PROPUESTA PARA IMPLEMENTACION DE CONTROLES ESTABLECIDOS POR LA NORMA ISO/IEC 27001:2013 - ANEXO A, APLICABLES EN EL CENTRO DE DIAGNOSTICO AUTOMOTOR - CEDAC LTDA., UBICADO EN LA ZONA INDUSTRIAL DE LA CIUDAD DE CÚCUTA

MARTIN JAVIER DIEZ CONTRERAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
CUCUTA
2018

PROPUESTA PARA IMPLEMENTACION DE CONTROLES ESTABLECIDOS POR LA NORMA ISO/IEC 27001:2013 - ANEXO A, APLICABLES EN EL CENTRO DE DIAGNOSTICO AUTOMOTOR - CEDAC LTDA., UBICADO EN LA ZONA INDUSTRIAL DE LA CIUDAD DE CÚCUTA

MARTIN JAVIER DIEZ CONTRERAS

Proyecto de grado para optar al título de
Especialista en seguridad informática

Director de proyecto
Esp. Freddy Enrique Acosta
Ingeniero de sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
CUCUTA, NORTE DE SANTANDER
2018

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del director del proyecto

_____

Firma del jurado

_____

Firma del jurado

Cúcuta 8 de junio de 2018

DEDICATORIA

El presente proyecto de grado para optar al título de Especialista en Seguridad Informática lo dedico a mis padres, hermanas y muy especialmente a mi esposa quien me ha acompañado a lo largo de este proceso, apoyándome con su tiempo y dedicación.

Martin Javier Diez Contreras

AGRADECIMIENTOS

Martin Javier Diez Expresa su Agradecimiento a Dios por haberme dado la oportunidad, la fuerza y la salud para poder realizar estos estudios y los tutores Ingeniera especialista Helena Alemán quien me oriento en la forma como debía enfocar este proyecto y el Ingeniero especialista Freddy Enrique Acosta quien me dirigió y me ayudo a estructurar el trabajo final.

Martin Javier Diez Contreras

GLOSARIO

Amenaza. en seguridad de la información se define como toda situación, circunstancia o persona ya sea interna o externa en una entidad, organización, red pública o privada, que pueda causar daño a la información de un sistema como robo, divulgación de datos confidenciales, alteración de datos, borrado total de datos, negación de un servicio, entre otros[1].

Autorización: Acción de otorgar el acceso a usuarios o grupo de usuarios con el fin de que puedan usar los recursos de un sistema como aplicaciones, internet, descarga de datos entre otros[1].

Control de acceso. Limitar el acceso a objetos de acuerdo a los permisos de acceso del sujeto, es decir, se puede otorgar una autorización para acceder al sistema, pero sus permisos son limitados ejemplo poder acceder a una determinada información para consultarla, pero no poner ni modificarla, descárgala o borrarla[2].

Cortafuego. Herramienta de seguridad que proporciona un límite entre redes de distinta confianza o nivel de seguridad mediante el uso de políticas de control de acceso de nivel de red, esta herramienta viene integrada con algunos sistemas operativos y su configuración es modificable por el administrador del equipo con el fin de establecer hasta qué punto pueda otorgar un determinado acceso[1].

Disponibilidad. Acceso y utilización de la información y los sistemas en los que la misma es procesada por parte de los individuos, entidades o procesos que se encuentran autorizados para ello[2].

Ethernet. Sistema de red de área local de alta velocidad en los que se pueden conectar un grupo determinado de equipos[1].

---

[1] ARAYA, D. Glosario de términos de Seguridad Informática. [En línea]. [Consultado 20 de noviembre 2016]. Disponible en Internet: (http://safemode-cl.blogspot.com.co/2006/07/glosario-de-terminos-de-seguridad.html).

[2] GOMEZ, Á. Enciclopedia de la Seguridad Informática. México: Alfaomega; 2007.

Gestión de redes. Controlar diversos aspectos de una red para optimizar su eficiencia como por ejemplo monitorizar, probar, configurar, analizar y evaluar los recursos de una red[3].

Gestión de seguridad. Proceso de establecer y mantener la seguridad en un sistema o red de sistemas informáticos. Las etapas de este proceso incluyen la prevención de problemas de seguridad, detección de intrusiones, investigación de intrusiones, y resolución[3].

Integridad. Hace referencia a la exactitud y completitud que posee la información, es decir, que la misma no le falten datos o tenga datos que no corresponden a dicha información[4].

Paquete. Estructura de datos con una cabecera que puede estar o no lógicamente completa, es decir, es cada uno de los tramos en el que se divide la información que se va a enviar a través del nivel de red[3].

Política de seguridad. Conjunto de estatutos que describen la filosofía de una organización respecto a la protección de su información y sistemas informáticos, todas estas componen unas reglas que la empresa seguirá para minimizar riesgos y amenazas en sus sistemas de información[4].

Riesgo: es aquella probabilidad que tienen los activos ya sean de hardware o software de sufrir algún daño debido a las vulnerabilidades y amenazas que estos puedan tener[4].

SGSI: Sistema de gestión de seguridad de la información.

Vulnerabilidades. Hace referencia a las debilidades que puede tener un sistema las cuales podrían ser aprovechadas por un pirata informático para realizar un ataque, estas debilidades pueden ser a nivel de hardware o software[5].

---

[3] ARAYA, Op cit. p1.
[4] GOMEZ. Op cit. p.4-25.
[5] SUAREZ, S. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Tesis de Especialización. Bogotá: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería; 2015.

RESUMEN

El Centro de Diagnóstico Automotor de Cúcuta - CEDAC Ltda., es una Empresa Industrial y Comercial del Estado – EICE, de naturaleza jurídica pública, de carácter oficial, del orden nacional y de responsabilidad limitada; su información juega un papel esencial puesto que en ella se incluye todo lo relacionado con procesos de contratación con capital público, datos contables, datos financieros, datos personales de trabajadores, contratistas, proveedores, usuarios, datos de facturación y por su puesto las Revisiones Tecnicomecanicas y de Emisiones Contaminantes – RTyEC que son de vital importancia relacionadas directamente con el objeto misional de la entidad y que se realizan diariamente.

Por lo anterior, este trabajo busca proponer la implementación de los controles establecidos por la norma ISO/IEC 27001 - anexo A, aplicables en el Centro de Diagnóstico Automotor de Cúcuta - CEDAC Ltda., ubicado en la zona industrial de la ciudad de Cúcuta; con el fin de mitigar los riesgos asociados a la seguridad de la información recomendando el estableciendo unas políticas de seguridad que permitan que la información sea integra, confiable y que este siempre disponible.

Palabras claves: Amenaza, Ataque, controles de seguridad, ISO 27001, Políticas de seguridad, SGSI, Vulnerabilidad.

ABSTRACT

The Automotive Diagnostic Center of Cúcuta - CEDAC Ltda., Is an Industrial and Commercial Company of the State - EICE, of public juridical nature, of an official nature, of the national order and of limited responsibility; your information plays an essential role since it includes everything related to contracting processes with public capital, accounting data, financial data, personal data of workers, contractors, suppliers, users, billing information and, of course, the Mechanical-Mechanical Reviews and Pollutant Emissions - RTyEC, which are of vital importance directly related to the missionary purpose of the entity and which are carried out daily.

Therefore, this work seeks to propose the implementation of the controls established by ISO / IEC 27001 - Annex A, applicable in the Automotive Diagnostic Center of Cúcuta - CEDAC Ltda., Located in the industrial zone of the city of Cúcuta; in order to mitigate the risks associated with information security by recommending establishing security policies that allow information to be integrated, reliable and always available.

Keywords: Threat, Attack, security controls, ISO 27001, Security policies, ISMS, Vulnerability

CONTENIDO

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

INTRODUCCION

En este trabajo se lleva a cabo la determinación de la situación actual de la seguridad de la información en el Centro de Diagnóstico Automotor de Cúcuta - CEDAC Ltda., que es una Empresa Industrial y Comercial del Estado – EICE, de naturaleza jurídica pública, de carácter oficial, del orden nacional y de responsabilidad limitada, con el fin de observar si se cumplen algunos de los controles establecidos por la norma ISO/IEC 27001 en su Anexo A y en tal caso Proponer la implementación de los controles que apliquen a esta entidad, ya que dicha norma tiene como principal objetivo proteger la integridad, confidencialidad y disponibilidad de todos los activos de una organización, como dice **Kenneth Amaditz** "*La Seguridad no es solo un proceso Tecnológico… Es un proceso Organizacional*"[6] esta frase aplica extraordinariamente a la norma antes mencionada ya que esta no reduce la seguridad a controles basados solamente en software o hardware sino a políticas de seguridad que van desde el proceso de contratación, capacitación del personal hasta cada uno de los activos de la entidad.

Uno de los activos más importantes que tiene una organización hoy en día es la información y en este nuevo mundo la gran mayoría por no decir que toda la información se encuentra de manera digital ya sea en los equipos de cómputo o servidores, discos duros extraíble o espacios en la nube. Muchas empresas aun no ven la importancia de implementar sistemas que mitiguen la perdida de este valioso activo como lo establece la revista Semana en su artículo "*Las empresas en Colombia no invierten en seguridad digital*"[7],

El Centro de Diagnóstico Automotor de Cúcuta - CEDAC Ltda. Posee información que juega un papel esencial puesto que en ella se incluye todo lo relacionado con procesos de contratación con capital público, datos contables, datos financieros, datos personales de trabajadores, contratistas, proveedores, usuarios, datos de facturación y por su puesto las Revisiones Tecnicomecanicas y de Emisiones Contaminantes – RTyEC que son de vital importancia relacionadas directamente con el objeto misional de la entidad y que se realizan diariamente.

---

[6] RODRIGUEZ, A. La importancia de la Seguridad Informática. [En línea]. [Consultado 10 de mayo 2018]. Disponible en internet: http://www.trustdimension.com/la-importancia-de-la-seguridad-informatica/

[7] SEMANA. Tecnología. Las empresas en Colombia no invierten en seguridad digital. Bogotá. 09, junio, 2016. [En línea]. [Consultado 10 de mayo 2018]. Disponible en Internet: https://www.semana.com/tecnologia/articulo/colombia-no-invierte-en-seguridad-digital/492724.

1. DEFINICION DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La información que maneja el Centro de Diagnóstico Automotor de Cúcuta Ltda., juega un papel fundamental en el funcionamiento de la empresa, dentro de esta información se incluye todo lo relacionado con contrataciones, datos contables de la entidad, datos personales de sus empleados y proveedores, datos de facturación y por su puesto y de gran importancia todos los datos de sus clientes y las revisiones tecnicomecanicas y de emisiones contaminantes que se realizan diariamente.

La integridad y disponibilidad de esta información es crucial para el correcto funcionamiento de la empresa, por lo que, si se llegara a perder o la información fuese robada, alterada o borrada, la compañía podría estar en grandes problemas que pudieran llevar a detener la continuidad del negocio, imposibilidad de prestar un servicio y por ende perder mucho dinero, por ejemplo en el año 2017 se propago como una pandemia uno de los virus informáticos que causo uno de los mayores daños registrados en la historia el cual secuestraba los datos de las computadoras que infectaba e hizo que compañías como Telefónica, en España, Renault, en Francia, y de entidades como el Ministerio de Interior de Rusia tuvieran que cesar sus actividades, Se calcula, según la compañía de seguridad Cyence, que este ciberataque llegó a afectar alrededor de 10.000 organizaciones y 200.000 computadores en 150 países, con pérdidas que podrían superar los 4.000 millones de dólares[8].

La empresa cuenta con un gran número de activos como lo son equipos de cómputo, servidores, impresoras, toda una red LAN, paquetes de software como TNS para la contabilidad, software de revisión tecnicomecánica SOLTELEC y sistemas operativos Windows para los equipos de cómputo, sin embargo todos estos activos carecen de controles de seguridad que mitiguen los riesgos de pérdidas, alteración o robo de la información e incluso controles en la red que impidan el ataque de intrusos desde fuera de la entidad.

Dentro de las vulnerabilidades y riesgos que pueden tener los activos de la entidad al carecer de controles se pueden mencionar: ataques por piratas informáticos; inclusión de algún virus, troyano, bomba lógica u otro malware que puedan afectar

[8] PORTAFOLIO. Así roban la información de las empresas los piratas informáticos. [En línea]. [Consultado 10 de mayo 2018]. Disponible en Internet: http://www.portafolio.co/innovacion/asi-roban-la-informacion-de-las-empresas-los-piratas-informaticos-506522.

el funcionamiento de los equipos de cómputo o incluso dejar totalmente inoperante el sistema operativo; daño de algún equipo por picos de energía al no contar con reguladores de voltaje; perdida de información de la base de datos por no realizarse adecuadamente los Backup; entre otras vulnerabilidades y riesgos que se puedan detectar durante el desarrollo del proyecto.

Con todo esto la empresa se encuentra expuesta no solo a una posible pérdida de la información; sino también, a empleados que con malas intenciones quieran entorpecer el trabajo de la compañía, lo cual puede desencadenar en una interrupción del servido prestado por la entidad que desde un punto de vista financiero se traduciría en una gran pérdida de dinero.

En la actualidad existen normas que establecen unos procedimientos, metodologías y que ayudan a minimizar al máximo el riesgo de perder información; así como, controles que se pueden llevar a cabo para mantener segura la información y estar alerta ante cualquier vulnerabilidad que se pueda presentar y poder minimizarla.

1.2 FORMULACIÓN DEL PROBLEMA

¿En qué medida la implementación de los controles establecidos por la norma ISO/IEC 27001 – Anexo A, aplicables en el Centro de Diagnóstico Automotor – CEDAC LTDA. Ubicada en la Zona Industrial de la ciudad de Cúcuta, podrá mejorar la seguridad de sus activos informáticos?

1.3 ALCANCE Y LIMITACIONES

1.3.1 Alcance. El presente trabajo de grado se encuentra entre los proyectos de gestión de seguridad y lo que pretende es realizar una propuesta para realizar la implementación de controles establecidos por la norma ISO/IEC 27001:2013 del Anexo A, aplicables en el centro de diagnóstico automotor - CEDAC Ltda., ubicado en la zona industrial de la ciudad de Cúcuta.

1.3.2 Limitaciones. Es conveniente resaltar que el desarrollo del presente proyecto no abarcara temas como los que se definen a continuación:

- No se realizará el proceso de gestión para la determinación de riesgos en la entidad.

- No se realizará el proceso de implementación de un sistema de seguridad de la información.

- No se implementará ninguna política de seguridad para la entidad ni tampoco se implementará ningún control de la Norma ISO/IEC 27001:2013.

- No se realizará ningún Test de penetración para comprobar la seguridad de la red.

- No se llevarán a cabo capacitaciones de los empleados en temas de seguridad de la información.

- No se llevará a cabo el proceso de certificación de la entidad en la ISO/IEC 27001:2013.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Proponer la implementación de los controles establecidos por la norma ISO/IEC 27001 - ANEXO A, aplicables en el CENTRO DE DIAGNOSTICO AUTOMOTOR - CEDAC LTDA., ubicado en la Zona Industrial de la Ciudad de Cúcuta.

2.2 OBJETIVOS ESPECÍFICOS

- Estudiar cada uno de los controles establecidos por la norma ISO/IEC 27001 - ANEXO A.

- Determinar los controles establecidos por la norma ISO/IEC 27001 - ANEXO A que le son aplicables al CENTRO DE DIAGNOSTICO AUTOMOTOR - CEDAC LTDA., ubicado en la Zona Industrial de la Ciudad de Cúcuta.

- Proponer el aplicar los controles que no se encuentren establecidos, con políticas de seguridad de la información, basados en la norma ISO/IEC 27001 - ANEXO A, los cuales minimicen riesgos, vulnerabilidades que puedan afectar la integridad y la disponibilidad de los datos del CENTRO DE DIAGNOSTICO AUTOMOTOR - CEDAC LTDA., ubicado en la Zona Industrial de la Ciudad de Cúcuta.

3. JUSTIFICACIÓN

El Centro de Diagnóstico Automotor de Cúcuta - CEDAC Ltda., es una Empresa Industrial y Comercial del Estado – EICE, de naturaleza jurídica pública, de carácter oficial, del orden nacional y de responsabilidad limitada. Es además, un instrumento técnico de las autoridades de tránsito y ambiente, siendo su misión la de contribuir y fomentar la cultura en seguridad vial, movilidad y conservación del medio ambiente a través del diagnóstico al estado de los vehículos, así como el desarrollo de programas de formación e integración de servicios relacionados con el sector de tránsito y transporte[9].

La Revisión Tecnicomecanica y de Emisiones Contaminantes – RTyEC es un procedimiento obligatorio para todos los vehículos automotores de acuerdo con la ley, los criterios y pruebas establecidas en las Normas Técnicas Colombianas NTC- 5375, NTC- 5385 que utilizan las autoridades colombianas para saber si poseen las condiciones mecánicas óptimas para poder circular por las vías públicas y privadas del país[10], a raíz de lo anterior la empresa maneja una gran cantidad de información que se encuentra de forma digital en sus servidores y diferentes equipos de cómputo y esta crece día a día de forma exponencial con cada una de las revisiones.

Por consiguiente, se hace indispensable garantizar la protección de todos los activos de hardware y software, así como toda la información que maneja la entidad, con el fin de poder mitigar o reducir a lo más mínimo el riesgo de daño, perdida, alteración, suplantación o robo de dichos activos y datos de la empresa, ya que si se cumpliera cualquiera de estas amenazas a la información la entidad se enfrentaría a sanciones como cierre parcial o definitivo por parte de los entes de control y vigilancia como lo sería en este caso la Superintendencia de puertos y trasportes y el Organismo Nacional de Acreditación-ONAC.

Con fundamento en lo anterior y con la realización de este proyecto, se pretende garantizar que en el Centro de Diagnóstico Automotor de Cúcuta – CEDAC Ltda., la protección de todos los activos de hardware y software así como toda su información (base de datos de los procesos de contratación con capital público, datos contables, datos financieros, datos personales de trabajadores, contratistas, proveedores, usuarios, datos de facturación y por su puesto la base de datos más

[9] CENTRO DE DIAGNÓSTICO AUTOMOTOR DE CÚCUTA LTDA. Manual de Procedimientos Administrativos: GTH-02-R-03, Versión 1. Cúcuta: CEDAC; 2017.

[10] MINISTERIO DE TRANSPORTE DE COLOMBIA. Resolución 3768 (26, septiembre, 2013). Por la cual se establecen las condiciones que deben cumplir los Centros de Diagnóstico Automotor para su habilitación, funcionamiento y se dictan otras disposiciones. Diario oficial. Bogotá, 2013. No. 48.926. p.16.

significativa como lo es la de las Revisiones Tecnicomecanicas y de Emisiones Contaminantes – RTyEC) que son de vital importancia para cumplir directamente con el objeto misional de la entidad y todo lo exigido por las autoridades nacionales, departamentales y locales.

4. MARCO REFERENCIAL

4.1 MARCO TEORICO

4.1.1 La seguridad informática. Anteriormente, la seguridad informática era un tema del cual tal vez no se hablaba mucho; sin embargo, hoy en día la seguridad de la información ha tomado mucha importancia en la comunidad, en los hogares, en las empresas, en las instituciones educativas, a nivel económico, legislativo, político y social en general.

La gran mayoría de las personas manejan información que en algunos casos es de vital importancia ya sea para el trabajo diario (archivos de texto, hojas de cálculo, presentaciones) o incluso para la comunicación con otras personas (números de teléfono, correos electrónicos). Sin embargo, no solo cada persona maneja su propia información sino también las empresas, organizaciones y entidades poseen bases de datos las cuales van creciendo diariamente con información ya sea de usuarios, clientes, proveedores o cualquier otro dato relacionado con la actividad que se desarrolle.

Hace unos 25 años atrás, la seguridad de la información solo se centraba en proteger el funcionamiento de los equipos para que la información contenida en ellos se conservara, mantenerlos en óptimas condiciones físicas y prolongar la vida útil de la maquina dado que no se tenía el gran riesgo de los ataques por parte de piratas informáticos. No obstante, con la aparición del internet, las facilidades de acceso a la red y la necesidad de adquirir el conocimiento en informática fueron apareciendo las amenazas, los ataques por virus se incrementaron exponencialmente lo que obligo a todos los expertos en la materia el buscar métodos para proteger las redes y a las compañías el invertir sumas considerables de dinero para mantener toda la información segura.

La nueva etapa del ciberdelito como la llaman, en la que el avance de la tecnología, la utilización de equipos informáticos, dispositivos inalámbricos, la conformación del crimen organizado, inadecuados sistemas de seguridad de la información, la fácil captación de imágenes o de voz de cualquier objeto o persona, la presencia de menores de edad en el crimen virtual y de estos igualmente como víctimas del delito ha dado origen al aumento de las amenazas a través de los medios y las redes con fines criminales lo que se ha convertido en un reto para los legisladores, juristas, doctrinantes y especialistas en seguridad informática para la toma de medidas preventivas y de seguridad ante la comisión de conductas que atenten contra los bienes jurídicos protegidos.

4.1.2 La norma ISO 27001.

4.1.2.1 Aspectos Generales de la Norma ISO 27001. Esta norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización. Los requisitos establecidos en esta Norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza[11].

En la actualidad está vigente la ISO/IEC 27001 versión 2013, con un total de 14 dominios y 113 controles, además de contar con nuevos controles de seguridad.

4.1.3 Objetivos de la seguridad informática. De los principales objetivos que puede tener la seguridad informática se destacan los siguientes:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas de la seguridad.

- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de algún incidente de seguridad.

- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema[12]

Una empresa u organización puede contemplar cuatro planos de actuación que se describen claramente en la Figura 1.

[11] ICONTEC. Compendio seguridad de la información: norma técnica colombiana NTC-ISO-IEC 27001. 2 ed. Bogotá D.C.: ICONTEC, 2015. 1p.
[12] GOMEZ VIEITES, Álvaro. En: Enciclopedia de la Seguridad Informática. Alfaomega Grupo Editor, S.A. de C.V. México. 2007. p. 8.

Figura 1. Planos de actuación de la seguridad informática

Fuente: GOMEZ, Á. Enciclopedia de la Seguridad Informática. México: Alfaomega; 2007.

4.1.4 Tipos de ataques informáticos. Cuando se habla de diferentes tipos de ataques podemos diferenciar entre lo que son Ataques activos, los cuales un cambio en la información a la cual se esta accediendo o alteración de los recursos del sistema y los ataques pasivos que se limitan solo a registrar el uso de los recursos o también a acceder a la información guardada con el único fin de espiarla mas no modificarla.

Dentro de los ataques más comunes que presenta las redes y sistemas informáticos están:

Detección de vulnerabilidades del sistema: en este tipo de ataque, el atacante lo primero que hace es estudiar el sistema que desea acceder, enfocándose en detectar las vulnerabilidades que este pueda tener para posteriormente por medio de algunas herramientas ya sean desarrolladas por el mismo u obtenidas a través de internet poder explotarlas dichas herramientas son conocidas popularmente como Exploits.

Robo de información mediante interceptación de mensajes: estos ataques como su nombre lo indica tienen la finalidad de obtener información a través de la interceptación ya sea de correos electrónicos o también de archivos que se envían a través de redes privadas de usuarios y/o internet perdiéndose lo que es la confidencialidad de la información.

Modificación del contenido y secuencia de los mensajes transmitidos: aquí los intrusos del sistema tratan de reenviar mensajes o documentos que ya habían sido previamente transmitidos, tras haberlos modificados de forma maliciosa, este tipo de ataque es conocido también como “ataques de repetición” o en inglés “replay attacks”, es muy común este tipo de ataque en redes bancarias.

Análisis de tráfico de red: en este tipo de ataque el intruso realmente no está modificando absolutamente ningún dato, pero al estar analizando los paquetes o mensajes que se envían a través de la red que tiene intervenida, este puede tomar datos importantes con lo que después podría realizar un ataque como lo es por ejemplo Nombre de usuarios, contraseñas de acceso, números de cuentas entre otros[14].

Suplantación de identidad: en este tipo de ataque una de las formas mas conocidas y utilizadas por los atacantes es la denominada “IP Spoofing”, en donde los atacantes tratan de enmascarar su IP con la IP de un equipo que si está autorizado en el sistema que están atacando y alterando la cabecera de los mensajes para simular que estos proceden desde un equipo autorizado[13].

4.1.5 Tipos de intrusos en las redes.

Hackers: los hackers son intrusos que se dedican a estas tareas muchas veces como pasatiempos o como un reto, tratan de poner a prueba sus capacidades y demostrar que son capaces de burlar la seguridad de cualquier sistema, sin embargo, al acceder sin autorización a información confidencial, aunque no la alteren, la extraigan o borren esta actividad esta catalogada como un delito en muchos países[14].

Crackers: estos individuos a diferencia de los hackers buscan atacar un sistema informático con el fin de obtener beneficios de forma ilegal o por el simple hecho de provocar un daño al sistema que están atacando motivados por intereses económicos, sociales, religiosos, políticos entre otros[14].

Spammers: estos son los responsables del envío masivo de miles de mensajes de correo electrónicos no solicitados a través de redes como el internet con el fin de provocar un colapso en los servidores y una sobrecarga de los buzones de los correos de usuarios[14].

[13] GOMEZ, Á. Enciclopedia de la Seguridad Informática. México: Alfaomega; 2007.

Piratas Informáticos: estos individuos están especializados en pirateo de programas y contenidos digitales, violando el derecho de propiedad intelectual[14].

Creadores de virus y códigos maliciosos: estos son expertos en informática pero que utilizan sus conocimientos desarrollando códigos que infectan otros sistemas, alterando su funcionamiento o registrando la actividad del sistema, algunos lo hacen solo por diversión y otros con fines económicos[14].

Lamers: estos individuos también son conocidos como "script kiddies" o "click kiddies", son personas con poco conocimiento en informática pero que obtienen programas a través de internet y se documentan en cómo tratar de usarlos en algunas ocasiones pueden tener éxito y logran alterar algún sistema sin embargo se dejan detectar fácilmente debido al poco conocimiento que tienen[14].

4.2 MARCO CONCEPTUAL

4.2.1 Sistema de gestión de la seguridad informática. Se puede definir el Sistema de gestión de la seguridad informática (SGSI), como aquella parte del sistema general de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información en una organización.[14]

Es preciso contemplar toda una serie de tareas y procedimientos para poder gestionar la seguridad de la información que permitan garantizar los niveles de seguridad exigibles en una organización y hay que dejar muy claro que los riesgos nunca se eliminaran totalmente, pero si se pueden gestionar, como dijo el experto Gene Spafford, "*el único sistema verdaderamente seguro es aquel que se encuentre apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón, rodeado de gas nervioso y vigilados por guardias armados y bien pagados. Incluso entonces yo no apostaría mi vida por ella*"[15]

Cuando una organización desea establecer procesos de gestión de seguridad de la información puede seguir la metodología PHVA.

- P "Plan": selección y definición de medidas y procedimientos.

[14] Ibid. p.8.
[15] Ibid. p.19.

- H “Hacer”: implantación de medidas y procedimientos de mejora.

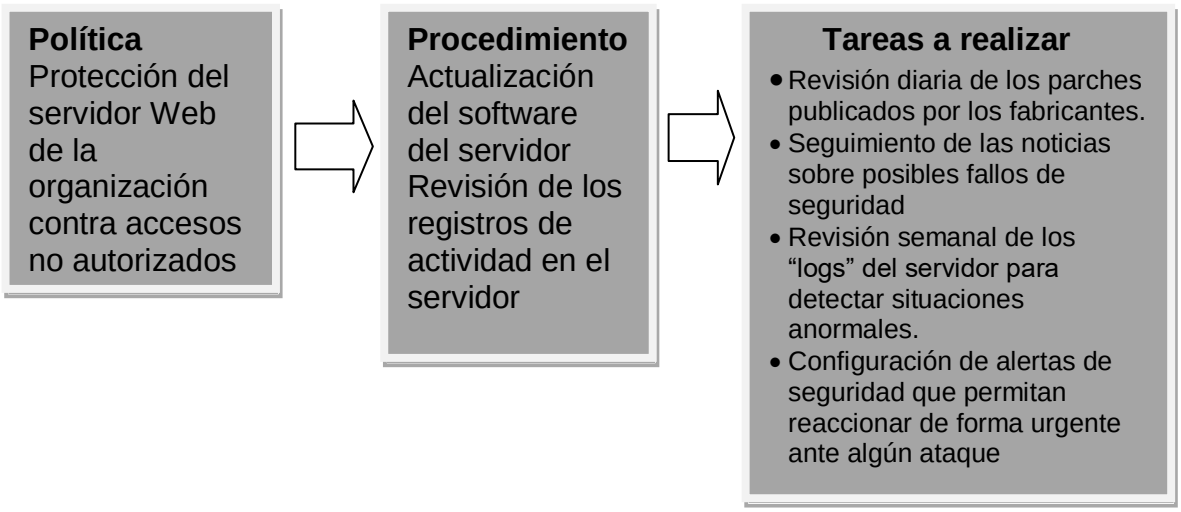
- V “Verificar”: comprobación y verificación de las medidas implantadas

- A “Actuar”: Actuación para corregir las deficiencias encontradas en el sistema.

4.2.2 Políticas de seguridad de la información. Cuando se habla de políticas de seguridad de la información se hace referencia a todo el conjunto de normas reguladoras, procedimientos, reglas y buenas prácticas que determinan el modo en que los activos y recursos, incluyendo la información, son gestionados, protegidos y distribuidos dentro de una organización.

En este sentido las políticas definen **qué** se debe proteger en el sistema, sin embargo, también debemos establecer **cómo** se debe de conseguir esta protección, para lo cual se deben establecer los **Procedimientos de seguridad** y en le definir muy bien las tareas a realizar en la Figura 2 se puede observar la relación entre Políticas, Procedimientos y Tareas a realizar.

Figura 2. Relación entre política, procedimiento y tareas a realizar



Fuente: GOMEZ, Á. Enciclopedia de la Seguridad Informática. México: Alfaomega; 2007.

4.2.3 Servicios de la seguridad informática. La seguridad informática nos brinda un gran número de servicios, pero dentro de los principales e incluso los que algunos autores los definen como pilares de la seguridad informática están:

- **Confidencialidad**: este servicio de la seguridad garantiza que cada dato almacenado o mensaje transmitido en un sistema informático solo pueda ser leído por su legítimo destinatario, si este mensaje llegara a caer en manos de terceros estos no podrían acceder al contenido del mismo.

- **Integridad**: la función de integridad se encarga de garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de la red informática.

- **Disponibilidad**: la disponibilidad del sistema es una cuestión de especial importancia, ya que si no se cumpliera con esto prácticamente se incumpliría con los objetivos del SGSI, se debe diseñar un sistema lo suficientemente robusto frente a cualquier ataque, lo cual garantice su correcto funcionamiento de manera que pueda estar a disposición de cualquier usuario que requiera de los servicios del sistema**.16**

4.2.4 Tipos de controles en seguridad informática. Cuando se habla de controles en seguridad informática se hace referencia a las acciones que se llevaran a cabo para proteger todos los activos y recursos de los sistemas informativos estos controles pueden ser de tres tipos.

Controles Físicos: se habla de controles físicos cuando se implemente alguna medida de seguridad en áreas definidas con el fin de prevenir el acceso no autorizado de personas o animales e incluso factores ambientales como polvo, tierra o agua.

- Techos, muros o paredes que delimiten el área y puertas que impidan el acceso no autorizado.

- Guardias de vigilancia.

- Cámaras de vigilancia.

[16] Ibid. 9 - 10.

- Sensores de movimiento.

Controles Tecnológicos: como su nombre lo indica estos controles usan la tecnología para poder establecer formas de autenticación de usuarios, limitaciones para acceso a la red, protección de datos confidenciales entre otros. Algunos ejemplos de estos pueden ser:

- Encriptación.

- Tarjetas inteligentes.

- Autenticación a nivel de la red.

- Software de auditoria de integridad de archivos.

Controles administrativos: estos controles hacen referencia al factor humano, este sea tal vez el factor más difícil de controlar, este involucra todos los niveles del personal dentro de la organización y determina cuáles usuarios tienen acceso y a qué recursos e información.

- Entrenamiento y conocimiento.

- Sensibilización para el uso correcto de contraseñas.

- Capacitaciones que los ayuden a no ser víctimas de ingeniería social.

- Estrategias de selección de personal, registro y contabilidad de los mismos.

4.2.5 Consecuencias de la falta de seguridad informática en las organizaciones. Anteriormente la seguridad en las organizaciones se enfocaba mas en proteger las instalaciones y personal contra robos, catástrofes naturales, incendios entre otros, la información que se manejaba prácticamente estaba en físico, pero hoy en día más del 90% de la información de una compañía se encuentra de forma digital y esto por no decir que el 100% y de ella depende el funcionamiento de una empresa.

Por estas razones es necesario trasladar a los directivos la importancia de valorar y proteger la información de sus compañías. Según un estudio realizado por la Asociación Española para la Dirección Informática (AEDI) en mayo del 2002, establecieron que el 72% de las empresas españolas quebrarían en 4 días si perdieran los datos guardados en sus ordenadores[17], por esto cuando se trata de explicar a los directivos es de vital importancia poner en conocimiento cual es el costo e impacto de los incidentes de seguridad informática en términos económicos y no en informes llenos de definiciones técnicas los cuales muy probablemente no entenderán y no pondrán la especial atención que esto requiere, de esta forma se puede hacer entender a los altos mandos de una organización que la implementación de un sistema de gestión de seguridad informática aunque pueda representar un esfuerzo económico para la compañía, no es mucho frente al beneficio que representara permitiendo que las empresas pueda continuar sus actividades aun después de una catástrofe natural o algún incidente de seguridad informática.

4.3 ANTECEDENTES

La norma ISO/IEC 27001 – ANEXO A, es la principal fuente de referencia para el desarrollo del proyecto. “Esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización”[18].

Como antecedentes de investigación se tendrá en cuenta la monografía para optar al título de Especialista en seguridad informática de SUAREZ PADILLA Sandra Yomai ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA EN LA EMPRESA ASEGURADORA SUÁREZ PADILLA & CÍA. LTDA, QUE BRINDE UNA ADECUADA PROTECCIÓN EN SEGURIDAD INFORMÁTICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN, Universidad Nacional Abierta y a Distancia. En él se concluyó que la falta de políticas, controles y normativas de seguridad pueden ocasionar consecuencias graves en el cumplimiento de los objetivos organizacionales[19].

[17] Ibid. p.14.
[18] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Compendio seguridad de la información: norma técnica colombiana NTC-ISO-IEC 27001. Bogotá: ICONTEC; 2015. p.1.
[19] SUAREZ, S. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Tesis de Especialización. Bogotá: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería; 2015.

A su vez, se tendrá en cuenta la tesis de grado para optar al título de Especialista en seguridad informática de VARON PERALTA Edwin Javier DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICABLES PARA LA EMPRESA GRUPO EMPRESARIAL ARDILA & ASOCIADOS ALINEADAS A LA NORMA ISO27001:2013, Universidad Nacional Abierta y a Distancia. En este proyecto se concluyó que una de las fuentes de amenaza más frecuente es el error humano, lo cual para el Grupo Empresarial Ardila y Asociados fue uno de sus puntos críticos, para evitar esto se configurado un dominio, control parental y permisos de usuarios, con el objetivo de resguardar la información existente en el grupo empresarial; también se crearon políticas de usuarios y de administración de la seguridad informática, y por último se crearon planes de auditorías para vigilar el cumplimiento de estas políticas con esto se busca reducir potenciales problemas al futuro y mejorar la seguridad en la entidad[20].

Igualmente, se tendrá en cuenta la tesis de grado para optar al título de Especialista en seguridad informática de PALACIOS PORTILLA Duban DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE INFORMÁTICA DE LA COOPERATIVA DEL MAGISTERIO DE TÚQUERRES BAJO LA NORMA ISO 27001:2013. Universidad Nacional Abierta y a Distancia. En este proyecto se concluyó Los servidores y la información contenida en los mismos, son los principales y más importantes activos de información que posee el área de informática, es por esto que se deben crear y mantener planes de contingencia en caso de un evento que atente contra la seguridad[21].

4.4 MARCO LEGAL

Ley 603 de 200022. Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

[20] VARON, E. Diseño de las políticas de seguridad de la información aplicables para la empresa grupo empresarial Ardila & Asociados alineadas a la norma ISO27001:2013.Tesis de Especialización. Bogotá: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería; 2015.

[21] PALACIOS, D. Diseño de un sistema de gestión de seguridad de la información (SGSI) para el área de informática de la Cooperativa del Magisterio de Túquerres bajo la norma ISO 27001:2013. Tesis de Especialización. San Juan de Pasto: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería; 2015.

[22] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 603 (27, julio, 2000). Por la cual se modifica el artículo 47 de la Ley 222 de 1995. Diario oficial. Bogotá D.C., 2000. No. 44.108. 2 p.

Ley Estatutaria 1266 del 31 de diciembre de 200823. "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 1273 del 5 de enero de 200924. "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 1341 del 30 de julio de 200925. "Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones."

Ley Estatutaria 1581 de 201226. "Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional."

[23] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley Estatutaria 1266 (31, diciembre, 2008). 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. Diario oficial. Bogotá D.C., 2008. No. 47.219. 17 p.

[24] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 (05, enero, 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. Diario oficial. Bogotá D.C., 2009. No. 47.223. 4 p.

[25] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1341 (30, julio, 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Diario oficial. Bogotá D.C., 2009. No. 47.426. 33p.

[26] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley Estatutaria 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario oficial. Bogotá D.C., 2012. No. 48.587. 13p.

5. DISEÑO METODOLOGICO

5.2.1 Unidad de análisis. Este trabajo de grado se llevó a cabo en un Centro de diagnóstico automotor (CDA). Actualmente en Colombia existen 364 CDA habilitados por el Ministerio de Transporte y acreditados por el Organismo Nacional de Acreditación-ONAC, los cuales almacenan y custodian los datos de todas las Revisiones Tecnicomecanicas y Emisiones contaminantes que se realizan diariamente en ellos.

5.2.2 Población y muestra.

5.2.2.1 Población. La población corresponde a todos los centros de diagnóstico automotor (CDA) del departamento Norte de Santander, Colombia que es el departamento en donde se llevó a cabo este proyecto, los cuales corresponden exactamente a 12 CDA y se encuentran en los siguientes municipios del departamento[27].

- 8 en el municipio de Cúcuta
- 2 en el municipio de Ocaña
- 1 en el municipio de Los Patios
- 1 en el municipio de Villa del Rosario

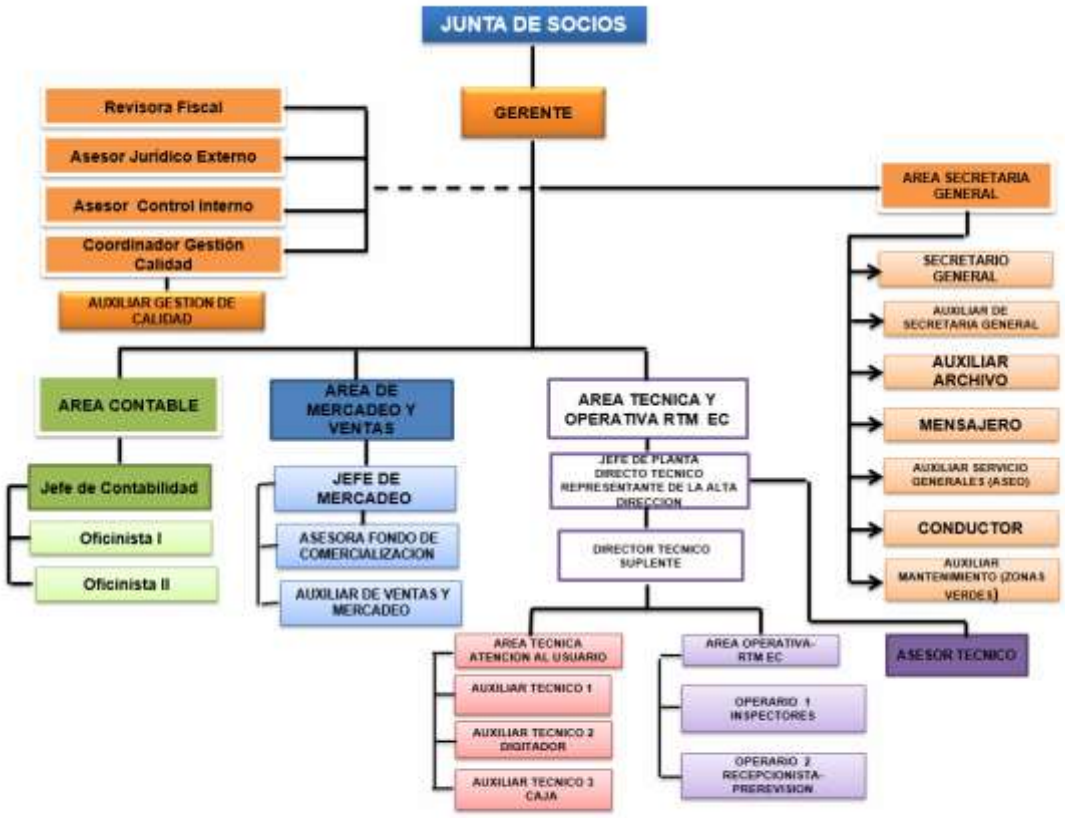
5.2.2.2 Muestra. Se tomó como muestra el Centro de Diagnóstico Automotor de Cúcuta Ltda. CEDAC y todos sus trabajadores de planta, esta es una Empresa Industrial y Comercial del Estado – EICE, de naturaleza jurídica pública, de carácter oficial, del Orden Nacional y de Responsabilidad Limitada. La sociedad gira bajo la razón social de Centro de Diagnóstico Automotor de Cúcuta Ltda. CEDAC y se ratifica como un centro de carácter oficial, una Sociedad del Orden Estatal por cuanto sus únicos socios son entidades gubernamentales. En atención a lo anterior sus socios son La Nación – Ministerio de Transporte y su capital

[27] MINISTERIO DE TRANSPORTE DE COLOMBIA. Registro Único Nacional de Tránsito - RUNT. Organismos de Tránsito. [En línea]. [Consultado 14 de mayo 2018]. Disponible en internet: (http://www.runt.com.co/directorio-de-actores?title=&field_tipo_value=3&field_c_digo_municipio_value=54001000&field_c_digo_departamento_value_1=54).

social representa el 82.25%, en segundo lugar, el Municipio de Cúcuta con un capital social que representa el 17.75%[28].

Su estructura administrativa y operativa la integran la Junta de socios, Gerente, Secretario General, Jefe de Planta, Jefe de Contabilidad, Oficinista I, Oficinista II, 4 Operarios Técnicos, Mensajero, Vigilante y Asesor Jurídico, tal como se muestra en la Figura 3

Figura 3. Organigrama Centro de Diagnóstico Automotor de Cúcuta – CEDAC Ltda.



Fuente: Secretaria Gerencia Centro de Diagnóstico Automotor de Cúcuta – CEDAC Ltda.

[28] NOTARIA PRIMERA DE CUCUTA. Escritura Pública Nº 857 (18, abril, 1980). Cúcuta, 1980. 16 p.

5.2.3 Estudio metodológico. La investigación fue de tipo descriptiva, se basó en recopilar, sistematizar y analizar la información existente acerca de la problemática de la falta de seguridad física y lógica de la información de la base de datos del Centro de Diagnóstico Automotor de Cúcuta Ltda. – CEDAC, con lo cual se buscó la recopilación de datos precisos que permitieran profundizar en esta problemática.

5.2.3.1 Fuentes de información primaria. En el proceso se recurrió al jefe de planta, jefe de contabilidad, encargado del recaudo y encargado del ingreso de datos al sistema para lograr la información necesaria; además, se buscó la información por medio de la observación directa y entrevistas no estructuradas (Ver anexo A) a los operarios técnicos.

5.2.3.2 Fuentes de información secundaria. Como fuente de información secundaria se tomaron los archivos de los sistemas de gestión de calidad, lo cual sirvieron de información.

6. ESTUDIO DE CADA UNO DE LOS CONTROLES ESTABLECIDOS POR LA NORMA ISO/IEC 27001 - ANEXO A

6.1 BREVE HISTORIA DE LA ISO 27001

La norma ISO 27001 surgió como una gran necesidad de protección de la información para mitigar los riesgos a los que está expuesta en este nuevo mundo digital y en el cual más del 90 por ciento de las transacciones se hacen a través de redes. Fue publicada por primera vez en el año 2005 por la Organización Internacional de Estandarización y por la Comisión Electrónica Internacional. Se considera como un estándar internacional, debido a que hace referencia a un compendio de requisitos que exige que los sistemas de seguridad de la información en la organización garanticen la mejora continua y la administración adecuada de la información.

Sin embargo, para poder llegar como tal a lo que es hoy en día la norma ISO 27001 hubo una serie de normas en las cuales se basaron hasta llegar a lo que fue la primera publicación de la norma en el año 2005 en la figura se puede apreciar de una forma muy practica su evolución.

Figura 4. Evolución de la Norma ISO/IEC 27001

Fuente: VILLACIS, M. Diseño de un sistema de seguridad de la información (SGSI) basado en la Norma ISO 27001:2013 para la red corporativa de la empresa Ecuatronix. Trabajo de grado. Quito Ecuador: Universidad Politécnica Salesiana Sede Quito, 2016.

6.2 ESTRUCTURA DE LA NORMA

La versión actual de la norma (NTC-ISO-IEC 27001:2013) se encuentra normalizada por el Instituto Colombiano de Normas y Técnicas y Certificación ICONTEC. Dicha norma es una adopción idéntica (IDT) por traducción de la norma ISO/IEC 27001:2013[29].

Esta norma se encuentra dividida en dos partes; la primera se compone de 10 puntos entre los que los que se encuentran los objetivos de la norma, las referencias normativas y muy importante cada uno de los componentes con los que la entidad puede formar su ciclo PHVA (Planear, Hacer, Verificar y Actuar), los cuales serán explicados más claramente en el numeral 3.3 del presente capitulo

La segunda parte de la norma está conformada por el Anexo A, el cual establece las categorías de control, los objetivos de control y los controles que se pueden implementar en una entidad con el fin de dar mayor seguridad a todo el sistema de información.

La ISO/IEC 27001 versión 2013 está vigente con un total de catorce (14) dominios y ciento trece (113) controles, además de contar con nuevos controles de seguridad, cada uno de estos controles esta enfocado a un punto en especial dentro del sistema de información de un organización por ejemplo: Recursos Humanos, Gestión de Archivos, Seguridad Física y Ambiental, Seguridad en redes entre otros, cabe aclarar que el orden en que están establecidas las categorías de control, y cada uno de los controles dentro de la Norma no tiene nada que ver con su importancia es decir cada categoría de control y controles establecidos en el Anexo A de la Norma ISO/IEC 27001 es igual de importante al control inmediatamente anterior o siguiente control.

La forma en que están estructuradas las categorías de control, los objetivos de control y los controles del Anexo A se pueden explicar con mayor facilidad basándonos en la Figura 5.

[29] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Op cit. p.95.

Figura 5. Estructura del Anexo A de la ISO/IEC 27001

A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**	
A5.1	**Orientación de la dirección para la gestión de la seguridad de la información**	
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes		
A.5.1.1	Políticas para la seguridad de la información	*Control* Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información.	*Control* Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.

Fuente: Norma ISO27001:2013 - ANEXO A

Cada una de las categorías de control de las que se conforma el Anexo A de la ISO27001:2013 están identificadas desde la A5 hasta la A18 en la figura 4 claramente podemos ver la primera categoría de control que es la A5 y lleva por título “POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION”

El objetivo de control se encuentra bajo la categoría de control y se identifica siguiendo la nomenclatura de la categoría segunda por un Punto y el número del objetivo de control de esta Categoría, en la Figura 4 se observa el objetivo de control A5.1, es decir que es el primer control de la categoría A5.

Por último tenemos los controles que la norma ISO27001:2013 establece para cada objetivo de control, estos continúan llevando la misma nomenclatura es decir primero hace referencia a la categoría de control seguido por un punto y el numero del objetivo de control seguido por un ultimo punto y el numero que corresponde al control del objetivo, en este orden de ideas en la Figura 4 podemos observar el control A.5.1.1 lo cual nos indica que es el primer control del primer objetivo de control de la categoría A5 y el control A.5.1.2 que hace referencia al segundo control del primer objetivo de la Categoría A5.

De esta forma se pudo comprender mucho mejor a que se refiere la Norma ISO27001:2013 en su Anexo A cuando habla de Categorías de control, objetivos de control y controles.

6.3 CICLO PHVA VS LA NORMA ISO/IEC 27001:2013

El ciclo PHVA (Planear, Hacer, Verificar y Actuar) es muy importante dentro de una organización ya que es un ciclo diseñado con el fin de tener una mejora continua en todos los procesos que lleva a cabo la entidad, la norma ISO 27001 nos da unas pautas que podemos ajustar perfectamente a este ciclo como se describe a continuación.

6.3.1 Planear. Es aquí donde la organización debe establecer sus objetivos, alcances y definir claramente los responsables dentro del sistema de gestión de seguridad de la información, la norma ISO 27001:2013 nos establece 3 puntos que se adaptan al Planear del ciclo PHVA, en la cuadro 1 se puede comprender con mayor facilidad lo que correspondería al planear según lo que nos plantea la Norma.

Cuadro 1. Planear - ciclo PHVA VS la norma ISO/IEC 27001:2013

Ciclo PHVA	ISO/IEC 27001:2013	Que es lo que se busca o se quiere establecer
PLANEAR	**CONTEXTO DE LA ORGANIZACIÓN** • Conocimiento de la organización y de su contexto • Comprensión de las necesidades y expectativas de las partes interesadas • Determinación del alcance del sistema de gestión • De la seguridad de la información • Sistema de gestión de la seguridad de la información	Busca determinar las necesidades y expectativas dentro y fuera de la organización que afecten directa o indirectamente al sistema de gestión de la seguridad de la información. Adicional a esto, busca determinar el alcance
	LIDERAZGO • Liderazgo y compromiso • Política • Roles, responsabilidades y autoridades en la organización	Habla sobre la importancia de la alta dirección y su compromiso con el sistema de gestión, estableciendo políticas, asegurando la integración de los requisitos del sistema de seguridad en los procesos de la organización, así como los recursos necesarios para su implementación y operabilidad.

Cuadro 1. (Continuación)

	PLANIFICACIÓN • Acciones para tratar riesgos y oportunidades. • Objetivos de seguridad de la información y planes para lograrlos.	Persigue valorar, analizar y evaluar los riesgos de seguridad de acuerdo a los criterios de aceptación de riesgos, adicional mente se debe dar un tratamiento a los riesgos de la seguridad de la información. Los objetivos y los planes para logar dichos objetivos también se deben definir en este punto

Fuente: El autor

6.3.2 Hacer. En esta etapa del ciclo PHVA se debe de empezar a establecer procedimientos y actividades de cómo se va a desarrollar todo lo que se ha planeado en la etapa anterior en la cuadro 2 se expone lo que nos plantea la Norma ISO 27001:2013 en el Hacer del Ciclo PHVA

Cuadro 2. Hacer - ciclo PHVA vs la norma ISO/IEC 27001:2013

Ciclo PHVA	ISO/IEC 27001:2013	Que es lo que se busca o se quiere establecer
HACER	**SOPORTE** • Recursos • Competencia • Toma de conciencia • Comunicación • Información documentada	Se establecen los recursos destinados por la organización, la competencia de personal, la toma de conciencia por parte de todas las partes interesadas, la importancia sobre la comunicación asertiva en la organización, todo dentro del sistema de gestión debe de estar debidamente documentado y poseer su registro
	OPERACIÓN • Planificación y control operacional • Valoración de riesgos de la seguridad de la información • Tratamiento de riesgos de la seguridad de la información	Aquí la organización debe de implementar y controlar los procesos que hagan parte del sistema de gestión de seguridad de la información, valorar los riesgos

Fuente: El autor

6.3.3 Verificar. En esta etapa del ciclo es donde se debe estar constantemente evaluando todos los objetivos, políticas y procedimientos con el fin de determinar que el sistema esta cumplimento con su finalidad o si es necesario mejorar o modificar alguna política o procedimiento en pro de una mejora continua

Cuadro 3. Verificar - ciclo PHVA vs la norma ISO/IEC 27001:2013

Ciclo PHVA	ISO/IEC 27001:2013	Que es lo que se busca o que se quiere establecer
VERIFICAR	**EVALUACIÓN DEL DESEMPEÑO** • Seguimiento, medición, análisis y evaluación • Auditoría interna • Revisión por la dirección	Se debe realizar un seguimiento, medición, análisis y evaluación del sistema de gestión de la información.

Fuente: El autor

6.3.4 Actuar. En esta etapa del ciclo damos tratamiento a las no conformidades que se puedan presentar en el sistema de gestión de seguridad de la información y a la vez se evalúa porque la organización se desvió del cumplimiento de sus políticas para que no se vuelva a incurrir en estos errores, incluso estableciendo nuevas políticas o procedimientos que ayuden a mejorar el sistema.

Cuadro 4. Actuar - ciclo PHVA vs la norma ISO/IEC 27001:2013

Ciclo PHVA	ISO/IEC 27001:2013	Que es lo que se busca o que se quiere establecer
ACTUAR	**MEJORA** • No conformidades y acciones correctivas • Mejora continua	tratamiento de las no conformidades, las acciones correctivas y a mejora continua que la entidad debe realizar con el fin de buscar siempre un sistema de gestión de seguridad de la información más sólido

Fuente: El autor

7. CONTROLES DEL ANEXO A, APLICABLES AL CENTRO DE DIAGNOSTICO AUTOMOTOR - CEDAC LTDA., UBICADO EN LA ZONA INDUSTRIAL DE LA CIUDAD DE CÚCUTA

7.1 ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACION EN EL CEDAC-LTDA

Con el apoyo del personal de planta del Centro de Diagnóstico Automotor de Cúcuta – CEDAC Ltda., mediante la observación directa, entrevistas no estructuradas y aplicación de encuesta al Gerente de la entidad, Secretario General, Jefe de Planta, Jefe de Contabilidad, Encargado del Recaudo, Encargado de Archivo, Encargado del Ingreso de datos al sistema y Operarios Técnicos se llevó a cabo la evaluación del estado, el conocimiento y responsabilidad que tiene el personal sobre un tema tan importante como lo es la seguridad de la información de la entidad, arrojando los siguientes resultados que se observan en la cuadro 5:

Cuadro 5. Verificación de cumplimiento requisitos básicos, conocimiento y responsabilidad para la seguridad de la información

REQUISITOS BASICOS PARA LA SEGURIDAD DE LA INFORMACIÓN – CEDAC LTDA.	SI CUMPLE	NO CUMPLE
El CEDAC LTDA., cuenta con Comité de Seguridad de la Información.		X
El CEDAC LTDA., cuenta con personal técnico y/o profesional especializado para la seguridad de la información.		X
El CEDAC LTDA., cuenta con la integración de otros sistemas de gestión.	X	
El CEDAC LTDA., cuenta con apoyo y participación de control interno.	X	
Los trabajadores oficiales o personal de planta del CEDAC LTDA., conocen las responsabilidades respecto a la seguridad de la información de la entidad oficial.		X
Los contratistas del CEDAC LTDA., conocen las responsabilidades respecto a la seguridad de la información de la entidad oficial.		X
Los proveedores del CEDAC LTDA., conocen las responsabilidades respecto a la seguridad de la información de la entidad oficial.		X

Fuente: el autor

El Centro de Diagnóstico Automotor de Cúcuta – CEDAC Ltda., cuenta con un gran número de activos como lo son sistemas operativos, procedimientos, documentación entre los que se encuentran: equipos de cómputo, servidores, impresoras, toda una red LAN, paquete de software como TNS para la contabilidad, software de Revisión Tecnicomecánica - SOLTELEC y sistemas operativos Windows para los equipos de cómputo.

Sin embargo, estos activos carecen de controles de seguridad que mitiguen los riesgos de pérdidas, alteración o robo de la información e incluso controles en la red que impidan el ataque de intrusos desde fuera de la entidad.

Al Centro de Diagnóstico Automotor - CEDAC Ltda., son aplicables todos los controles establecidos por la norma ISO/IEC 27001 - ANEXO A; excepto: 1. El objetivo de control A.6.2., con sus dos respectivos controles (A.6.2.1. – A.6.2.2.), los cuales hacen referencia a dispositivos móviles y teletrabajo; dado que, la entidad efectúa el cumplimiento de su objeto misional con inspección, control y vigilancia en tiempo real. 2. La categoría de control A14 en su totalidad que hace referencia al desarrollo, mantenimiento y soporte de software; dado que, el objeto misional de la entidad es la Revisión Tecnicomecanica y de Emisiones Contaminantes, mas no el desarrollo mantenimiento y soporte de software.

7.2 DECLARACIÓN DE APLICABILIDAD (DDA) PARA SEGURIDAD DE LA INFORMACIÓN

A continuación, en la cuadro 6 se muestran las Categorías de control, los objetivos de control y controles establecidos por la norma ISO/IEC 27001 - ANEXO A que le son aplicables al Centro de Diagnóstico Automotor - CEDAC Ltda. Para mayor claridad y entendimiento en la cuadro 2 se muestra una columna APLICA en la cual se establece si el control aplica o no a la entidad y una columna CUMPLE en donde se especifica si la empresa está cumpliendo o no con este control, por último, hay una columna EVIDENCIA en donde se explica por la empresa no está cumpliendo con un determinado control o porque si está cumpliendo en caso de que lo esté haciendo

Cuadro 6. Declaración de aplicabilidad (DDA) para seguridad de la información

A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**						
A5.1	Orientación de la dirección para la gestión de la seguridad de la información		APLICA		CUMPLE		EVIDENCIA
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes			SI	NO	SI	NO	
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	X			X	-Al contar con un grupo de activos informáticos e información sensible la entidad debe de tener unos controles que mitiguen el riego de daño, perdida o alteración de los mismos, sin embargo no hay escrita ninguna política ni procedimiento para este fin
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	X			X	-No hay escrita ninguna política ni procedimiento para este fin
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**						
A6.1	Organización interna		APLICA		CUMPLE		EVIDENCIA
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.			SI	NO	SI	NO	
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	X			X	-No hay asignada responsabilidades de los activos de información

Cuadro 6. (Continuación)

A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	X			X	-Al no haber definidas responsabilidades, tampoco se han separado deberes y las áreas no poseen letreros de acceso restringido o solo personal autorizado
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	X			X	-Se mantiene contacto con la autoridad ambiental del departamento, sin embargo, no hay establecidas unas políticas en donde se especifique la confidencialidad de los datos que se manejan
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	X			X	-No se tiene contacto, con ningún grupo o especialistas en seguridad
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	X			X	-No se ha tenido en cuenta hasta el momento la seguridad de la información, ya que incluso no hay ninguna política de seguridad establecida
A6.2	Dispositivos móviles y teletrabajo		APLICA		CUMPLE		EVIDENCIA
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles			SI	NO	SI	NO	
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.		X			No hay lugar para el teletrabajo en el CEDAC, ya que todo su objeto misional se debe de realizar bajo el monitoreo de las cámaras del Sistema

Cuadro 6. (Continuación)

A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.		X			de control y vigilancia (SICOV), en tiempo real
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		APLICA		CUMPLE		EVIDENCIA
A7.1	Antes de asumir el empleo						
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.			SI	NO	SI	NO	
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	X			X	-Al ser una entidad del estado se deben de verificar todos los antecedentes del personal que se va a contratar, sin embargo, aunque esto se realiza no queda registrado en ninguna parte, ni tampoco hay establecidos procedimientos y responsables de esta tarea
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	X			X	-En cada contrato deben quedar establecidas las responsabilidades de los empleados mas no se esta realizando nada de esto ya que no hay políticas de seguridad que así lo establezcan

Cuadro 6. (Continuación)

A7.2	Durante la ejecución del empleo		APLICA		CUMPLE		EVIDENCIA
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.			SI	NO	SI	NO	
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	X			X	-No se han establecido responsabilidades de ningún tipo con respecto a los activos informáticos.
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	X			X	-Nunca se ha sensibilizado al personal en cuanto a la importancia de la seguridad informática, no existe registro alguno
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	X			X	-No hay establecido procesos disciplinarios para alguna falla en la seguridad de la información, no se ha tenido en cuenta ya que ni siquiera se han establecido políticas de seguridad de la información.

Cuadro 6. (Continuación)

A7.3	Terminación y cambio de empleo		APLICA		CUMPLE		EVIDENCIA
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo			SI	NO	SI	NO	
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	X			X	-No se han establecido responsabilidades en cuanto a seguridad de la información.
A8	**GESTION DE ACTIVOS**						
A8.1	Responsabilidad por los activos		APLICA		CUMPLE		EVIDENCIA
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas**.**			SI	NO	SI	NO	
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	X			X	-No se tiene inventario de activos informáticos, ni siquiera un inventario actualizado de todos los activos de la entidad
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	X			X	-No se tiene definido propietario ni responsable
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	X			X	-No hay definido políticas de uso de los activos, por lo que los usuarios no saben lo que es un buen trato de los equipos

Cuadro 6. (Continuación)

A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	X			X	-No se hace verificación de estado de los activos cuando un empleado abandona el cargo y si hay problemas con el mismo el nuevo empleado es el que lo hace evidente
A8.2	Clasificación de la información		APLICA		CUMPLE		EVIDENCIA
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.			SI	NO	SI	NO	
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	X			X	-Solo se tiene clasificada la información de calidad, referente a los procesos de revisión tecnicomecanica, mas no
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X			X	-Al no estar clasificada no se tiene toda la información etiquetada, como se expreso en el control inmediatamente anterior solo alguna información esta clasificada como confidencial.
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X			X	-No se tienen procesos de manejos de activos información según su clasificación ya que tampoco se tienen clasificados los mismos

Cuadro 6. (Continuación)

A8.3	Manejo de medios		APLICA		CUMPLE		EVIDENCIA
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios			SI	NO	SI	NO	
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	X			X	-No hay políticas para establecer la limitación de uso de medios móviles o removibles
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	X			X	-No se tienen establecidas responsabilidades del uso y disposición de los medios removibles que pertenezcan a la entidad o que contenga información sensible de la misma
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	X			X	-Cuando se envían datos a las autoridades de vigilancia, estos no son protegidos de ninguna forma, lo cual permite que puedan ser alterados o robados
A9	**CONTROL DE ACCESO**						
A9.1	Requisitos del negocio para el control de acceso		APLICA		CUMPLE		EVIDENCIA
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.			SI	NO	SI	NO	
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	X			X	-No se tienen establecidas ningún tipo de políticas en la entidad referente a limitar el acceso de usuarios a información sensible
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	X			X	-No existe control de acceso a la red y los usuarios muchas veces suministran las claves de red a cualquier persona

Cuadro 6. (Continuación)

A9.2	Gestión de acceso de usuarios		APLICA		CUMPLE		EVIDENCIA
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.			SI	NO	SI	NO	
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	X			X	-No se tiene implementado un sistema donde se autoricen o se cancelen usuarios en el sistema
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	X			X	-No se tiene implementado ningún proceso o sistema para el suministro de acceso a usuarios con sus respectivos privilegios
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	X			X	-No se tiene implementado ningún proceso o sistema para el suministro de acceso a usuarios con sus respectivos privilegios
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	X			X	-No se tiene implementado ningún proceso o sistema para el suministro de acceso a usuarios con sus respectivos privilegios
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	X			X	-No se tiene implementado ningún proceso o sistema para el suministro de acceso a usuarios con sus respectivos privilegios

Cuadro 6. (Continuación)

A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.					-No se tiene implementado ningún proceso o sistema para el suministro de acceso a usuarios con sus respectivos privilegios
A9.3	Responsabilidades de los usuarios		APLICA		CUMPLE		EVIDENCIA
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.			SI	NO	SI	NO	
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	X			X	-No se ha capacitado ni sensibilizado a los empleados sobre el buen uso de autenticaciones y claves
A9.4	Control de acceso a sistemas y aplicaciones		APLICA		CUMPLE		EVIDENCIA
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.			SI	NO	SI	NO	
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	X			X	-No hay ninguna política de acceso creada en la entidad
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	X			X	-No hay ninguna política de acceso creada en la entidad
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	X			X	-No existe ningún sistema de gestión de contraseñas, ni políticas para el uso de las mismas

Cuadro 6. (Continuación)

A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	X			X	-No existen políticas para la restricción y uso de programas no autorizados, ni tampoco usuarios limitados para impedir la instalación de programas sin permiso de administradores
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	X			X	-No existen políticas para restringir el acceso a carpetas de los programas instalados
A10	**CRIPTOGRAFIA**		APLICA		CUMPLE		EVIDENCIA
A10.1	Controles criptográficos						
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información			SI	NO	SI	NO	
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	X			X	-No existen políticas para controles criptográficos, ni tampoco existe ningún hardware criptográfico para acceso a la información de la entidad.
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	X			X	- No existen políticas para controles criptográficos, ni tampoco existe ningún hardware criptográfico para acceso a la información de la entidad.
A11	**SEGURIDAD FISICA Y DEL ENTORNO**		APLICA		CUMPLE		EVIDENCIA
A11.1	Áreas seguras						
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			SI	NO	SI	NO	
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	X			X	-Si se tienen definidas las áreas, sin embargo, en algunas se puede acceder sin necesidad de llaves es decir permanecen sin candado

Cuadro 6. (Continuación)

A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	X			X	-Las áreas no permanecen bajo llave y no poseen letrero que indiquen que solo se permite el acceso a personal autorizado
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	X			X	-Están definidas las áreas, pero estas no permanecen bajo llave, solo la gerencia permanece con llave
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	X			X	-Algunas oficinas poseen goteras y no hay ningún sistema para detección de humo en caso de incendio
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	X			X	-No se encuentra establecido ningún procedimiento y la empresa tampoco cuenta con un sistema de seguridad y salud en el trabajo
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	X			X	-No existen letreros que indique prohibido el acceso a personal no autorizado, ni tampoco formas de prohibir el ingreso

Cuadro 6. (Continuación)

A11.2	Equipos		APLICA		CUMPLE		EVIDENCIA
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			SI	NO	SI	NO	
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	X			X	-Los equipos no poseen protección como forros para protegerlos de amenazas del entorno
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	X			X	-hacen falta UPS para impedir que los equipos no sufran en caso de fallas de energía
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	X			X	-La empresa cuenta con una planta eléctrica no obstante nunca se prende por lo tanto habría que verificar con técnicos especializados, si esta aun funciona
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	X			X	-Algunas veces se les realiza mantenimiento a los equipo sin embargo no hay un cronograma ni un procedimiento establecido
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	X			X	-Muchos equipos son movidos de lugar y al no haber establecidas unas responsabilidades pues lo hacen sin solicitar permisos a nadie

Cuadro 6. (Continuación)

A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	X			X	-Cuando se envían equipos para reparación no se realizan actas de salida del mismo, no hay establecido un procedimiento adecuado para esta labor
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso.	X			X	-no hay procedimientos establecidos para saber que hacer con los equipos que salen de uso y que tratamiento se le dará a la información en el contenida
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	X			X	-No existen capacitaciones a los empleados para enseñarles cómo proteger sus equipos y la información en ellos contenida
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	X			X	-No existen capacitaciones a los empleados para enseñarles cómo proteger sus equipos y dejar bien archivados las información que estén manejando en físico

Cuadro 6. (Continuación)

A12	SEGURIDAD DE LAS OPERACIONES		APLICA		CUMPLE		EVIDENCIA
A12.1	Procedimientos operacionales y responsabilidades						
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.			SI	NO	SI	NO	
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	X			X	-No hay ni políticas no procedimientos establecidos de seguridad informática en la entidad
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	X			X	-Aunque la entidad ha ido creciendo aun no se han establecidos procedimientos ni políticas de seguridad informática.
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	X			X	-No se realiza ningún tipo de seguimiento ni tampoco hay registros que así lo indiquen
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.		X			-La entidad no desarrolla software por tanto no hay un ambiente de pruebas ni desarrollo

Cuadro 6. (Continuación)

A12.2	**Protección contra códigos maliciosos**		APLICA		CUMPLE		EVIDENCIA
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.			SI	NO	SI	NO	
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	X			X	-No procedimientos establecidos para la recuperación de los datos, ni sensibilización a los empleados para no ser víctimas de ataques por códigos maliciosos enviados por correos o descargados de internet
A12.3	Copias de respaldo		APLICA		CUMPLE		EVIDENCIA
Objetivo: Proteger contra la perdida de datos			SI	NO	SI	NO	
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	X			X	-Solamente se hacen copias de respaldo de la información de las revisiones tecnicomecanicas y la contabilidad de la entidad, sin embargo estas no se pruebas regularmente para confirmar la fiabilidad, integridad y disponibilidad de los datos
A12.4	**Registro y seguimiento**		APLICA		CUMPLE		EVIDENCIA
Objetivo: Registrar eventos y generar evidencia			SI	NO	SI	NO	
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	X			X	-No se llevan ningún tipo de registros de incidentes de seguridad de la información.
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	X			X	-No existen sistemas de prevención de acceso no autorizado que ayude a registrar las actividades en el sistema

Cuadro 6. (Continuación)

A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	X			X	-No existen sistemas de prevención de acceso no autorizado que ayude a registrar las actividades en el sistema
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	X			X	-No existen sistemas de prevención de acceso no autorizado que ayude a registrar las actividades en el sistema
A12.5	**Control de software operacional**		APLICA		CUMPLE		EVIDENCIA
Objetivo: Asegurarse de la integridad de los sistemas operacionales			SI	NO	SI	NO	
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	X			X	-No existen restricciones para la instalación de software sin autorización como por ejemplo usuarios con cuentas limitadas
A12.6	**Gestión de la vulnerabilidad técnica**		APLICA		CUMPLE		EVIDENCIA
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas			SI	NO	SI	NO	
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	X			X	-No existe registro de realización de una matriz de riesgos para detectar vulnerabilidades del sistema que ayuden a implementar controles y procedimientos para mitigarlas

Cuadro 6. (Continuación)

A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	X			X	-No existen restricciones para la instalación de software sin autorización como por ejemplo usuarios con cuentas limitadas
A12.7	**Consideraciones sobre auditorias de sistemas de información**		APLICA		CUMPLE		EVIDENCIA
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos			SI	NO	SI	NO	
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	X			X	-No existen controles ni registros de auditorías en la entidad
A13	**SEGURIDAD DE LAS COMUNICACIONES**						
A13.1	Gestión de la seguridad de las redes		APLICA		CUMPLE		EVIDENCIA
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.			SI	NO	SI	NO	
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	X			X	-No hay políticas de protección de redes, los usuarios muchas veces comparten la clave de acceso a la red con cualquier amigo que llegue a verlo a la entidad
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	X			X	No hay políticas de protección de redes establecidos en la entidad y muchas veces los servicios de red son usados para cosas ajenas a la actividad del usuario en la empresa

Cuadro 6. (Continuación)

A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	X			X	-Todos los servicios y aplicaciones que maneja la entidad están a través de la misma red
A13.2	**Transferencia de información**		APLICA		CUMPLE		EVIDENCIA
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			SI	NO	SI	NO	
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	X			X	-No existen políticas de seguridad ni procedimientos en la entidad para la transferencia de información que mitigue el riesgo de pérdida, robo o alteración.
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	X			X	-No existen acuerdos entre entidades externas como la entidad ambiental para la transferencia segura de la información.
A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	X			X	-Varias personas de la entidad tienen acceso al correo de la misma y jno se lleva un contro, de que es lo que hace cada una de estas personas.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	X			X	-No existen firmados acuerdos de confidencialidad y no divulgación entre empleados y la entidad o entre proveedores y la entidad que reflejen la importancia y problemas legales que esto puede acarrear.

Cuadro 6. (Continuación)

A14	**Adquisición, desarrollo y mantenimiento de sistemas**		APLICA		CUMPLE		EVIDENCIA
A14.1	Requisitos de seguridad de los sistemas de información						
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.			SI	NO	SI	NO	
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.		X			-La entidad no desarrolla software por lo cual no le aplican estos controles.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.		X			-La entidad no posee aplicaciones que pasen sobre redes públicas o servidores que puedan ser accedidos públicamente
A14.2	Seguridad en los procesos de Desarrollo y de Soporte		APLICA		CUMPLE		EVIDENCIA
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			SI	NO	SI	NO	
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.		X			-La entidad no desarrolla software por lo cual no le aplican estos controles.

Cuadro 6. (Continuación)

A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.		X			La entidad no desarrolla software por lo cual no le aplican estos controles.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.		X			La entidad no desarrolla software por lo cual no le aplican estos controles.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.		X			La entidad no desarrolla software por lo cual no le aplican estos controles.
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.		X			La entidad no desarrolla software por lo cual no le aplican estos controles.

Cuadro 6. (Continuación)

A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.		X			La entidad no desarrolla software por lo cual no le aplican estos controles.
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.					La entidad no desarrolla software por lo cual no le aplican estos controles.
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.					La entidad no desarrolla software por lo cual no le aplican estos controles.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.					La entidad no desarrolla software por lo cual no le aplican estos controles.
A14.3	Datos de prueba		APLICA		CUMPLE		EVIDENCIA
Objetivo: Asegurar la protección de los datos usados para pruebas.			SI	NO	SI	NO	
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.		X			La entidad no desarrolla software por lo cual no le aplican estos controles.

Cuadro 6. (Continuación)

A15	**RELACIONES CON LOS PROVEEDORES**		APLICA		CUMPLE		EVIDENCIA
A15.1	Seguridad de la información en las relaciones con los proveedores.						
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.			SI	NO	SI	NO	
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	X			X	-No existen acuerdos en los contratos con proveedores donde se establezcan este tipo de políticas de seguridad.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	X			X	No existen acuerdos en los contratos con proveedores donde se establezcan este tipo de políticas de seguridad.
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	X			X	-No existen acuerdos en los contratos con proveedores donde se establezcan este tipo de políticas de seguridad.

Cuadro 6. (Continuación)

A15.2	**Gestión de la prestación de servicios de proveedores**		APLICA		CUMPLE		EVIDENCIA
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores			SI	NO	SI	NO	
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	X			X	-No existen acuerdos en los contratos con proveedores donde se establezcan este tipo de políticas de seguridad.
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la reevaluación de los riesgos.	X			X	-No existen acuerdos en los contratos con proveedores donde se establezcan este tipo de políticas de seguridad.
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**						
A16.1	Gestión de incidentes y mejoras en la seguridad de la información		APLICA		CUMPLE		EVIDENCIA
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.			SI	NO	SI	NO	
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	X			X	-No se han definido ni políticas no responsabilidades dentro de la entidad.

Cuadro 6. (Continuación)

A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	X			X	-No se han establecido procedimientos ni existen registros sobre incidentes de seguridad informática aunque puedan haber ocurrido
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	X			X	-No se han capacitado a los empleados para esta labor, para que puedan entender que es una debilidad en el sistema.
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	X			X	-No existen una matriz para la clasificación de los eventos de seguridad de la información.
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	X			X	-No existen procedimientos establecidos y mucho menos documentados para tal fin
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	X			X	-No hay documentado ningún incidente de seguridad para poder estudiarlo y establecer controles que impidan que vuelva a suceder

Cuadro 6. (Continuación)

A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	X			X	-No existen datos de evidencias ya que nunca se ha reportado un incidente aunque estos si puedan haber ocurrido
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**		APLICA		CUMPLE		EVIDENCIA
A17.1	Continuidad de Seguridad de la información						
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.			SI	NO	SI	NO	
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	X			X	-No hay establecidos procedimientos en caso de desastres como garantizar la continuidad del negocio.
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	X			X	-No hay establecidos procedimientos en caso de desastres como garantizar la continuidad del negocio.

Cuadro 6. (Continuación)

A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	X			X	-No hay establecidos procedimientos en caso de desastres como garantizar la continuidad del negocio.
A17.2	**Redundancias**		APLICA		CUMPLE		EVIDENCIA
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.			SI	NO	SI	NO	
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	X			X	-No existe redundancia en los datos que garantice la disponibilidad en caso de daño del sistema en que se encuentra almacenado
A18	**CUMPLIMIENTO**						
A18.1	Cumplimiento de requisitos legales y contractuales		APLICA		CUMPLE		EVIDENCIA
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.			SI	NO	SI	NO	
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	X			X	-Al no haber un sistema de gestión de seguridad de la información establecido, no existen registros ni documentación alguna sobre este tema

Cuadro 6. (Continuación)

A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	X			X	-Se tienen licencias de software utilizados por la entidad pero no se lleva un registro que ayude a mostrar ante una autoridad que se cumple con la adquisición legal de los mismos.
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	X			X	-Se tienen licencias de software utilizados por la entidad pero no se lleva un registro que ayude a mostrar ante una autoridad que se cumple con la adquisición legal de los mismos
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige la legislación y la reglamentación pertinentes, cuando sea aplicable.	X		X		-Se tienen establecidas unas políticas de protección de datos de los clientes y claramente sensibilizado al personal que los datos no pueden ser divulgados sin autorización de los o según lo establecido en el artículo 10 de la ley 1581 de 2012
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	X			X	No hay evidencias de la utilización de controles criptográficos.

Cuadro 6. (Continuación)

A18.2	Revisiones de seguridad de la información		APLICA		CUMPLE		EVIDENCIA
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.			SI	NO	SI	NO	
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	X			X	-Primero se deben establecer las políticas e implementar todos los controles que sean aplicables para poder llevar un seguimiento de todos estos mediante los registros y documentación que se establezca.
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	X			X	-Primero se deben establecer las políticas e implementar todos los controles que sean aplicables para poder llevar un seguimiento de todos estos mediante los registros y documentación que se establezca
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	X			X	-Primero se deben establecer las políticas e implementar todos los controles que sean aplicables para poder llevar un seguimiento de todos estos mediante los registros y documentación que se establezca

Fuente: Norma ISO27001:2013 - ANEXO A

8. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN, BASADOS EN EL ANEXO A DE LA NORMA ISO/IEC 27001

En este capítulo se desarrolló una de los objetivos más importantes del proyecto como lo es proponer a la entidad unas políticas de seguridad de la información basada en los controles establecidos por la Norma ISO/IEC 27001:2013, para tal fin se tomaron todas las categorías de control con sus respectivos objetivos de control como los establece la Norma en su Anexo A y que le son aplicables a la empresa, para cada uno de ellos se definió su aplicabilidad y se redactaron unas directrices que el CEDAC puede implementar con el fin de mitigar los riesgos en sus activos y sistemas de información.

Es importante primero describir la empresa objeto de estudio, es decir; el CENTRO DE DIAGNOSTICO AUTOMOTOR DE CUCUTA LIMITADA - CEDAC, dado que es para ella que se están proponiendo las políticas de seguridad.

8.1 IDENTIFICACION DE LA EMPRESA

8.1.1 Nombre. Centro de Diagnóstico Automotor de Cúcuta Limitada– CEDAC.

8.1.2 Misión. Contribuir y fomentar la cultura en seguridad vial, movilidad y conservación del medio ambiente a través del diagnóstico al estado de los vehículos, así como el desarrollo de programas de formación e integración de servicios relacionados con el sector de tránsito y transporte[30].

8.1.3 Visión. El Centro de Diagnóstico Automotor de Cúcuta – CEDAC Ltda., para el 2016 mantendrá su posición de liderazgo orientado a desarrollar las políticas, planes y programas de los Ministerios de Transporte y Ambiente, Vivienda y Desarrollo Territorial en la ciudad de Cúcuta y el Departamento Norte de Santander[31].

8.2 POLITICAS ADMINISTRATIVAS

8.2.1 Política de calidad. El Centro de Diagnóstico Automotor de Cúcuta – CEDAC Ltda., está comprometido en contribuir a la preservación del medio ambiente y al mejoramiento de la seguridad vial, a través de la prestación del

[30] CENTRO DE DIAGNÓSTICO AUTOMOTOR DE CÚCUTA LTDA. Op cit. p.5.
[31] Ibid.p.6.

servicio de Revisión Tecnicomecanica y análisis de gases en fuentes móviles terrestres, mediante la utilización de personal altamente calificado y los equipos necesarios para asegurar la calidad del servicio, mediante la satisfacción a nuestros usuarios, la oportunidad, pertinencia y amabilidad en la prestación de nuestros servicios y suministros de información, el mejoramiento continuo en todos sus procesos, el cumplimiento de los términos legales y la cualificación, capacitación y seguridad del personal[32].

8.3 DESARROLLO DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACION APLICABLES AL CEDAC

Como se explicó al principio del presente capitulo se tomó cada categoría de control con sus respectivos objetivos de control y para cada uno de ellos se definió su aplicabilidad y se establecieron unas políticas de seguridad e la información y las cuales se presentan a continuación

8.3.1 A.5 Políticas de seguridad de la información.

5.3.1.1 A.5.1 Política para la Orientación de la Dirección para la Gestión de la Seguridad de la Información. Objetivo. Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

Aplicabilidad:

Estas políticas aplican a la Alta gerencia, empleados de planta, contratistas, proveedores y demás funcionarios que interfieran en el proceso de gestión de seguridad de la información de la entidad.

Directrices:

- Establecer los objetivos y alcance de cada una de las políticas de seguridad que se establezcan en la entidad

- la Gerencia debe de establecer claramente las responsabilidades de cada persona dentro del sistema de gestión de seguridad de la información.

[32] Ibid.p.7.

- Desarrollar procesos para llevar a cabo el cumplimiento de las políticas de seguridad.

- La gerencia debe de garantizar la divulgación y correcta comunicación de las políticas de seguridad

- Cada responsable debe de informar si existe alguna forma de mejoramiento de las políticas o si es necesario modificarlas con el objetivo de buscar una mejora continua.

- La gerencia debe gestionar la capacitación del personal de la entidad en la importancia, seguimiento de las políticas de seguridad, manejo e identificación de incidentes de seguridad

- Cada persona dentro del proceso es responsable del cumplimiento de las políticas de seguridad de la información.

8.3.2 A.6 Política de organización de la seguridad de la información.

8.3.2.1 A.6.1 Política para la organización interna. Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del Sistema de gestión de seguridad de la información

Aplicabilidad:

Esta política aplica a la Gerencia, personal de recursos humados y cada uno de los responsables del manejo de información de la entidad.

Directrices:

- La gerencia debe de establecer y comunicar las responsabilidades de cada persona dentro del proceso de gestión de seguridad de la información.

- Cada persona dentro del sistema de gestión de seguridad de la información es responsable por el uso y almacenamiento de información en los activos que tenga a su cargo.

- La gerencia debe establecer los procedimientos para contactar e informar lo que sea necesario a las autoridades de control como el SiCoV, la Superintendencia y la autoridad ambiental del departamento.

- Está totalmente prohibido la transferencia de información por parte de cualquier responsable sin la debida autorización de la gerencia o saltando los procedimientos establecidos.

- Cada persona dentro del sistema de gestión es responsable por la información de maneje y asumirá las consecuencias legales y disciplinarias que su mal uso conlleve.

8.3.3 A.7 Política para seguridad de los recursos humanos.

8.3.3.1 A.7.1 Políticas de seguridad Antes de asumir el empleo. Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

Aplicabilidad:

Esta política aplica a la Gerencia y personal de recursos humanos encargados de la selección y verificación de datos de las personas a contratar.

Directrices:

- La gerencia debe definir claramente todos los antecedentes que la ley solicita y que la persona que aspira al cargo en convocatoria debe presentar sin ninguna excepción.

- El personal de recursos humanos es responsable y debe verificar la veracidad de los documentos presentados por el aspirante, que garanticen su idoneidad y que no presenta inhabilidad alguna para el cargo que se aspira.

- Los aspirantes al cargo en convocatoria son responsables de la documentación presentada y los problemas legales que conlleve el presentar una información falsa a la entidad.

- La Gerencia y personal de recursos humanos deben establecer en cada contrato con sus empleados, contratistas y proveedores, las responsabilidades que tienen dentro del sistema de gestión de la información dentro de la entidad y aun cuando su contrato o labor allá finalizado.

8.3.3.2 A.7.2 Políticas de seguridad durante la ejecución del empleo.

Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan

Aplicabilidad:

Esta política aplica a la Gerencia y cada uno de los empleados y contratistas dentro del sistema de gestión de la información.

Directrices:

- La gerencia del CEDAC debe comunicar, sensibilizar y exigir a todos los responsables ya sean empleados de planta o contratistas el cumplimiento e todas las políticas y procedimientos establecidos para el aseguramientos de la información.

- Cada empleado y contratista debe tomar conciencia de la responsabilidad que tiene en el cumplimiento de las políticas y procedimientos establecidos en el sistema de gestión de seguridad de la información.

- La gerencia debe redactar los procesos disciplinarios que se aplicaran en caso de que se compruebe, el incumplimiento de las políticas de seguridad por parte de algunos de los responsables dentro del sistema de gestión de seguridad de la información.

8.3.3.3 A.7.3 Políticas de seguridad para la Terminación o cambio de empleo.

Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo

Aplicabilidad:

Esta política aplica a la gerencia, personal de recursos humanos, empleados y contratistas de la entidad.

Directrices:

- La gerencia y personal de recursos humanos deben establecer en cada contrato y garantizar la comunicación de las responsabilidades que tienen los empleados y contratistas aun después de la culminación de su contrato o labor.

- Cada persona que culmine sus actividades o contrato en el CEDAC es responsables por la divulgación de la información a la que pudo tener acceso en este periodo de tiempo.

- La gerencia debe comunicar y capacitar a todo su personal sobre las consecuencias legales y disciplinarias que conllevan el incumplimiento de las políticas de seguridad establecidas.

8.3.4 A.8 Políticas de seguridad para la gestión de activos.

8.3.4.1 A.8.1 Política de responsabilidad para los activos. Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada

Aplicabilidad:

Esta política aplica directamente a la Gerencia, empleados y contratistas responsable de los activos de la entidad y a cada una de las personas que tengan bajo su responsabilidad un activo de información de la empresa.

Directrices:

- El responsable del manejo de los activos debe mantener un inventario de activos completamente actualizado y en donde se especifique su ubicación, fecha de ingreso a la entidad y responsable directo.

- El responsable del manejo de los activos de la entidad debe comunicar a cada uno de los empleados y contratistas la responsabilidad que tienen sobre cada activo que se le asigne.

- Se debe hacer firmar a cada responsable la entrega y comunicación de las responsabilidades que tienen sobre un determinado activo de información.

- La gerencia debe de gestionar capacitaciones comunicación de los procedimientos al personal sobre el uso aceptable de los activos de información.

- Cada persona es directamente responsable por el uso que le dé o que permita que otro le dé al activo de información a su cargo y asumirá las consecuencias legales y disciplinarias que esto implique.

- Todos los usuarios tienen prohibido el consumo de alimentos sobre los equipos.

- Cada persona es responsable de la devolución de sus activos en correcto estado tal y como se les entrego de lo contrario deberá responder económica, legal y disciplinariamente por el estado del mismo.

8.3.4.2 A.8.2 Política para clasificación de la información. Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.

Aplicabilidad:

Esta política aplica a la Gerencia, secretaria general, jefe de contabilidad, jefe de planta, jefe de archivo, asesor de calidad que son los encargados de manejar la información sensible de la empresa.

Directrices:

- Se debe clasificar la información contenida tanto en físico como en medios digitales según su nivel de criticidad.

- La información según su clasificación debe ser etiquetada y resguardada según su nivel.

- Se debe de establecer procedimientos de almacenamiento de la información física con el fin de preservarla y protegerla de cualquier factor ambiental.

- Se deben de establecer métodos de encriptación y acceso solo a personal autorizado para la información sensible que se encuentre almacenada digitalmente.

- Se deben establecer procedimientos para el traspaso o extracción de la información sensible cuando esto sea necesario.

8.3.4.3 A.8.3 política para el manejo de medios de soporte. Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.

Aplicabilidad:

Esta política aplica a la Gerencia, secretaria general, jefe de contabilidad, jefe de planta, jefe de archivo, asesor de calidad que son los encargados de manejar la información sensible de la empresa.

Directrices:

La información sensible almacenada en medios extraíbles se debe almacenar o resguardar en un lugar seguro como una caja fuerte a la cual solo tenga acceso la máxima autoridad de la entidad.

- Se deben establecer procedimientos de encriptación para los medios de soporte donde se almacene información sensible de la empresa.

- Se deben de establecer procedimientos de transporte seguro en caso de ser necesario él envió de medios extraíble con información sensible de la entidad.

8.3.5 A.9 políticas de control de acceso.

8.3.5.1 A.9.1 política de requisitos del negocio para control de acceso. Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información

Aplicabilidad:

Esta política aplica a la Gerencia, administrador del sistema y responsables del manejo de información de la entidad.

- El responsable de la administración del sistema debe establecer procedimientos que limiten el acceso de los usuarios solo a la información que estén autorizados a manejar.

- Se deben de restringir el acceso de usuarios no autorizados a los servicios de red mediante procedimientos de segmentación de la red.

- Cada usuario que tenga permisos para acceso a la red es responsable de la administración y custodia de sus credenciales de acceso y las consecuencias legales y disciplinarias que conlleve el suministrarlas.

8.3.5.2 A.9.2 política de gestión de acceso de usuarios. Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios

Aplicabilidad:

Esta política aplica a la Gerencia, administrador del sistema y responsables del manejo de información de la entidad.

Directrices:

- Se deben establecer procedimientos para la asignación de usuarios autorizados en el sistema y la información o servicios de red que el mismo puede utilizar.

- Se deben de establecer privilegios en los usuarios del sistema que limite la posibilidad de acceder o modificar información que no tenga nada que ver con su objeto de contrato.

- Se deben de revocar los usuarios que ya no pertenezcan a la entidad o modificar los privilegios de los usuarios que así lo requieran por modificación de sus actividades.

8.3.5.3 A.9.3 política de Responsabilidades de los usuarios. Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación

Aplicabilidad:

Esta política aplica a la gerencia y todo el personal empleados de planta y contratistas de la entidad responsables del manejo de la información.

Directrices:

- La gerencia debe de comunicar y exigir el cumplimiento de las políticas de seguridad y la importancia de no divulgar sus contraseñas y usuarios del sistema.

- La gerencia debe coordinar capacitaciones y charlas de sensibilización sobre buenas prácticas para el manejo de contraseñas

8.3.5.4 A.9.4 política de control de acceso a sistemas y aplicaciones. Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones

Aplicabilidad:

Esta política aplica al administrador del sistema y de la red de la entidad y cada empleado o contratista que tenga bajo su responsabilidad un activo de la entidad.

Directrices:

Se deben establecer procedimientos que impidan que personal no autorizado pueda entrar a la información o a los recursos de red de la entidad.

Se deben de establecer la asignación de usuarios y contraseñas para el ingreso a los recursos de red del sistema.

Se debe de limitar los usuarios de los sistemas operativos con el fin de impedir que estos puedan instalar programas que puedan anular la seguridad del sistema e impidan el acceso a las carpetas que contienen los códigos fuentes de los programas instalados por el administrador.

8.3.6 A.10 política de seguridad para la criptografía.

8.3.6.1 A.10.1 política para controles criptográficos. Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.

Aplicabilidad:

Esta política aplica al responsable de la administración del sistema y a cada usuario que tenga a sus cargos credenciales de autenticación para acceso a la información.

Directrices:

- Se deben desarrollar métodos de encriptación de la información lo cual impida que personal no autorizado la pueda acceder, modificar o borrar.

- Se deben de establecer procedimientos para la asignación de llaves criptográficas las cuales permitan firmar digitalmente la información para garantizar su procedencia.

- Está prohibido que los usuarios que tenga bajo su responsabilidad una llave criptográfica, la presten o suministre las credenciales para que sean usadas por otra persona diferente.

- Los usuarios que tengan asignadas llaves criptográficas deben responder legal y disciplinariamente por lo que con la misma se realice.

8.3.7 A.11 políticas para la seguridad física y del entorno.

8.3.7.1 A.11.1 política para áreas seguras. Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización

Aplicabilidad:

Esta política aplica a la Gerencia y a cada jefe de área, los cuales tienen bajo su cargo las llaves de acceso a las oficinas de la entidad.

Directrices:

- Se deben de señalizar y nombrar con claridad cada área de la empresa y delimitarlas mediante divisiones o muros.

- Cada área de la empresa debe de tener sus limitaciones de acceso como puertas con cerraduras.

- Se deben de señalizar las áreas con acceso restringido mediante letreros de prohibido el ingreso o solo personal autorizado.

- Cada área en de almacenamiento de información como archivo o cuarto de servidores deben permanecer bajo llave y con señalización de solo personal autorizado.

- Cada personal debe de informar sobre filtraciones o alteraciones en su área de trabajo que puedan poner en riesgo los activos que allí se encuentren.

8.3.7.2 A.11.2 Políticas para seguridad de los equipos. Objetivo. Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

Aplicabilidad:

Esta política aplica a todos los usuarios empleados y contratistas de la entidad que tengan a su cargo algún equipo de la misma.

Directrices:

- Se deben proteger los equipos mediante forros para impedir la acumulación de polvo o derrames de líquidos que puedan afectar su funcionamiento.

- Se deben e instalar UPS que impidan los cortes bruscos de energía y regulen el voltaje que llega a los equipos

- Las tomas de corriente y cables de energía conectados a los equipos deben de estar en buen estado, sin peladuras que puedan ocasionar un corto eléctrico.

- Se deben de establecer un cronograma claro para el mantenimiento de los equipos para asegurar su funcionamiento y disponibilidad.

- Se deben de establecer procedimientos adecuados para el mantenimiento preventivo y correctivo de los equipos.

- Se deben de establecer procedimientos para el retiro de los equipos de la entidad en caso que sea necesario el cual asegure la protección e integridad del equipo y la información que este pueda contener.

- Cuando un equipo vaya a ser reutilizado o se vaya a cambiar su usuario responsable se debe verificar la información que este contenga y de ser necesario removerla de forma segura, para impedir que el nuevo propietario

del activo tenga acceso a ella.

- Cada propietario de los activos debe de bloquear su equipo cada vez que se retire de su puesto de trabajo para impedir que personal no autorizado pueda acceder.

- Cada persona es responsable por la información física que deje sobre sus escritorios sin ninguna protección y asumirá las consecuencias que esta acción pueda traerle.

8.3.8 A.12 política para seguridad de las operaciones.

8.3.8.1 A.12.1 política para los procedimientos operacionales y responsabilidades. Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

Aplicabilidad:

Esta política aplica a la Gerencia y todos los responsables dentro del sistema de gestión.

Directrices:

- Se debe de establecer la forma adecuada para poner en conocimiento de todos los usuarios que lo requieran los procedimientos establecidos dentro del sistema de gestión de la seguridad de la información.

- la gerencia y cada uno de los responsables debe verificar continuamente cambios en la organización que puedan afectar los procedimientos establecidos y requieran de una modificación para no afectar la seguridad de la información.

- El responsable de la administración del sistema debe de verificar constantemente que los recursos ya sean de red o tecnológicos que maneja la entidad sean suficientes para su correcto funcionamiento y cumplimiento de su objeto misional

8.3.8.2 A.12.2 política para la protección contra códigos maliciosos. Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos

Aplicabilidad:

Esta política aplica a la gerencia, administrador del sistema y responsable de los activos.

Directrices:

- Se debe de adquirir un software especializado en la detección y eleimiacion de códigos maliciosos.

- El administrador del sistema debe de instalar en cada equipo de la entidad el software contra códigos maliciosos que se adquiera con su respectiva licencia.

- Cada responsable del activo debe de monitorear el correcto funcionamiento del software contra códigos maliciosos y verificar que se encuentre siempre actualizado.

8.3.8.3 A.12.3. Política para las Copias de respaldo.

Objetivo. Proteger contra la pérdida de datos.

Aplicabilidad:

Aplica al administrador del sistema y cada persona responsables de los activos informáticos dentro del sistema de gestión.

Directrices:

- El administrador del sistema debe de realizar una copia de seguridad del aplicativo de la base de datos de las revisiones tecnicomecanicas cada 24 horas y verificar su viabilidad.

- El administrador del sistema debe de realizar una copia de seguridad del software contable de la empresa cada 24 horas y verificar su viabilidad

- Los usuarios responsables de los activos de información deben de solicitar la realización de copias de respaldo de los archivos sensibles e indispensables para el cumplimiento de sus labores al administrador del sistema.

8.3.8.4 A.12.4 políticas para el registro y seguimiento. Objetivo. Registrar eventos y generar evidencia.

Aplicabilidad:

Esta política aplica a la gerencia, administrador del sistema y responsable del seguimiento y registros del sistema de gestión de seguridad de la información.

Directrices:

- Se deben crear todos los formatos de registro para todas las actividades que se llevan a cabo por los usuarios del sistema.

- Se deben establecer políticas de seguridad que garanticen la protección de estos registros e impidan su alteración o destrucción por personal no autorizado

- El administrador debe habilitar en el sistema los archivos logs que lleven un registro de auditoria de todas las actividades que se realizan en el y protegerlos para impedir que sean alterados o borrados

- El administrador del sistema debe de sincronizar todos los relojes a una misma fuente como por ejemplo el del servidor del NIST National Institute of Standards and Technology el cual lleva la hora mundial y en Colombia solo debemos de seleccionar la UTC que -5:00 horas.

- El responsable del seguimiento de los registros y eventos de seguridad debe de registrar absolutamente todo con el fin de evaluar y establecer acciones correctivas que impidan que esto se vuelva a presentar.

8.3.8.5 A.12.5 política para el control de software operacional. Objetivo. Asegurarse de la integridad de los sistemas operacionales

Aplicabilidad:

Esta política aplica directamente al administrador del sistema y a cada uno de los responsables de los activos de la entidad.

Directrices:

- El administrador del sistema debe configurar cuentas limitadas en los sistemas operativos para impedir que los usuarios instalen software no autorizado que pueda afectar el funcionamiento de los equipos

- El responsable de los activos tiene prohibido tratar de evadir las restricciones del administrador y asumirá las consecuencias legales y disciplinarias que esto conlleve.

8.3.8.6 A.12.6 política para la gestión de vulnerabilidades técnicas. Objetivo. Prevenir el aprovechamiento de las vulnerabilidades técnicas.

Aplicabilidad:

Esta política aplica al administrador del sistema y a todos los usuarios dentro del sistema de gestión de seguridad de la información.

Directrices:

- Cada usuario dentro del sistema de gestión de seguridad de la información está en la obligación de informar sobre posibles vulnerabilidades del sistema al administrador del sistema o a la gerencia con el fin de que se tomen medidas que eviten el aprovechamiento de estas vulnerabilidades.

- El administrador del sistema debe configurar cuentas limitadas en los sistemas operativos para impedir que los usuarios instalen software no autorizado que pueda afectar el funcionamiento de los equipos

- Está prohibido la instalación de software no autorizado en cualquier equipo de la entidad solo el administrador del sistema puede llevar a cabo esta función y después de haber verificado el derecho de propiedad intelectual del software.

8.3.8.7 A.12.7 políticas para las consideraciones sobre auditorías de sistemas de información. Objetivo. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos

Aplicabilidad:

Esta política aplica a la Gerencia y al administrador del sistema.

Directrices:

- El administrador del sistema debe de establecer un cronograma de auditorías y presentarlo a la gerencia para su aprobación.

- La gerencia debe de garantizar la comunicación del cronograma de auditoria con el fin de no causar mayor interrupción en las actividades de la entidad.

8.3.9 A.13 política para la seguridad de las comunicaciones.

8.3.9.1 A.13.1 política para la gestión de seguridad de redes. Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

Aplicabilidad:

Esta política de seguridad aplica directamente al administrador de la redes que maneja la entidad.

Directrices:

- El administrador de la red debe de establecer controles para impedir el acceso no autorizado a la misma

- El administrador de la red debe de establecer procedimientos para gestionar la identificación de los usuarios autorizados en el sistema y determinar a qué servicios de red tienen derecho según sus actividades.

- Se debe segmentar la red con el fin de que los usuarios solo tengan acceso a la información y servicios que su actividad requiera.

- No se deben compartir redes WiFi de la LAN privada de la empresa con los clientes de la misma

- Se debe de administrar una red totalmente separada de la red Privada de la entidad si se quiere dar el servicio de WiFi a los clientes

8.3.9.2 A.13.2 política para la transferencia de información. Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

Aplicabilidad:

Esta política de seguridad aplica a todos los usuarios dentro del sistema se seguridad de la información.

Directrices:

- Se deben de establecer procedimientos que garanticen que la transferencia de información es segura mitigando el riesgo de pérdida, alteración o daño de la misma.

- La gerencia debe de establecer dentro de los contratos con proveedores u otras partes externes cláusulas de transferencia segura de información y acuerdos de confidencialidad de la misma.

- El administrador del sistema debe configurar unos correos institucionales los cuales se puedan monitorear con el fin de garantizar que no se extraiga información sensible de la empresa a través de ellos.

- La gerencia y el personal de recursos humanos debe establecer dentro de los contratos de trabajo de los empleados de planta y contratistas acuerdos de confidencialidad y dejar clara las consecuencias legales y disciplinarias que su incumplimiento puede acarrear.

8.3.10 A.15 politicas de seguridad para las relaciones con los proveedores

8.3.10.1 A.15.1 política para la seguridad de la información en las relaciones con los proveedores. Objetivo. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

Aplicabilidad:

Esta política aplica a la Gerencia, personal de recursos humanos y proveedores.

Directrices:

- Cada vez que un proveedor deba acceder a la entidad la gerencia debe de delegar a una persona que le haga acompañamiento y garantice que nos e tengan accesos no autorizados a los activos de la entidad

- Cada proveedor que entre a la entidad se le debe comunicar por parte del área de recursos humanos que está siendo grabado y monitoreado para cámaras de vigilancia y que autoriza que su imagen sea registrada y administrada por el CEDAC.

- Se debe de comunicar a cada proveedor los acuerdos de confidencialidad que tiene establecidos la empresa y las consecuencias legales que implica el incumplirlos

8.3.10.2 A.15.2 política para la gestión de la prestación de servicios de proveedores. Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

Aplicabilidad:

Esta política aplica a la Gerencia, personal de recursos humanos y proveedores

Directrices:

- El personal de recursos humanos debe hacer seguimiento a las actividades de los proveedores con el fin de evaluar sus servicios

- La gerencia debe de gestionar cualquier cambio en el suministro de los servicios de los proveedores con el fin de evaluar las políticas de seguridad y verificar si es necesario mejorarlas o modificarlas

- La gerencia debe solicitar a los proveedores informe de sus actividades que garanticen el cumplimiento de sus objetivos.

8.3.11 A.16 política de seguridad para la gestión de incidentes de seguridad de la información.

8.3.11.1 A.16.1 política para la gestión de incidentes y mejoras en la seguridad de la información. Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.

Aplicabilidad:

Esta política aplica a la Gerencia y todos los responsables dentro del sistema de seguridad de la información.

Directrices:

- La gerencia debe establecer las responsabilidades de los usuarios que atenderán de forma rápida y eficaz los incidentes de seguridad de la información.

- Se debe establecer los procedimientos que los responsables de atender los incidentes de seguridad deben seguir para que esta labor se pueda realizar de forma ordenada.

- Los responsables de cada uno de los activos deben de informar a tiempo cualquier incidente de seguridad de la información que se presente

- Todos los usuarios dentro del sistema de seguridad de la información tienen la obligación de informar acerca de debilidades o vulnerabilidades que presente el sistema.

- El administrador del sistema debe establecer una clasificación de los incidentes de seguridad con el fin de poder establecer si lo que ocurre clasifica o no como un incidente de seguridad de la información.

- La gerencia y administrador del sistema deben de evaluar los incidentes de seguridad de la información con el fin de analizar su causa y establecer nuevas políticas o modificar las existentes para mitigar el riesgo de incidentes futuros.

- El administrador del sistema debe de recolectar evidencia que permita establecer porque se presentó el incidente de seguridad.

- El administrador del sistema debe de establecer procedimientos para la recolección, almacenamiento y análisis de la evidencia que se logre reunir.

- Se deben de aplicar las cláusulas legales y disciplinarias a los usuarios que se les compruebe su responsabilidad en un incidente de seguridad de la información.

8.3.12 A.17 política para los aspectos de seguridad de la información de la gestión de la continuidad de negocio.

8.3.12.1 A.17.1 política para la continuidad de seguridad de la información. Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.

Aplicabilidad:

Esta política es aplicable a la Gerencia administrador del sistema y jefes de área

Directrices:

- La gerencia, administrador del sistema y los jefes de área deben definir claramente los requisitos de información que requiere la entidad para continuar con su funcionamiento aun después de una crisis o un desastre natural

- El administrador del sistema debe de establecer los procedimientos a seguir en caso que aseguren la restauración de la información que necesita la empresa para poder seguir operando.

- El administrador del sistema debe de verificar cada determinado periodo de tiempo que los procesos establecidos para la restauración de la información sean eficaces y funcionales de los contrario se deben de replantear los procedimientos y evaluarlos con el fin de garantizar la continuidad del negocio.

8.3.12.2 A.17.2 política para el aseguramiento de la redundancia. Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información.

Aplicabilidad:

Esta política de seguridad aplica directamente al administrador del sistema.

Directrices:

- El administrador del sistema debe de configurar los servidores en RAID 1 como mínimo o Mirror (espejo), lo cual garantice que la información se está copiando en dos discos duros simultáneamente y en caso de que uno falle toda la información estará almacenada en el otro disco.

- El administrador debe de verificar periódicamente que los dos discos estén trabajando

- El administrador del sistema debe de establecer procedimientos para el reemplazo de los discos duros en caso de que estos se llenen por completo.

8.3.13 A.18 políticas de seguridad para el cumplimiento.

8.3.13.1 A.18.1 política para el cumplimiento de requisitos legales y contractuales. Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

Aplicabilidad:

Esta política aplica a la Gerencia y todos los usuarios dentro del sistema de seguridad de la información.

Directrices:

- La gerencia debe de mantener actualizados todos los requisitos legales, contractuales y estatutarios que la empresa como entidad pública debe de cumplir referente a cada sistema de información que maneje.

- El personal de recursos humanos debe mantener actualizados en la página del Secop toda la contratación que la empresa como entidad pública realiza.

- La gerencia y el administrador del sistema deben de garantizar que todo el software que utiliza la empresa esté debidamente licenciado cuando se requiera.

- Cada usuario es responsable por la violación de los derechos de propiedad intelectual que conlleve el almacenamiento de información no autorizada en sus equipos como música, videos, juegos entre otros.

- La gerencia y el personal de recursos humanos debe asegurar de colocar en sus contratos que el empleado, contratista, proveedor o cliente de la empresa autoriza al CEDAC a administrar la información de los datos personales que estos suministren a la entidad y que son informados de sus derechos tal como lo establece la Ley 1581 de 2012.

- El administrador del sistema debe de garantizar la encriptación de la información sensible que se encuentre almacenada en los servidores del CEDAC.

8.3.13.2 A.18.2 política para las revisiones de seguridad de la información. Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.

Aplicabilidad:

Esta política aplica a la gerencia y cada uno de los usuarios dentro del sistema de seguridad de la información.

Directrices:

- La gerencia debe de garantizar el seguimiento y cumplimiento de todas las políticas de seguridad establecidas en la empresa.

- La gerencia y usuarios dentro del sistema de seguridad de la información debe de verificar que todos los procedimientos de seguridad de la información establecidos para su área se estén cumpliendo de forma apropiada

- Los usuarios deben de informar el incumplimiento de cualquier política de seguridad de la información ya sea de su área o cualquier otra con el fin de impedir cualquier incidente de seguridad.

- Los usuarios deben ser conscientes que el incumplimiento de las políticas y procedimientos establecidos para la seguridad de la información conllevara a investigaciones y aplicación de cláusulas legales y disciplinarias.

9. CONCLUCIONES

Con el estudio de cada uno de los objetivos de control que establece la norma ISO/IEC 27001:2013 - ANEXO A se entendió con mayor claridad y de esta forma se explicó a la empresa porque le son aplicables o no estos controles y a quienes aplicaría o va dirigido estas políticas de seguridad, lo cual es de suma importancia porque en un sistema de gestión de seguridad de la información se deben definir y comunicar muy bien las responsabilidades y deberes que tienen cada persona, sea empleado, contratista, proveedor o incluso la alta gerencia dentro del sistema.

Se pudo determinar que en la entidad son aplicables todos los controles establecidos en la Norma; excepto: 1. El objetivo de control A.6.2., con sus dos respectivos controles (A.6.2.1. – A.6.2.2.), los cuales hacen referencia a dispositivos móviles y teletrabajo; dado que, la entidad efectúa el cumplimiento de su objeto misional con inspección, control y vigilancia en tiempo real. 2. La categoría de control A14 en su totalidad que hace referencia al desarrollo, mantenimiento y soporte de software; dado que, el objeto misional de la entidad es la Revisión Tecnicomecanica y de Emisiones Contaminantes, mas no el desarrollo mantenimiento y soporte de software.

Se determinó que la empresa cuenta con un gran número de activos como lo son equipos de cómputo, servidores, impresoras, toda una red LAN, paquetes de software como TNS para la contabilidad, software de revisión tecnicomecánica SOLTELEC y sistemas operativos Windows para los equipos de cómputo, pero ninguno de estos activos poseen controles para mitigar cualquier tipo de amenazas como riesgos de pérdidas, alteración o robo de la información e incluso controles en la red que impidan el ataque de intrusos desde fuera de la entidad; es decir, la empresa se encuentra totalmente vulnerable a cualquier ataque o es más, una simple falla en el sistema podría terminar en una gran pérdida de información que a su vez se podría traducir en un detrimento patrimonial y sanciones por parte de las autoridades de control, por tal motivo se propuso unas políticas de seguridad de la información basadas en la Norma ISO/IEC 27001 – ANEXO A para todos los controles que le son aplicables a la empresa y que con su implementación podrían mitigar considerablemente los riesgos de amenazas al sistema de información.

Se pudo proponer a La Gerencia de la entidad y esta logró comprender que la Propuesta para Implementación de Controles Establecidos por la Norma ISO/IEC 27001 - ANEXO A, aunque represente una inversión económica, esta no es nada comparable con los grandes beneficios que traería a la empresa y a su vez se dejó claro que este trabajo no contempla el proceso de certificación de la misma, ya que para ello será necesario el desarrollo de un nuevo proyecto que lo

establezca dentro de sus objetivos y que dependerá de la aceptación por parte del máximo órgano de la entidad como lo es la Junta Directiva.

10. RECOMENDACIONES

Se recomienda a la alta gerencia del CEDAC capacitar y sensibilizar a todo su personal en lo que es Seguridad de la información haciendo énfasis en los grandes beneficios que esto puede traer a la compañía.

Todos los usuarios de la empresa deben asumir su responsabilidad sobre todos los activos que manejen y protegerlos como si fueran de su propiedad, con el fin de prevenir pérdidas de información lo cual les impedirá realizar correctamente sus actividades e incluso traer pérdidas económicas a la entidad.

Se deben de proteger las áreas como oficinas, cuarto de servidores, central de redes entre otras de acceso de personal no autorizados que puedan tener la intensión realizar daño a la entidad.

Se recomienda a la gerencia no compartir redes WiFi que pertenezcan a la red privada con los clientes, ya que estarían dando acceso a cualquier persona a la información de viaja a través de esta red.

Si se quiere dar servicio de WiFi gratuito a los clientes se debe de instalar un servicio totalmente aparte de la red LAN de la compañía.

Para la ingesta de alimentos los empleados y contratistas deben de usar solo el área de cafetería, por ningún motivo se deben de ingerir alimentos en las oficinas o sobre los equipos, ya que esto aumenta el riesgo de derrame de algún liquido o residuos de comida que pueden alterar el funcionamiento de los mismos o incluso dañar información que se tenga sobre los escritorios.

La Gerencia debe prohibir el uso de dispositivos externos que no pertenezcan a la entidad y los que pertenezcan solo deben ser utilizados por personal autorizado para impedir la extracción no autorizada de información.

Se recomienda a la gerencia prohibir totalmente la grabación de música en los equipos de la entidad ya que si no se conoce su procedencia puede acarrear problemas legales por derechos de propiedad intelectual o al ser descargadas desde internet pueden ir ocultos en estos archivos códigos maliciosos que terminarían infectando los equipos.

Se debe de establecer correos institucionales los cuales puedan ser fácilmente monitoreados ara tener una constante verificación de que información reciben los usuarios y que no envíen información la cual no tengan autorizada.

Se recomienda a todos los responsables de los activos informar a tiempo sobre cualquier mensaje de error o de falta de actualización que muestre el sistema con el fin de tener siempre las últimas actualización de seguridad correctamente instalada.

Se recomienda a la Gerencia y personal de recursos Humanos establecer cláusulas de confidencialidad o no divulgación para empleados, contratistas y proveedores y dejar claro las consecuencias legales que conlleva su incumplimiento.

Se recomienda a la Alta Gerencia la implementación de todos los controles de la Norma ISO 27001:2013 que le sean aplicables a la empresa, ya que aunque se deba realizar un esfuerzo económico, este sería poco en comparación con los grandes beneficios que un sistema de gestión de seguridad de la información (SGSI) traería a la organización.

BIBLIOGRAFÍA

ARAYA, D. Glosario de términos de Seguridad Informática. [En línea]. [Consultado 20 de noviembre 2016]. Disponible en Internet: http://safemode-cl.blogspot.com.co/2006/07/glosario-de-terminos-de-seguridad.html.

CENTRO DE DIAGNÓSTICO AUTOMOTOR DE CÚCUTA LTDA. Manual de Procedimientos Administrativos: GTH-02-R-03, Versión 1. Cúcuta: CEDAC; 2017.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 (05, enero, 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. Diario oficial. Bogotá D.C., 2009. No. 47.223. 4 p.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1341 (30, julio, 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Diario oficial. Bogotá D.C., 2009. No. 47.426. 33p.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 603 (27, julio, 2000). Por la cual se modifica el artículo 47 de la Ley 222 de 1995. Diario oficial. Bogotá D.C., 2000. No. 44.108. 2 p.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley Estatutaria 1266 (31, diciembre, 2008). 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. Diario oficial. Bogotá D.C., 2008. No. 47.219. 17 p.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley Estatutaria 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario oficial. Bogotá D.C., 2012. No. 48.587. 13p.

GOMEZ, Á. Enciclopedia de la Seguridad Informática. México: Alfaomega; 2007.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Compendio seguridad de la información: norma técnica colombiana NTC-ISO-IEC 27001. Bogotá: ICONTEC; 2015. p.1.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Normas Colombianas para la Tecnología de la Información. Técnicas de Seguridad. Código de Practica para la Gestión de la Seguridad de la Información. Bogotá: ICONTEC; 2007.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Normas Colombianas para la presentación de documentación; presentación de tesis; trabajos de grado y otros trabajos de investigación. Bogotá: ICONTEC; 2008.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Normas Colombianas para las referencias bibliográficas; contenido; forma y estructura. Bogotá: ICONTEC; 2008.

LOPEZ, D. Evolución de la Seguridad Informática. [En línea]. [Consultado 18 de noviembre 2016]. Disponible en Internet: https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica.

MINISTERIO DE TRANSPORTE DE COLOMBIA. Registro Único Nacional de Tránsito - RUNT. Organismos de Tránsito. [En línea]. [Consultado 14 de mayo 2018]. Disponible en internet: (http://www.runt.com.co/directorio-de-actores?title=&field_tipo_value=3&field_c_digo_municipio_value=54001000&field_c_digo_departamento_value_1=54).

MINISTERIO DE TRANSPORTE DE COLOMBIA. Resolución 3768 (26, septiembre, 2013). Por la cual se establecen las condiciones que deben cumplir los Centros de Diagnóstico Automotor para su habilitación, funcionamiento y se dictan otras disposiciones. Diario oficial. Bogotá, 2013. No. 48.926. p.16.

NOTARIA CUARTA DE CUCUTA. Escritura Pública Nº 3585 (23, diciembre, 1992). Cúcuta, 1992. 7 p.

NOTARIA PRIMERA DE CUCUTA. Escritura Pública Nº 1077 (10, mayo, 2006). Cúcuta, 2006. 5 p.

NOTARIA PRIMERA DE CUCUTA. Escritura Pública Nº 857 (18, abril, 1980). Cúcuta, 1980. 16 p.

NOTARIA QUINTA DE CUCUTA. Escritura Pública Nº 1271 (07, abril, 1994). Cúcuta, 1994. 4 p.

PALACIOS, D. Diseño de un sistema de gestión de seguridad de la información (SGSI) para el área de informática de la Cooperativa del Magisterio de Túquerres bajo la norma ISO 27001:2013. Tesis de Especialización. San Juan de Pasto: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería; 2015.

PORTAFOLIO. Así roban la información de las empresas los piratas informáticos. [En línea]. [Consultado 10 de mayo 2018]. Disponible en Internet: http://www.portafolio.co/innovacion/asi-roban-la-informacion-de-las-empresas-los-piratas-informaticos-506522.

RODRIGUEZ, A. La importancia de la Seguridad Informática. [En línea]. [Consultado 10 de mayo 2018]. Disponible en internet: http://www.trustdimension.com/la-importancia-de-la-seguridad-informatica/

SEMANA. Tecnología. Las empresas en Colombia no invierten en seguridad digital. Bogotá. 09, junio, 2016. [En línea]. [Consultado 10 de mayo 2018]. Disponible en Internet: https://www.semana.com/tecnologia/articulo/colombia-no-invierte-en-seguridad-digital/492724.

SUAREZ, S. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Tesis de Especialización. Bogotá: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería; 2015.

VARON, E. Diseño de las políticas de seguridad de la información aplicables para la empresa grupo empresarial Ardila & Asociados alineadas a la norma ISO27001:2013.Tesis de Especialización. Bogotá: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería; 2015.

VILLACIS, M. Diseño de un sistema de seguridad de la información (SGSI) basado en la Norma ISO 27001:2013 para la red corporativa de la empresa Ecuatronix. Trabajo de grado. Quito Ecuador: Universidad Politécnica Salesiana Sede Quito, 2016.