cesar, 01 de junio de 2016

Doctor
Eduardo Solano Forero
Director Ejecutivo
Cámara de Comercio de Aguachica
Aguachica

Asunto: Notificación de Auditoria de Sistemas a la Cámara de Comercio, basados en la norma ISO 27001:2013

Cordial saludo,

Por medio del presente escrito nos permitimos notificarle a usted de manera formal de la realización de la auditoria de sistemas a la Cámara de Comercio de Aguachica, el objetivo es evaluar el estado actual de la seguridad de la información en la misma.

La auditoría se realizará bajo el seguimiento de la Norma ISO/IEC 27001:2013; para la recolección de información se hará uso de los siguientes instrumentos: entrevistas, encuestas, observaciones, listas de chequeo y revisión Documental, para ello se solicita el acceso a información pertinente de los procesos de la Cámara de Comercio de Aguachica, de igual manera se informa que el tratamiento de dicha información se realizara bajo parámetros de confidencialidad.

El grupo de auditores está conformado por:

Auditor 1, María Alejandra Merchán Villalba - Ingeniera De Sistemas

Auditora 2, Erney Ramírez Camargo - Ingeniero De Sistemas

Auditora 3, Yaditza Suarez de la Cruz - Ingeniera de Sistemas

Auditora 4, Alexander Meneses Martínez – Administrador de Empresas

Cordialmente,

ERNEY RAMIREZ CAMARGO
INGENIERO DE SISTEMAS

MARIA ALEJANDRA MERCHAN VILLALBA
INGENIERA DE SISTEMAS

YADITZA SUAREZ DE LA CRUZ
INGENIERA DE SISTEMAS

ALEXANDER MENESES MARTINEZ
ADMINISTRADOR DE EMPRESAS

Anexos: dos (6 hojas)

Copia: Dra. Lud Pabón Chona, Directora Administrativa y Financiera Cámara de Comercio de Aguachica

María M.

Apéndices B. Entrevista dirigida a la Directora Administrativa y Financiera de la Cámara de Comercio de Aguachica.

Entrevista dirigida a la Directora Administrativa y Financiera de la Cámara de Comercio de Aguachica

Fecha: 03/06/2016	**Nomenclatura: E003**

Objetivo: Evaluar los Aspectos Organizativos de la Seguridad de la Información.
Criterio: Estándar ISO/IEC ISO 27001, objetivo de Control (6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION).

1. **¿Tienen definido quienes son los responsables de la seguridad de la información, que empleado y que cargo desempeña dentro de la Cámara de Comercio?**

   R: "El responsable de la seguridad es del área de sistemas, ella es la que tiene la responsabilidad de estar pendiente de toda la parte de la seguridad de la información."

2. **¿Qué otras personas hacen parte del grupo de los responsables de la seguridad de la información de la cámara de comercio de Aguachica, tienen definido un comité y además que función cumple cada uno, se encuentran repartidas las tareas que cada quien debe ejecutar y sus responsabilidades en cuando al manejo de información?**

   R: "Actualmente la cámara de comercio debido al programa cidfre que es con relación al sistema de fraude y seguridad de la información, se vio en la necesidad de crear este comité y de crear el manual de seguridad de la información. Este manual fue un modelo enviado por confecamaras a nivel de cámaras de comercio, fue como un criterio unificado que se realizó, y pues tenemos el modelo. Actualmente no se ha conformado como tal el comité, estamos en ese proceso y con la ayuda de la ingeniera María, estamos adelantando toda esta parte para tener mayor control sobre toda la parte de la seguridad de la información."

3. **¿Ustedes tienen un listado actualizado de los contactos con autoridades pertinentes al área de seguridad de la Información por Ejemplo: Policía Nacional, Fiscalía, Bomberos, autoridades de supervisión en materia de seguridad, etc.?**

   R: "Con respecto a contacto con las autoridades, existe en la cartelera un listado de las entidades que en cualquier caso de urgencia están disponibles como la policía, bomberos, la fiscalía etc. Para el caso de la seguridad de la información, cualquier inconveniente que

se presente están los contactos de los ingenieros de confecamaras que son los encargados directamente de esta parte, si llega a existir inconveniente o algún fraude o robo de información."

4. **¿Se encuentran en contacto con grupos o foros de interés en el área de seguridad de la información, cuáles son?**

   R: "Los contactos de los foros está encargada la funcionaria de sistemas, ella es la que organiza la parte de la asistencia técnica por la parte de sistemas; la ingeniera de sistemas es la encargada de los foros y tiene los contactos de los ingenieros de confecamaras igualmente con el soporte del programa docuwer que es el programa de digitalización de la entidad. Cualquier inconveniente que se presente ella está al tanto y cualquier falla de seguridad ella tiene los contactos y hace saber al encargado para el soporte correspondiente a esto."

5. **¿Qué políticas tienen asociadas para los empleados que en ocasiones trasladan los equipos de la empresa como portátil, celular, entre otros a instalaciones fuera de la empresa, teniendo en cuenta que estos dispositivos almacenan información de la entidad?**

   R: "Para el caso de las funcionarios que están ya autorizados para tener acceso a los equipos de la entidad, está el caso de la persona que hace la visita a los municipios, pues se deja la constancia en el oficio que se envía al municipio correspondiente que ella va a realizar, pues esa sería la única formalización de que ella está en visita y que tiene que llevarse los equipos; también está el caso de la persona que debe hacer capacitación en otros municipios, entonces queda el registro de que está realizando en otro municipio con los equipos de la entidad, pero un formato o acta en especial de que se llevan los equipos, no se ha implementado."

Firma del Auditor	Firma del Auditado
Nombre:	Nombre:
Cargo:	Cargo:

Entrevista dirigida a la Directora Administrativa y Financiera de la Cámara de Comercio de Aguachica

Fecha: 03/06/2016	**Nomenclatura: E004**

Objetivo: Evaluar la seguridad de la información relacionados con los recursos humanos.
Criterio: Estándar ISO/IEC ISO 27001, objetivo de control (7.SEGURIDAD LIGADA A LOS RECURSOS HUMANOS).

1. **¿En el proceso de selección de candidatos para un empleo, que mecanismos utiliza para la verificación de antecedentes?**

   R: "Normalmente en el caso de las vacantes existentes, siempre se hace por recomendaciones, hojas de vida recomendadas de que son personas que cumplen con el perfil, que tienen las capacidades idóneas tanto intelectuales como personales, pero como tal que se busquen antecedentes en algún medio, hasta el momento no."

2. **¿Al nuevo empleado como le dan entrega del manual de funciones, principios institucionales, restricciones de acceso a la información de acuerdo a su cargo y demás documentación necesaria para que el comprenda las leyes y su rol dentro de la Cámara de Comercio?**

   R: "actualmente no se entrega el manual de funciones como tal, en el caso de los cargos donde se debe hacer la respectiva entrega, el funcionario que va a salir le explica al nuevo funcionario sus funciones y todo lo que le corresponde realizar; tampoco se entrega principios ni objetivos de la entidad, existe un código de ética pues en el momento está en la secretaria general, pero como una publicación como tal a los funcionarios no se ha realizado. Dentro del acuerdo de confidencialidad eso se va a realizar con el nuevo manual de seguridad de la información que es lo que queremos llegar con la información que se está recolectando."

3. **¿El empleado que es contratado se le hace entrega oficial de las políticas de seguridad de la información y es consciente de la importancia que tienen para la organización el correcto cumplimiento de las mismas?**

   R: "Con respecto al manual de las políticas de seguridad no se ha entregado ni se ha realizado nada al respecto de este tema porque es algo nuevo que la cámara de comercio

está implementando y es mas a nivel de cámaras de comercio es un proceso que se está iniciando y que se está implementando en cada entidad, por consiguiente no era algo obligatorio ni tan esencial como en estos momentos. Así mismo la cámara de comercio tiene un modelo de programa de manual de políticas de seguridad de la entidad el cual se está adaptando a la entidad y actualizando para que quede acorde a nuestra realidad y después de que se realice y de que se socialice, se hará la respectiva entrega a los funcionarios."

4. **¿Comprendiendo la importancia de la disponibilidad, integridad y confidencialidad de la información que maneja la Cámara de Comercio, ustedes como empresa de qué manera capacitan o le dan a conocer a los empleados con el fin que tomen conciencia de la importancia de la seguridad de la información dentro de la institución en busca de optimizar sus funciones y reducir el riesgo relacionado con los recursos humanos?**

   R: "Generalmente cuando el asesor jurídico va a las capacitaciones, hace reunión de todo el personal de registros públicos y les explica el tema que se trató, referente a la seguridad de la información actualmente está el sistema de fracción autoregistrable que es el cifpre donde se trata de prevenir pues de que sean personas que no corresponden al registro que vengan de pronto a realizar trámites los cuales no están autorizados, entonces este sistema comprende la seguridad de la información del comerciante donde el funcionario tiene conocimiento. Este sistema se encarga de que realmente la persona que esté haciendo el trámite en el caso de matrícula se le deje un documento de constancia, la verificación del documento, se le hace la huella, se le toma la foto, verificando que realmente sea la persona autorizada y que sea la persona que esté haciendo el registro; cada funcionario tiene el conocimiento de la importancia de la seguridad de la información y pues se trata de tener un sistema confiable dentro de la entidad."

5. **¿Qué medidas disciplinarias toman con el empleado que infrinja algunas de las características de la seguridad de la información (disponibilidad, integridad y confidencialidad), están contempladas en las Políticas de Seguridad de la Información?**

   R: "Hasta el momento en la entidad no se ha presentado ningún fraude relacionado con que algún funcionario infrinja alguna característica de la seguridad de la información; dentro del manual que se está elaborando está contemplado las políticas y las sanciones que se aplicaran en el caso de que ocurra algún accidente, pero el manual está en estado de elaboración."

6. **¿Cuándo un empleado se retira de la empresa por cualquier motivo, ustedes qué medidas toman con respecto al acceso de la información de la empresa, por ejemplo: contraseñas de acceso a servidores, bases de datos, cuentas de correo electrónico y demás?**

   R: "En el caso de los correos, la persona encargada de sistemas cambia las claves de los correos o se elimina el correo que el funcionario estaba manejando. En cuanto a las demás contraseñas y de los sistemas de la entidad, se eliminan las cuentas o se cambian las contraseñas, pero algo formalizado no hay en el momento."

7. **¿Si cuentan con Políticas de Seguridad de la Información, ustedes contemplan esta fase de retiro de un empleado con el fin de que cuando firme al momento que ingreso a trabajar sea consiente que las cuentas de usuario no le pertenecen a si no a la Cámara de Comercio?**

   R: "Muchos de los aspectos que nos envuelven en este caso no están contemplados porque es un proceso nuevo que se está buscando un mejoramiento continuo dentro de la entidad, estas políticas se comenzó a implementar como obligatoriedad desde septiembre de 2015; estamos en un proceso donde tenemos un manual que se está terminando de elaborar para ser respectivamente aprobado y publicado a los funcionarios, entonces algunos aspectos de los cuales hemos dicho que no están es porque estamos en proceso de elaboración e implementación de este manual y de estas políticas de seguridad de la informacion."

Firma del Auditor Nombre: Cargo:	Firma del Auditado Nombre: Cargo:

Entrevista realizada a la Directora Administrativa y Financiera de la Cámara de Comercio de Aguachica

Fecha: 03/06/2016	**Nomenclatura: P002**

Objetivo: Identificar la estructura organizacional de la Cámara de Comercio de Aguachica y sus funciones.

Criterio: "ISO/IEC 27001"

1. **¿Describa brevemente cuales son las funciones principales de la Cámara de Comercio?**

   R: "En cumplimiento a la ley 1712 del 6 de marzo del 2014, la cámara de comercio en la disposición de la ciudadanía, toda la información pertinente a funciones, derechos, deberes y todo por parte de los comerciantes. Dentro de esta información esta las funciones que señala el artículo 86 del código de comercio y las demás normas legales reglamentarias.

   Una de las funciones más relevante es que sirve como órgano consultivo en el gobierno nacional y en consecuencia estudia los asuntos que este someta a consideración y rendir los informes que se soliciten sobre la industria, comercio y demás ramas relacionada con sus actividades, como llevar los registros públicos, dentro de estos registros públicos está el registro mercantil, el registro proponente, los radicales y los nuevos registros que se constituyeron como los juegos de azar, el reunión que es el registro de libranza y el registro de turismo, esos son los últimos registros recientemente.

   Además de esto cabe resaltar que la cámara de comercio entes privados sin ánimo de lucro pero que llevan una función pública designada por el estado como son llevar los registros públicos, que es toda la parte del registro de los comerciantes."

2. **¿De qué manera la Cámara de Comercio está cumpliendo con los objetivos organizacionales planeados?**

   R: "primero que todo la cámara de comercio tiene un plan estratégico donde está estructurado y enfocado para dar cumplimiento a sus objetivos, así mismo se elabora para las vigencias siguientes se elabora plan de trabajo donde se estipulan cada una de las actividades de las diferentes áreas las cuales nos llevan a cumplir cada uno de los objetivos de la entidad."

3. **¿La Cámara de Comercio de Aguachica, dispone de un manual de funciones, y es del conocimiento de los funcionarios?**

R: "Actualmente si hay un manual de funciones donde están estipulados lo que le corresponde a cada funcionario, actualmente la cámara de comercio tiene un crecimiento lo que ha presentado que haya mayor número de funcionarios a los que habían normalmente por lo que también se han creado nuevos cargos y eso nos hace falta actualizarlo y como establecer parámetros que cada funcionario tenga presente de cada una de sus funciones.

Debido a esto, que acabo de explicar de que hay nuevos funcionarios, que hay nuevos cargos, pues falta actualizarlo y de la misma manera darlo a conocer para que se tenga en cuenta las nuevas funciones y los nuevos cargos que se han implementado."

4. **¿De qué manera la Cámara de Comercio de Aguachica está involucrando las Tecnologías de la Información y la Comunicación y la adquisición de las mismas a su modelo de negocio?**

R: "Actualmente y por recomendación de la superintendencia y los entes de control, la cámara de comercio se ha venido actualizando en toda la parte de las TICS así como en el año 2015 la cámara de comercio inicio con el proceso de digitalización de los archivos públicos, con esto logramos adquirir nueva tecnología en computadores, escáner, impresoras, nuevos software que nos facilitan una mayor agilidad para consultar los archivos, para brindarle un mejor servicio a los comerciantes."

5. **¿Cuáles son sus funciones como Directora Administrativa y Financiera?**

R: "Soy la encargada de la parte administrativa, de la toma de decisiones importantes junto con el presidente ejecutivo y la encargada de organizar y de llevar toda la parte financiera de la entidad, el manejo de recursos humanos y de personal de la cámara de comercio."

6. **¿Qué procesos relacionados con la información maneja usted?**

R: "Manejo toda la parte de informes que se envían a los entes de control, manejo la parte financiera de la entidad, los balances, los estados financieros, los ingresos de caja y también la parte de las historias laborales de los funcionarios y toda la parte importante de la correspondencia, como son derechos de petición, los requerimientos que nos hagan a la cámara de comercio y que se deben dar respuesta."

7. **¿De qué forma está conformada en la cámara de Comercio de Aguachica el diagrama organizacional, Cadena de mando, Distribución de la autoridad y Departamentalización**?

R: "dentro de la estructura organizacional de la cámara, existe una junta directiva, luego está la presidencia ejecutiva, dentro de los departamentos existe la dirección de registros públicos, la dirección jurídica, la dirección administrativa y financiera y la dirección de centro de conciliación arbitraje, esas son nuestras principales jefaturas."

8. **¿Qué grado de importancia dan al área de Sistemas dentro de la organización y porqué es considerado como proceso de apoyo y no como un proceso estratégico, teniendo en cuenta que actualmente en un alto porcentaje de las funciones de la cámara son soportados por infraestructura tecnológica?**

R: "el área de sistemas actualmente está dentro de un proceso de apoyo ya que es el encargado de apoyar los procesos misionales de nuestra entidad como son registros públicos comisión y desarrollo y conciliación; porque no estratégico, porque dentro del proceso estratégico tenemos el proceso administrativo de la entidad como organizar, direccionar, controlar planear y organizar, por lo tanto este proceso no complementaria lo visional de la entidad mas no sería como un proceso estratégico.

La cámara de comercio en este proceso de las tecnologías, hace dos años que ha comenzado a tenerlo como un proceso más importante que anteriormente, de pronto por eso no se ha tenido como un proceso principal o estratégico. Inicialmente estamos con el proceso de digitalización, todo esto también abarca lo que tiene que ver con la gestión documental que sería un proceso que sistemas apoyaría y de pronto más adelante que se volviera a reestructurar todo ese aspecto, se podría tener en cuenta dentro de los procesos más importantes que es como iniciar la planeación y toda la parte organizacional dentro de los procesos estratégicos y tenerlo en cuenta en el proceso de sistemas."

Apéndice C. Entrevista Dirigida al Coordinador de Sistemas de la Cámara de Comercio De Aguachica.

Entrevista Dirigida al Coordinador de Sistemas de la Cámara de Comercio De Aguachica.

Fecha: 03/06/2016	**Nomenclatura: E006**

Objetivo: Evaluar los aspectos relacionados con la gestión de activos.
Criterio: Estándar ISO 27001, Objetivo de Control (9.CONTROL DE ACCESO).

1. **¿Quién es responsable y cuánto tiempo se requiere para que el administrador de seguridad cambie los privilegios de acceso a los sistemas después de que se le notifica de un cambio de empleado o de función de sub-contratista o estatus de trabajo?**
   La persona encargada de administrar los privilegios soy yo Maria Alejandra Merchan, realmente no existe un procedimiento formal que me notifique del cambio de empleo de un funcionario o subcontratista, simplemente me anuncian por teléfono y de manera inmediata realizo los cambios en los sistemas de información y correo electrónico.

2. **¿Permite que los empleados tengan acceso remoto a su red corporativa desde la computadora de su hogar o desde otros dispositivos propios de los empleados? Si es así, ¿qué mecanismos específicos de autentificación de acceso remoto se utilizan? ¿Pueden tener acceso a información de todas las aplicaciones?**
   Los empleados no tienen acceso remoto a la red corporativa de la Cámara de Comercio.

3. **¿Permite el uso de redes de área local inalámbricas (WLANs) y de otros dispositivos inalámbricos en su red en donde se puede tener acceso a información confidencial? ¿Qué protocolos se utilizan y qué controles de seguridad tiene?**
   La Cámara de Comercio cuenta con dos redes inalámbricas pero están ubicadas en redes diferentes a la corporativa, esto quiere decir que las personas que se conectan a la red inalámbrica no tienen acceso a la información confidencial, el protocolo de autenticación es WPA2.

4. **¿Permite que los empleados tengan acceso a cuentas externas de correo electrónico de Internet (ejem., Yahoo, Hotmail, etc.) desde su red? ¿Qué controles de seguridad tiene?**
   SI, los empleados tienen acceso a cuentas de correos electrónicos diferentes a los corporativos, el único control que utilizamos es que el antivirus tiene activo un filtro para correo de esa manera está notificando si detecta spam en los correos.

5. **¿Permite que los empleados utilicen programas de mensajes instantáneos (ejem., MSN messanger), redes de peer-to-peer (par-a-par) u otras herramientas de grupos de Internet o que almacenen información dentro o más allá de su red? Si es así, ¿Qué controles de seguridad tiene?**
   Ningún equipo de la Cámara de Comercio tiene instalado este tipo de aplicaciones, la verdad hasta el momento no se tiene controles para evitar su instalación, simplemente se realizan revisiones periódicas a cada equipo para realizar mantenimientos preventivos al software y de esa manera se eliminan los programas que no sean de uso corporativo.

6. **Además de su personal, ¿quién más tiene acceso a cualquiera de sus Sistemas de Información administrativos?**
   En estos momentos tres personal tenemos acceso como administradores a los diferentes sistemas de información, la señora coordinadora de sistemas quien labora en el área de registro y sistemas, tiene acceso como administradora al SII (Sistema Integrado de Información) y al DocuWare (Sistema encargado de la digitalización); La Administradora Financiera de la Cámara de Comercio, administra el GS7 (sistema Contable) y la Ingeniera de Sistemas de la Cámara de Comercio y administro el SII y el DocuWare.

7. **¿Tiene procedimientos para la instalación y administración controlada de quemadores de CD, unidades ZIP y memorias USB que puedan utilizarse para copiar información de cualquier tipo?**
   No existe ningún procedimiento hasta el momento a la mayoría de los trabajadores por lo general se les asigna una memoria USB para el transporte de información, pero no es controlado si extraer información.

8. **¿Cuál es el proceso para otorgar y/o revocar el acceso y privilegios a los sistemas informáticos? ¿Se documentan las solicitudes?**
   No existe ningún proceso y tampoco se documentan las soluciones para otorgar y/o revocar el acceso y privilegios a los sistemas informáticos, esto se realiza de manera informal, simplemente la Dr Lud en conjunto conmigo definimos los privilegios y los definimos en los sistemas de información y cuando ocurre algo extraordinario la Dr Lud me comunica lo que se debe cambiar y yo realizo las respectivas modificaciones.

9. **Enumere las personas/grupos responsables de otorgar y revocar acceso a aplicaciones que procesan la información. ¿Cómo se documenta esta autorización (facultamiento) y de quién la reciben?**
   En el área contable la encargada es la Dr Lud y en los demás sistemas de información yo soy la encargada, no están documentadas las autorizaciones.

10. **¿Aplican los procedimientos anteriores (8 y 9) a los empleados de planta, eventuales y sub-contratistas a quienes se les da acceso al sistema?**
    El acceso a los sistemas de información se da dependiendo de su rol en la Cámara de Comercio, a todos los empleados de planta que trabajan en el área de registro, archivo, desarrollo empresarial y conciliación tienen acceso al SII. Los contratistas no tienen acceso a los sistemas de información.

11. **¿Cómo se protege la información Confidencial/Restringida de acceso no autorizado en los sistemas de producción de la Cámara de Comercio de Aguachica?**
    Se protege a través de contraseñas de acceso, los servidores que contienen la información confidencial poseen contraseñas de acceso para acceder, y solo las maneja la coordinadora de sistemas y la Ingeniera de sistemas.

12. **Enumere todos los productos de seguridad (ejem., Antivirus, IDS, Firewalls, etc.) que se utilizan para todas las plataformas de los sistemas operativos que procesan información confidencial.**
    Solo tenemos antivirus.

13. **Los usuarios de los sistemas que contienen información confidencial, ¿tienen un solo nombre de usuario (User ID) por sistema?**
    Si, por sistema de información solo tiene un nombre de usuario.

14. **Donde no es posible tener control de acceso, ¿existen controles por medio de pruebas de auditorías (audit trails) y procesos de conciliación?**
    No existe algo que no sea posible de controlar.

15. **¿Tiene un proceso documentado para habilitar a los gerentes de negocio para que revisen y verifiquen las autorizaciones cuando menos semestralmente para los sistemas y aplicaciones que procesan información?**
    No existe un proceso documentado, la alta gerencia requiere informes de manera anual, semestral y trimestral para ello no acceden directamente al sistema de información si no que solicitan los respectivos reportes en formato de Excel. Pero de igual manera la Dr Lud Pabón tiene acceso al sistema de información SII el cual almacena toda la información Cameral.

16. **¿Qué políticas o criterios tienen establecidos para la creación de contraseñas robustas, para los usuarios que utilizan los sistemas de información muestre la documentación?**

El manual de Políticas de Información de la Cámara de Comercio de Aguachica, contempla las Políticas de Uso de las Contraseña pero este manual no está aprobado ni se ha dado a conocer a los empleados.

17. **¿De qué manera controlan el acceso de personal no autorizado al código fuente de los programas?**
    El único servidor que posee el código fuentes del sistema de información es el DocuWare y este posee contraseñas de accedo para ingresar.

18. **¿Qué herramientas para la administración de sistemas utilizan?, mencione cada una.**
    No contamos con ninguna herramienta para administrar el sistema, simplemente utilizamos la administración de cada sistema de información.

Firma del Auditor	Firma del Auditado
Nombre:	Nombre:
Cargo:	Cargo:

Entrevista Dirigida al Coordinador de Sistemas de la Cámara de Comercio De Aguachica.

Fecha: 03/06/2016	**Nomenclatura: E007**

Objetivo: Evaluar los aspectos relacionados con la gestión de activos.

Criterio: Estándar ISO 27001, Objetivo de Control (11.SEGURIDAD FÍSICA Y AMBIENTAL).

1. ¿Con qué frecuencia se realizan revisiones de seguridad física de las instalaciones? Proporcione los resultados de la última revisión.
No están reportadas las revisiones que se realizan pero constantemente se verifican las instalaciones físicas para realizarles mantenimientos o cuando surge una eventualidad se realizan los correctivos.

2. Describa los controles de acceso al perímetro de esta instalación (ejem., puntos de verificación del perímetro, uso de controles de acceso con tarjeta incluyendo retención del log (bitácora), revisión de paquetes, cobertura con circuito cerrado de televisión y monitoreo).
En las afueras de la cámara de comercio existen 4 cámaras de seguridad.

3. ¿Comparte estas instalaciones con otras personas diferentes a empleados de la Cámara de Comercio de Aguachica? De ser así, describa las zonas ocupadas y quiénes son las otras personas que ocupan el espacio contiguo al suyo.
Si, el señor Pedro Santana es el encargado del enlace territorial del Sur del Cesar con el Departamento, comparte las instalaciones de la Cámara de Comercio específicamente la sala de juntas.

4. ¿Existe alguna área de entrega o descarga? De ser así, describa los controles de acceso existentes. ¿Existe monitoreo por circuito cerrado de televisión en esta área?
No existe área de carga ni de descarga.

5. ¿Deben los visitantes firmar una bitácora de seguridad y estar acompañados por alguien mientras se encuentran en áreas de seguridad?
No deben firmar nada los visitantes, cuando ingresan al cuarto de telecomunicaciones van acompañados por mí.

6. ¿Qué tipo de controles existen para evitar el acceso no autorizado a áreas como data center?
Solamente se evita el acceso físicamente a través de puerta con llave.

7. ¿Se almacena la información de los clientes en un área segura con acceso restringido sólo a personal autorizado?
Físicamente la información de los clientes se encuentra almacenada en un archivo que está bajo llave y solo la encargada de archivo tiene acceso a esta área.

8. ¿Se necesita de una autorización diferente o adicional para tener acceso al interior del centro de datos (data center) y/o áreas restringidas?
Si, para acceder al data center deben ingresar conmigo y al resto de áreas de seguridad deben ingresar con la encargada de servicios generales quien es la que maneja las llaves de las oficinas.

9. Para el centro de datos (data center), existen plafones y pisos falsos que puedan utilizarse para tener acceso no autorizado a esta área restringida? ¿Los paredes exteriores que rodean la construcción del centro de datos (data center) son del piso al techo?
La data center se encuentra en un cuarto exclusivo para eso, las paredes son del piso al techo y no tiene pisos falsos.

10. ¿El ingreso a oficinas y despechos es controlada de qué manera, cualquier personal ingresa?
Por lo general el personal que llega pregunta en recepción por la persona que busca y se le da la orientación en donde la puede encontrar, pero no se acompaña, pero también existen personas que no preguntan por nadie y siguen e ingresan a donde deseen, la única oficina que siempre está cerrada es el Datacenter, el resto de oficinas por lo general están abiertas y no existe control de acceso del personal.

11. ¿Existe un proceso para controlar la existencia de llaves (ejem., asignación, copias de llaves)?
No existe un proceso para el control de las llaves, la persona encargada de las llaves es servicios generales, la Dr Lud, controlan el manejo de las llaves de todas las oficinas y el auditorio y en la noche el celador se encarga de controlar las llaves de las puertas de entrada principal.

12. ¿Tienen las instalaciones un sistema externo / interno de grabación de circuito cerrado de TV que guarde los registros por 31 días o más (digital o analógico)?
Si, existe sistema de grabación de circuito cerrado con 10 cámaras las cuales están conectadas en puntos estratégicos, pero solo permiten grabar por siete días seguidos, luego comienzan ha sobre escribirse u es digital.

13. Si es el caso, ¿se cambian las combinaciones de las cerraduras con regularidad? ¿Con qué frecuencia? ¿Qué evidencia existe de que se realizan estos cambios?
No se cambian con regularidad.

14. ¿Está constantemente vigilada la instalación por la policía pública o por un servicio privado de seguridad? Descríbalo.
La Cámara de Comercio tiene contratado a una persona que trabaja desde las 7 pm hasta las 6 am, es un vigilante particular; no existe un CAI cerca y tampoco la policía pública realiza revisión de manera frecuente.

15. ¿Están protegidas las instalaciones con algún sistema de alarma de detección de intrusión? ¿Existe una estación central que monitoree las alarmas?
Si, existe una alarma que está ubicada en la entrada principal y no está monitoreada por alguna centrar.

16. ¿Están protegidas las instalaciones con sistemas de alarma de detección de humo y fuego? Proporcione la documentación que señale la ubicación de dichos sistemas.
La Cámara de Comercio cuenta con una alarma anti humo y fuego, pero no existe documentación al respecto.

17. ¿Están protegidas las instalaciones por sistemas de supresión de fuego (rociadores/gas inerte)? ¿Cuándo se probaron por última vez?
Si, existen dos, no existen registros de las pruebas.

18. ¿Están los sistemas contra incendio/de entrada conectados a la central de bomberos local o a las autoridades correspondientes?
No

19. Si la instalación es un centro de datos (data center), ¿está identificado fácilmente como tal en el exterior? Describa los controles de acceso existentes.
El datacenter está ubicado en un cuarto y en la parte exterior del cuarto existe una tableta que indica el nombre de "Sistemas". El control de acceso es físico, se proteje con una puerta bajo llave.

20. ¿Tiene el centro de datos (data center) controles de temperatura y humedad que sean independientes del resto de la edificación?
No tiene controles de temperatura ni humedad.

21. ¿Tiene en las instalaciones fuentes de poder independientes y separadas, y se prueban constantemente estas fuentes de poder? Describa las pruebas y la frecuencia con la que se hacen.
Si, la Cámara de Comercio cuenta con fuentes de poder pero no son probadas con frecuencia.

22. ¿Tiene un respaldo de Fuente de Poder Ininterrumpible (UPS) para los sistemas de cómputo? ¿Cuál es su capacidad (en minutos de respaldo) y cuándo se probó y utilizó por última vez?
La Cámara de Comercio cuenta con una UPS de 1 KW de capacidad en la cual están conectados los servidores, y los equipos activos de red como Switch, Router, Modem. En tiempo y se hacen pruebas simplemente se sabe que funciona porque cundo se va la luz quedan prendidos los equipos mencionados y se apagan manualmente. La última vez que se utilizo fue el domingo 4 de junio.

23. ¿Tiene un generador de respaldo? Si es así, describa su capacidad, cuánto tiempo le lleva pasar al generador, con qué frecuencia se prueba, cuándo se utilizó por última vez para soportar los sistemas de producción, cuánto tiempo puede operar sin tener que ponerle combustible, y qué medidas se han tomado para asegurarse de cargarle el combustible oportunamente?
No existen plantas eléctricas en la Cámara de Comercio.

24. ¿Cómo están asegurados los Racks de las conexiones telefónicas y de los cables de datos? ¿Quién tiene acceso a estos y cómo se autoriza el acceso? ¿Puede proporcionar una

lista de las personas que tienen acceso, incluyendo las personas de las otras oficinas en el caso de estar en un edificio con diferentes inquilinos?
Existe un solo Rack en el cual están las conexiones telefónicas y de datos, están asegurados al piso con tornillos y se encuentran ubicados en el cuarto donde está el Datacenter. El control de acceso es físico con puerta de manera y asegurada con cerradura bajo llave, solo ingresan el personal encargado de sistemas, La coordinadora de sistemas y La Ingeniera de sistemas, y todos los empleados de la cámara si van a ingresar piden lo hacen bajo la supervisión del personal de sistemas.

25. ¿Está ubicado en el centro de datos (data center) o en sitios seguros de servidores todo el equipo (computadoras y servidores de producción y prueba)? Si no es así, indique la ubicación y cualquier otro control compensatorio.
Los servidores están ubicados en el Datacenter.

26. ¿Qué procedimiento es utilizado para eliminar de manera segura información o dispositivos de computo que ya no sea necesario?
La información es eliminada cuando ya no es necesaria para la Cámara de Comercio, no existe ningún procedimiento para hacerlo de forma segura, y para la eliminación de equipos de cómputo, se guardan en el cuarto de Archivo cuando ya no son necesarios, por lo general estos elementos son donados a colegios o personas que no necesiten y cuando son eliminados por que ya no sirven se arrojan a la basura.

27. ¿Con que frecuencia realiza mantenimientos preventivos a los equipos de cómputo, impresoras y escáneres, indique los registros de los mismos?
A los equipos de cómputo e impresoras cada tres meses, a los escáneres dependiendo del tipo que sea se realiza el manteniendo de acuerdo a la cantidad de hojas digitalizadas. El registro se lleva en Excel donde cada equipo tiene una hoja de vida y se registran los mantenimientos.

28. ¿Tiene registros de los mantenimientos correctivos, ejemplo: cambios al hardware y software?
Si, en la ficha técnica de cada equipo de cómputo, impresora y escáner si aloja una hoja de Excel con los mantenimientos ya sean correctivos o preventivos y una hoja para los cambios ya sea instalación de software o hardware.

29. ¿Tiene algún equipo de cómputo almacenado fuera de sus instalaciones que contenga información de la Cámara de Comercio de Aguachica? Si es así, describa cómo está asegurado.
No

30. ¿Puede hacerse de forma remota el mantenimiento al equipo de cómputo de su empresa? Si es así, ¿quién tiene acceso y cómo es controlado?
No se puede hacer de forma remota mantenimiento a los equipos de cómputo.

Firma del Auditor Nombre: Cargo:	Firma del Auditado Nombre: Cargo:

Apéndice D. Oficio de entrega del dictamen.

Aguachica - Cesar, 07 de Junio 2016

Señor
EDUARDO SOLANO FORERO
Director Ejecutivo
Cámara de Comercio
Aguachica

Cordial saludo,

En carácter de auditores de sistemas nos permitimos informar los resultados obtenidos en el proceso de auditoría que se realizó el 25 de mayo de 2016 al 05 de junio de 2016 en la oficina de sistemas de la Cámara de Comercio de Aguachica, cesar.

Se realizaron revisiones y evaluaciones de forma exhaustiva de la distribución organizacional, de los procesos, estructuración de funciones, seguridad de la información, seguridad física y del entorno.

Al respecto, cabe precisar, que la observación realizada se efectuó sobre el período auditado, para el cual se carecía, además, de un plan de revisión; en todo caso, en base a los antecedentes aportados, se levanta la observación formulada.

A continuación se plasma el dictamen correspondiente al proceso de auditoría que se realizó empleando métodos, operaciones y medios que permitieron identificar los hallazgos que ponen en riesgo el funcionamiento de la operativa y los principios básicos de la seguridad de la información.

Atentamente,

ALEXANDER MENESES MARTINEZ
Administrador de Empresas

ERNEY ALBERTO RAMIREZ CAMARGO
Ingeniero de Sistemas

MARIA ALEJANDRA MERCHAN VILLALBA
Ingeniera de Sistemas

YADITZA SUAREZ DE LA CRUZ
Ingeniera de Sistemas

Anexos: tres (39 hojas)

Copia: Dr. Lud Pabón Chona, Directora Administrativa y Financiera.

Apéndice E. Oficio de entrega de análisis de riesgos.

Aguachica, 27 de septiembre de 2016

Señor
EDUARDO SOLANO FORERO
Director Ejecutivo
Cámara de Comercio
Aguachica

Asunto: entrega del Análisis de Riesgos.

Cordial saludo:

Con el fin de dar cumplimiento al proyecto titulado: DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI BASADO EN EL ESTÁNDAR ISO 27001, PARA LOS PROCESOS SOPORTADOS POR EL AREA DE SISTEMAS EN LA CÁMARA DE COMERCIO DE AGUACHICA, CESAR, se hace entrega oficial del Análisis de Riesgos que corresponde a una de las actividades de la fase PLAN del ciclo PDCA del SGSI.

El documento contiene la estimación del Riesgo potencial, que fue hallado con los parámetros establecidos en la metodología Magerit V3, en donde se realizó caracterización de activos y amenazas, selección de salvaguardas, estimación de impacto y finalmente, estimación del riesgo potencial.

Atentamente,

ALEXANDER MENESES MARTINEZ
Administrador de Empresas

ERNEY ALBERTO RAMIREZ CAMARGO
Ingeniero de Sistemas

MARIA ALEJANDRA MERCHAN VILLALBA
Ingeniera de Sistemas

YADITZA SUAREZ DE LA CRUZ
Ingeniera de Sistemas

Anexos: uno (7 hojas)

Copia: Dr. Lud Pabón Chona, Directora Administrativa y Financiera.

Apéndice F. Oficio de entrega de Políticas de Seguridad de la Información.

Aguachica, 27 de septiembre de 2016

Señor
EDUARDO SOLANO FORERO
Director Ejecutivo
Cámara de Comercio
Aguachica

Asunto: entrega de las Políticas de Seguridad de la Información.

Cordial saludo:

Con el ánimo de mejorar la estrategia de Seguridad de la información de la CÁMARA DE COMERCIO DE AGUACHICA, 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 y se hace entrega oficial de la misma, para la Cámara de Comercio de Aguachica, Cesar. Como marco de trabajo de la organización en lo referente al uso adecuado de los recursos tecnológicos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

Atentamente,

ALEXANDER MENESES MARTINEZ
Administrador de Empresas

ERNEY ALBERTO RAMIREZ CAMARGO
Ingeniero de Sistemas

MARIA ALEJANDRA MERCHAN VILLALBA
Ingeniera de Sistemas

YADITZA SUAREZ DE LA CRUZ
Ingeniera de Sistemas

Anexos: uno (56 hojas)

Copia: Dr. Lud Pabón Chona, Directora Administrativa y Financiera.

Apéndice G. Acuerdo de confidencialidad.

ACUERDO DE CONFIDENCIALIDAD

Ciudad y Fecha: _____

Yo, _____ me comprometo a acatar y dar cumplimiento a cada una de las políticas establecidas en el documento POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN y así mismo mantener estricta confidencialidad sobre toda información que por una u otra razón deba conocer como producto del trabajo que actualmente realizo o realizaré.

Firma: _____

Documento de identificación: _____

Empresa: _____

Área de La Cámara de Comercio: _____

_____

Vo. Bo. Recursos Humanos

Apéndice H. Control de cambios

CONTROL DE CAMBIOS				
Versión	Fecha	Revisó	Aprobó	Cambio
1	2014-07-14	2014-07-14	CERTICÁMARA	

Apéndice I. Política de asuntos específicos: identificación biométrica.

POLÍTICA DE ASUNTOS ESPECÍFICOS: IDENTIFICACIÓN BIOMÉTRICA

1. ALCANCE

El presente apéndice al documento de Política de Seguridad de la Información, reglamenta la protección y uso de los activos de información relacionados con la integración de los servicios de la Cámara de Comercio, Confecámaras y la Registraduría Nacional del estado civil, 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 previamente un acuerdo de confidencialidad (Apéndice G), que los compromete con el cumplimiento de las políticas de seguridad ya descritas. Los usuarios de los activos de se denominan así:

Funcionarios de La Cámara de Comercio: Se definen como los empleados de la Cámara de Comercio que son susceptibles de manipular el sistema de autenticación biométrica en línea.

2. PROCEDIMIENTO

Los miembros del Comité de Seguridad, conscientes que los recursos de información son utilizados de manera permanente por los usuarios de la Cámara de Comercio que manipulan el servicio de identificación biométrica, definidos en este apéndice , 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.

3. Medidas disciplinarias por incumplimiento de políticas de seguridad

Cualquier 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 una sede, la Cámara de Comercio podrá suspender la prestación del servicio de identificación biométrica.